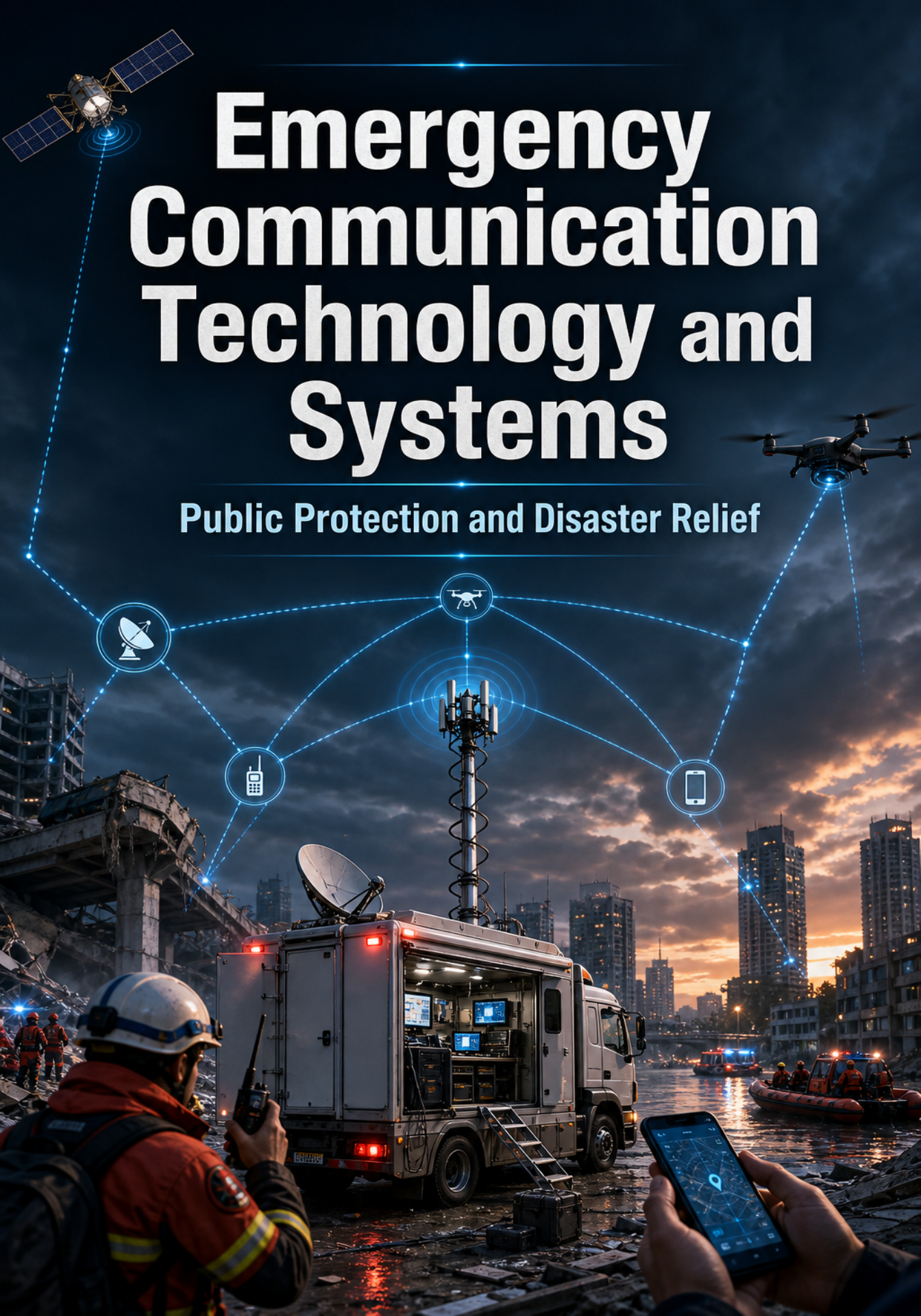
Emergency Communication Technology and Systems

Public Protection and Disaster Relief



Emergency Communication Technology and Systems:Public Protection and Disaster Relief

Kaven Wang

This book is available at https://leanpub.com/emcom

This version was published on 2026-08-09

Contents

Preface

Emergency communication serves as the "information lifeline" for handling sudden and unexpected incidents. In natural disasters, major accidents, and public safety events, conventional communication networks are often partially or completely disrupted due to damaged infrastructure. Emergency communication systems must therefore provide reliable information transmission under the most adverse channel conditions, supporting emergency command, rescue operations, and public services. As China's overall capacity for disaster prevention, mitigation, and relief continues to improve, the requirements for emergency communication support are also constantly rising, creating an urgent need to systematically master the principles, standards, and engineering practices of the various technical systems in the field of emergency communication.

This book systematically organizes the mainstream technical systems in the field of emergency communication. The book comprises twelve chapters in total, covering requirements analysis and system architecture for emergency communication, as well as various technical systems including satellite communication, shortwave communication, digital trunking communication, public mobile networks, ad hoc networks, space-air-ground integration, wireless through-the-earth communication, and multi-network converged emergency communication. It also looks ahead at the application of frontier technologies in emergency communication, such as integrated sensing and communication, large language models, network digital twins, reconfigurable intelligent surfaces, terahertz communication, and semantic communication. The arrangement of each chapter is as follows.

Chapter 1, Introduction, presents the basic concepts and classification of emergency communication, along with the domestic and international standard systems and development status of emergency communication. Chapter 2, Requirements Analysis for Emergency Communication Systems, systematically describes the requirement characteristics of emergency communication systems from the dimensions of services, performance, and reliability. Chapter 3, Emergency Communication System Architecture, establishes a layered reference model for emergency communication systems and discusses

the technology selection and engineering practice at the levels of on-site networking, regional relay, and wide-area transmission, while also introducing communication support contingency plans and drill mechanisms. Chapters 4 through 10 systematically introduce the operating principles, standard systems, key technologies, and engineering applications of each technical system for satellite emergency communication, shortwave emergency communication, digital trunking emergency communication, public mobile network emergency communication, ad hoc network emergency communication, space-air-ground integrated emergency communication, and wireless through-the-earth communication, respectively. Chapter 11, Multi-Network Converged Emergency Communication, focuses on the interconnection and interoperability mechanisms of heterogeneous networks, the design of converged communication gateways, and integrated networking strategies. Chapter 12, Frontier Technologies and Development Trends, introduces the latest advances in frontier technologies such as artificial intelligence, new wireless technologies, and semantic communication in the field of emergency communication.

This book strives to balance theoretical foundations with practical utility – tracing both the physical mechanisms and standard specifications of each technology, while also addressing the constraints and typical cases of engineering deployment; delving into the internal logic of individual technical systems while also focusing on the overall capability of multi-system integration. In terms of technical depth, the book provides a relatively detailed treatment of the air-interface standards, protocol systems, and key parameters of each communication system, offering readers a reference for engineering design and technical research.

This book is primarily intended for engineers, technical personnel, and researchers in emergency communication, wireless communication, and related fields. It can also serve as a teaching reference for graduate students and senior undergraduates in communication engineering, emergency management, and related disciplines at universities and colleges.

In the course of writing this book, extensive reference was made to technical standards, industry specifications, and research reports issued by international standardization bodies such as the ITU, 3GPP, ETSI, IETF, ATIS, and TIA, as well as by domestic authorities and standardization organizations such as the Ministry of Emergency Management, the Ministry of Industry and Information Technology, and the China Communications Standards Association, along with papers and monographs published by scholars in China and abroad

in the fields of emergency communication and wireless communication. The authors of the above-mentioned literature are hereby sincerely thanked.

Emergency communication technology is developing rapidly, and the related standards and engineering practices are continuously evolving. Given the limitations of the editors' expertise, shortcomings or omissions are unavoidable in this book, and readers and experts are earnestly invited to offer their criticism and corrections.

Chapter 1 Introduction

Emergency communication serves as the "information lifeline" for the disposal of sudden incidents (emergencies). It must provide reliable and timely communication support for first-line rescue personnel, minimize loss of life and property under emergency conditions to the greatest extent possible, and create favorable conditions for post-disaster recovery.

1.1 Concepts Related to Emergency Communication

1.1.1 Emergencies

An **emergency** is defined as a natural disaster, accident, public health incident, or social security incident that occurs suddenly, causes or may cause serious harm to society, and requires emergency response measures.

(1) **Natural disasters.** These mainly include flood and drought disasters, meteorological disasters, earthquake disasters, geological disasters, marine disasters, biological disasters, and forest and grassland fires.

(2) **Accidents.** These mainly include various production safety accidents at industrial, mining, and commercial enterprises; transportation accidents; marine oil spills; accidents involving public facilities and equipment; nuclear accidents; fires; and ecological and environmental incidents, network security incidents, network data security incidents, and information security incidents.

(3) **Public health incidents.** These mainly include infectious disease outbreaks, mass illnesses of unknown cause, mass poisoning incidents, food safety accidents, drug safety incidents, animal epidemics, and other incidents that seriously affect public health and safety.

(4) **Social security incidents.** These mainly include criminal cases, terrorist incidents, mass incidents, ethnic and religious incidents, and financial, foreign-related, and other emergencies that affect market and social stability.

Based on the degree of social harm and scope of impact, natural disasters, accidents, and public health incidents are classified into four levels: particularly major, major, relatively major, and general.

ITU-T Recommendation Y.1271 classifies emergencies by their possible source into natural disasters and man-made disasters, as shown in Table 1.

Table 1. Natural Disasters and Man-Made Disasters

Natural Disasters	Man-Made Disasters
Avalanche	Arson
Drought	Chemical spill
Earthquake	Industrial or national system collapse
Epidemic	Explosion
Flash flood	Gas leak
Famine	Fire
Flood	Nuclear explosion
Forest fire	Pipeline rupture
Lightning strike	Aircraft crash / emergency landing
Hurricane	Poisoning
Landslide / debris flow	Radiological contamination
Severe cold, snow disaster, hail, or extreme heat	Ship collision / capsizing
Storm tide	Stampede (of cattle, horses, etc.)
Tornado	Subway collision / derailment
Tsunami	Terrorist attack
Typhoon	Train collision / derailment
Volcanic eruption	Water-related accidents
Storm	

Emergencies are typically characterized by suddenness, destructiveness, and uncertainty, and may threaten the safety of people's lives and property, public safety, ecological and environmental security, or social order. Improving the capacity to prevent and respond to emergencies, and controlling, mitigating, and eliminating the harm they cause, are important goals of emergency management.

1.1.2 Emergency Response

The emergency response level for a given incident is classified, from highest to lowest, into Level I, Level II, Level III, and Level IV, based on the nature and

characteristics of the incident and the degree of harm and scope of impact it may cause.

The handling of an emergency typically proceeds in stages. First, first responders at the disaster site must promptly assess the extent of the disaster and control the scope of damage. Second, the primary task shifts to treating the injured and saving lives. Third, more rescue personnel, equipment, and supplies are typically brought in – these resources may come from pre-positioned sites, reserve facilities, or temporary staging areas. Fourth, the work turns mainly to on-site cleanup and restoration of order.

Ensuring the smooth progress of each stage of response depends critically on having a fast, reliable, and easy-to-operate emergency communication system – one that can sustain the continuity and effectiveness of rescue operations even when roads, power, and networks are all cut off, and that provides communication support for disaster dispatch, resource allocation, and life-safety assurance at every key link.

1.1.3 Emergency Communication Command

Emergency communication command refers to the overall management activity in which an authorized emergency command organization, building on the emergency communication system during the handling of an emergency, exercises unified organization, coordination, and control over all parties participating in rescue operations, through information collection, comprehensive assessment, instruction generation, resource dispatch, and effect feedback. Its core function is to convert communication capability into actual command effectiveness, ensuring efficient coupling between the "information flow" and the "command chain." Drawing on leading standards, the functional connotation of emergency communication command can be divided into the following four dimensions.

(1) **Command and coordination communication**: refers to the communication capability that achieves vertical connectivity between command echelons and horizontal coordination across them, supporting the operation of the command system. This specifically includes real-time voice, video, and data links between higher-level command centers and forward command posts, as well as cross-agency coordination communication capability among peer departments such as public security, fire and rescue, and medical services.

(2) **On-site response communication**: refers to the localized communication support capability built for the forward command post and the rescue site, including wireless trunked networking, on-site data aggregation, video backhaul, and emergency broadband access, which directly support real-time situational awareness, tactical coordination, and task dispatch for on-site rescue personnel.

(3) **Intelligence-gathering communication**: refers to the communication capability that achieves the collection, transmission, and aggregation of disaster information through forward reconnaissance, sensor network deployment, unmanned platform access, and external information retrieval, providing information support for command echelons at all levels to conduct situational assessment, intelligence processing, and decision support.

(4) **Public-facing command communication**: refers to the information-release and liaison communication capability directed at the public and social coordination forces, enabling functions such as disaster warning issuance, public information notification, acceptance of requests for public assistance, and coordinated mobilization of social resources, thereby improving the public-facing emergency response and public service capability.

To meet the needs of command activities, command organizations must, through the combined effect of personnel support, technical support, equipment support, and mechanism support during disaster response, provide efficient and reliable communication support for intelligence gathering, data transmission, and command dispatch on the ground. Emergency communication is responsible for the rapid and reliable delivery of information, while emergency communication command is responsible for processing, judging, and issuing action instructions based on that information. Table 2 illustrates the distinction and relationship between the two.

Table 2. Relationship Between Emergency Communication and Emergency Communication Command

Dimension	Emergency Communication	Emergency Communication Command
Core problem	Establishing a reliable communication link	Achieving efficient command decisions based on communication

Dimension	Emergency Communication	Emergency Communication Command
Object of study	Communication systems, protocols, spectrum, equipment	Command system, dispatch mechanisms, information processes, decision support
Technical focus	Radio propagation, network architecture, QoS, coverage	Audio/video calls, video conferencing, video surveillance, GIS situational display, dispatch platforms
Dependency	Emergency communication is the infrastructure of emergency communication command	Emergency communication command is the purpose for which emergency communication is used
Consequence of failure	Communication is interrupted and command cannot proceed	Command is thrown into disorder – rescue cannot be carried out effectively even if communication remains functional

1.1.4 Definition of Emergency Communication

The concept of "emergency communication" carries different emphases across different contexts and standards systems. The Radiocommunication Sector of the International Telecommunication Union (ITU-R), the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T), and various countries' laws, regulations, and industry standards have each defined emergency communication from the perspective of their own business scenarios and technical frameworks. Overall, they share a common core objective: to ensure that critical communication capability remains available under conditions of sudden incidents, disasters, or public crises, so as to provide communication support for emergency command, rescue operations, and public services.

1. ITU-R's Definition of PPDR

In the radiocommunication domain, ITU-R uses the term "Public Protection and Disaster Relief" (PPDR) to refer to the core scenarios of emergency com-

munication. Under Resolution 646 (Rev.WRC-19), adopted at the 2019 World Radiocommunication Conference, PPDR is defined as the combination of two categories of radiocommunication activity:

(1) **Public Protection (PP)**: radiocommunications used by agencies and organizations responsible for maintaining law and order, protecting life and property, and responding to emergencies. Typical implementing agencies include police, fire and rescue services, and emergency medical services – the day-to-day public-safety bodies.

(2) **Disaster Relief (DR)**: radiocommunications used by agencies and organizations responding to serious disruptions of societal functioning that pose a widespread threat to human life, health, property, or the environment, whether caused by accident, natural forces, or human activity, and whether occurring suddenly or developing over a long period.

PP communication is oriented toward routine, day-to-day public-safety law-enforcement communication and emphasizes continuity of coverage and service stability; DR communication targets large-scale, non-routine emergencies and emphasizes rapid deployment and interoperability under conditions of damaged infrastructure.

2. ITU-T's Definition of ETS

ITU-T instead approaches the subject from the perspective of network capability and service assurance, proposing the concept of "Emergency Telecommunications Service" (ETS). ITU-T Y.1271 expresses the core requirement of emergency telecommunications as follows: emergency telecommunications are intended to ensure that users who must communicate during a disaster obtain the communication channels they need, with appropriate security and the best possible quality of service. To meet this requirement, emergency communication can be realized using shared resources of public communication networks, or it can be supplemented by dedicated network resources such as public-safety networks; the underlying network architecture is evolving from traditional circuit switching toward packet switching.

3. Definitions of Emergency Communication in the United States

In the United States, the institutional definition of emergency communication is likewise dispersed across laws, executive orders, and technical standards at different levels.

(1) Title XVIII of the Homeland Security Act of 2002 (as amended repeatedly),

together with Executive Order 13618, "Assignment of National Security and Emergency Preparedness Communications Functions," signed in 2012 by then-President Obama, together establish the basic requirement for the federal government to build a sound emergency communication support system. The former authorizes and requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and continually update the National Emergency Communications Plan (NECP) to support and enhance the ability of emergency responders and relevant government officials to maintain continuous communication during a disaster, and to promote nationwide interoperable emergency communication. This plan is developed pursuant to Title XVIII of the 2002 Homeland Security Act, under which the law requires CISA to put forward recommendations that support and promote the continuous-communication capability of emergency responders and relevant government officials in the event of a disaster, and that ensure, accelerate, and achieve nationwide interoperable emergency communication. Executive Order 13618 explicitly requires that the federal government, under any circumstances, must always possess the communication capability needed to carry out its most critical and time-sensitive missions, and it designates the Department of Homeland Security as the coordinating body for National Security and Emergency Preparedness (NS/EP) communications. The order simultaneously revoked the earlier Executive Order 12472, abolishing the institutional structure of the National Communications System (NCS). CISA carried out a substantive revision of the NECP in 2019, adding cybersecurity objectives to address new technology developments and to remedy weaknesses in aging legacy systems; CISA has continued to publish updated materials for the plan as required by law since then.

(2) At the level of specific telecommunication resource dispatch and priority-assurance mechanisms, the U.S. Federal Communications Commission (FCC), pursuant to Appendix A of Part 64 of Title 47 of the Code of Federal Regulations, established the Telecommunications Service Priority (TSP) system. The U.S. grading mechanism is built on the importance of the telecommunication service itself to National Security and Emergency Preparedness (NSEP) missions: priority levels run from highest to lowest as Level E (dedicated to the activation of emergency telecommunication services) and Levels 1, 2, 3, 4, and 5 (applicable to the activation and line-repair/restoration of important telecommunication services). This system is governed by rules set by the FCC, with day-to-day administration by the U.S. Department of Homeland Security; it operates around the clock as a standing

system whose activation does not depend on whether a major disaster or state of war has occurred. Federal, state, tribal, and local public-safety agencies – police, fire, and emergency medical services – typically correspond to Priority Level 3, while national security leadership and certain military communication lines occupy the highest Levels 1 and 2.

(3) At the level of technical standards, the National Fire Protection Association (NFPA) published the first edition of NFPA 1225, *Standard for Emergency Services Communications*, in 2022, consolidating the earlier NFPA 1061, *Standard for Professional Qualifications for Public Safety Telecommunications Personnel*, and NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*. Although this standard is issued by a private standards-development organization rather than a federal agency, it has been widely adopted as a mandatory technical basis by fire and emergency-management departments across U.S. states and municipalities. It defines the minimum requirements for the job performance of public-safety telecommunications personnel, as well as the minimum technical requirements for communication systems, relay equipment, dispatch, performance levels, and installation quality.

Drawing on the relevant research and standards above, this book offers the following definition: **emergency communication** is a set of communication means and methods that comprehensively make use of various communication resources when an emergency occurs, in order to support rescue, emergency assistance, and other necessary communication needs. It is a temporary, special communication mechanism established to respond to natural or man-made emergencies – particularly one that, when conventional communication is interrupted, provides timely and reliable means of information transmission and ensures information exchange among all parties participating in emergency response.

1.1.5 Connotation and Core Characteristics of Emergency Communication

Emergency communication is not a single technical concept but a systemic capability formed by a set of interrelated characteristics. ITU-R defines emergency communication as “mission-critical communication”: regardless of the technology or network deployment form used, emergency communication must possess security, reliability, and high availability.

(1) **Mission-criticality.** Mission-criticality is the fundamental attribute that distinguishes emergency communication from other types of communication: a communication is mission-critical whenever its failure could directly lead to loss of life, major property damage, or the breakdown of societal functioning. From an engineering standpoint, this is mainly reflected in three respects. First, non-interruptibility: emergency communication systems must continue operating under extreme conditions such as damaged infrastructure or power outages, and therefore require survivability capabilities such as independent power supply, structural reinforcement, and seismic protection. Second, time-sensitivity: emergency instructions and on-site information must be transmitted within strict time limits — for example, ITU-R M.2377-2 specifies that call-setup latency for mission-critical voice communication should be less than 500 ms, and end-to-end voice/data transmission latency should be less than 1 s. Third, zero tolerance for error: in rescue and emergency decision-making scenarios, erroneous information, communication interruptions, or delayed instructions can all cause irreversible consequences, so system design must prioritize reliability and stability over cost or efficiency optimization alone.

(2) **High reliability and high availability.** Reliability describes a system's ability to perform its specified functions under specified conditions; availability describes the proportion of time a system remains in a normally usable state. Emergency communication systems' requirements for these two metrics far exceed those of commercial systems.

(3) **Security.** The information carried by emergency communication may be highly sensitive; if leaked or tampered with, it could adversely affect rescue operations. Security is therefore also a basic functional requirement of emergency communication systems.

(4) **Interoperability.** Major disasters rarely involve only a single agency. A highly destructive earthquake, for example, often requires coordinated response from fire and rescue, public security, armed police, medical emergency services, emergency management authorities, and even international rescue teams; cross-border disaster relief further involves interconnection between different countries' systems. Interoperability is therefore one of the basic requirements of emergency communication systems, and the factors affecting it span spectrum, technology, networks, standards, planning, and available resources.

(5) **Rapid deployability.** Emergency communication systems sometimes

need to be fully deployed within hours of a disaster occurring, a requirement that must be fully accounted for at the design stage.

(6) **Spectrum priority and efficient management.** Radio spectrum is a non-renewable public resource. When a disaster strikes, a large number of rescue agencies, volunteers, and members of the public converge on the same area, and competition for radio spectrum becomes extremely intense. Emergency command organizations should make maximum use of harmonized frequency ranges to gain the benefits of interoperability, economies of scale, and equipment compatibility.

Table 3 compares emergency communication with conventional commercial communication across several dimensions; emergency communication exceeds the requirements of conventional communication on core indicators such as reliability, security, priority, and coverage.

Table 3. System Comparison Between Emergency Communication and Conventional Commercial Communication

Dimension	Emergency Communication	Conventional Commercial Communication
Primary design goal	Mission accomplishment and personnel safety; system failure is unacceptable	Service quality and user experience; a certain probability of service degradation is acceptable
Core user base	Authorized first responders, emergency management agencies, rescue organizations	General public, enterprise users
Network architecture	Dedicated network or shared network with priority access; must support localized communication	Commercial network; optimized for dense population coverage and spectral efficiency
Coverage design	Disaster-prone and disaster-frequent areas	Designed by population density and business demand; remote areas may go uncovered

Dimension	Emergency Communication	Conventional Commercial Communication
Priority mechanism	Supports priority access and preemption; emergency communication users have the highest priority	Usually no differentiated priority, or only QoS-level differentiation
Availability target	99.999% or higher	99.9%–99.99%
Security mechanism	End-to-end encryption; two-way device/user authentication; key management, etc.	Mainly transport-layer encryption (TLS/DTLS); end-to-end encryption optional
Terminal requirements	Drop/water/dust resistant; intrinsically safe (explosion-proof) certification; ultra-long battery life	Consumer-electronics grade; prioritizes slim, attractive design; lower protection rating
Group call / dispatch	Supports PTT; supports emergency preemption and forced disconnection	Primarily individual calls, with group calling as a supplementary feature
Direct mode	Supports DMO/D2D, enabling communication even without infrastructure	Typically not supported
Operating entity	Government agency or a licensed dedicated-network operator	Commercial market operator
Cost orientation	Trades cost for reliability; invests extra resources for extreme scenarios	Cost-efficiency driven; lowers per-unit cost through economies of scale

Commercial networks mainly focus on meeting everyday communication demand under normal operating conditions, but in extreme scenarios such as disasters and accidents that require communication support, they often struggle to sustain rescue operations because of network congestion, damaged infrastructure, or inadequate security capability – this is precisely why emergency communication exists as an independent communication system. Compared with commercial communication networks, whose core objectives are service capacity and economic return, emergency communication places

greater emphasis on sustained availability, reliability, and rapid deployability under extreme conditions; its core mission is to continue providing stable, reliable information transmission support for emergency command, rescue, and coordinated response at the moment when communication is "most difficult, most critical, and most needed." At the technical level, however, emergency communication is not entirely independent of the commercial communication ecosystem – it in fact draws heavily on it. Whether cellular mobile communication, IP network architectures, cloud computing, satellite internet, or broadband multimedia technology, the underlying technology evolution of emergency communication keeps pace with that of commercial communication. The main difference is that emergency communication places greater emphasis on enhancing network reliability, resilience, low latency, and priority assurance, using mechanisms such as redundant design, dedicated spectrum, mission priority control, and rapid mobile deployment to adapt commercial technologies to mission-critical needs under extreme conditions.

1.2 Classification of Emergency Communication

Emergency communication covers an extremely wide range of scenarios, and different scenarios impose very different requirements on communication-system design. Establishing a systematic classification framework is therefore a prerequisite for understanding the technical system of emergency communication. This section classifies emergency communication along three dimensions: the type of user involved in the communication, the network solution relied upon, and the temporal evolution of the emergency.

1.2.1 Classification by User Type

The first classification dimension for emergency communication is the identity of the parties to the communication. Drawing on standards frameworks such as ITU-T Y.2205 and combining them with the organizational form of actual emergency response, emergency communication can be divided by user type into four categories.

1. Person-to-Authority (P2A)

P2A emergency communication refers to communication initiated by members of the public (individual users) toward a government agency or authorized organization with emergency-response functions; its core function is "calling

for help" and "reporting." This is the most direct way the public engages with the emergency communication system, and it is also the first link that triggers the entire emergency-response chain. Typical P2A scenarios include:

1) Emergency call-for-help: dialing emergency numbers such as 110 (police), 119 (fire), or 120 (medical emergency) – the most traditional and fundamental form of P2A communication;
2) Text-message alerting: for people seeking help under limited network conditions or in noisy environments, such as BeiDou short-message service or Tiantong satellite short messages;
3) Emergency-app reporting: submitting disaster information, location, and photos in real time through mobile applications developed by government agencies or authorized organizations;
4) Location sharing: some enhanced emergency-call services can automatically transmit the caller's location information to the command center.

The technical focus of P2A communication is reachability: the public must be able to reach the emergency number from any location and under any network condition (including a suspended account or a weak signal), and, when necessary, the precise location of the person seeking help must also be reported.

2. Person-to-Person (P2P)

P2P emergency communication refers to communication between individual users during an emergency, including mutual assistance and coordination among affected members of the public, coordination among volunteers, and informal communication among first responders on the ground. Unlike formal command communication between institutions, P2P communication is spontaneous and decentralized in character. Typical P2P scenarios include:

1) Commercial public-network calls/text messages: in the early stages of a disaster, the public's most natural choice is to make phone calls or send text messages to check on each other's safety and coordinate evacuation;
2) Social media and instant-messaging apps: platforms such as WeChat and Weibo become important P2P channels for information dissemination during disasters, offering the advantages of fast propagation and broad coverage, though the authenticity of information can be difficult to verify;

3) Amateur radio: when public networks fail, licensed amateur-radio operators can use HF/VHF/UHF bands to provide P2P communication and relay services – an important supplementary capability in extreme scenarios.

The main technical challenge for P2P communication is network congestion. After a disaster, large numbers of members of the public simultaneously make calls or send messages, causing severe overload of public networks. In the 2011 Great East Japan Earthquake, for example, call volume on Japan's mobile networks surged to more than 50 times normal levels within hours of the quake, causing many calls to fail to connect.

3. Authority-to-Authority (A2A)

A2A refers to command-and-dispatch communication between different emergency-management agencies (such as between an industry sector and local government, or between local government and national rescue forces) for the purpose of coordinating rescue operations. A2A communication is mainly implemented through two categories of system: first, narrowband dedicated digital trunking systems based on standards such as PDT and TETRA, which provide mature and reliable voice dispatch; and second, the rapidly developing broadband mission-critical communication systems based on 3GPP's Mission Critical Services (MCX) standards, which provide integrated dispatch of voice, video, and data over LTE/5G networks.

4. Authority-to-Person (A2P)

A2P emergency communication is the means by which government or authorized agencies broadcast urgent warnings, evacuation instructions, and rescue information to the public on a large scale. A2P communication is typically characterized by "one-to-many broadcasting," with the core objective of delivering accurate information to everyone in the affected area in the shortest possible time. Typical A2P scenarios include:

1) TV/radio interrupt broadcasts: traditional media's emergency interrupt broadcasts, which reach the population without mobile phones and carry strong authority;
2) Push notifications: pushing warnings over the internet to users who have installed a particular app, with coverage not limited by cell boundaries but dependent on users being online and having the app installed;

3) Outdoor broadcast systems: suitable for power outages or network disruptions, covering areas at the community level;
4) Cell broadcast: broadcasting warning messages to all terminals within a specific geographic area via mobile-network base stations, without requiring user subscription. The 2024 "Opinions of the Ministry of Industry and Information Technology and 13 Other Departments on Strengthening Emergency Communication Capability Building for Extreme Scenarios" explicitly calls for strengthening the dissemination of communication-network early-warning information based on cell broadcast technology, interfacing with the national emergency early-warning information release system, and achieving second-level, targeted, and secure release of early-warning information.

1.2.2 Classification by Network Type

The second classification dimension for emergency communication is the ownership and architectural form of the network infrastructure relied upon, which can be grouped into three broad categories: public-network solutions, dedicated-network solutions, and hybrid public/dedicated solutions. These solutions differ in control, reliability, cost, and coverage.

1. Public-Network Solutions

A public-network solution means that the emergency command organization relies entirely on a mobile operator's public mobile communication network to provide emergency communication support, without building a separate dedicated network. Under this model, emergency communication users are typically served as ordinary public-network subscribers, or they gain access and resource assurance that exceeds that of ordinary public users through a priority-control mechanism.

The main advantages of public-network solutions are:

1) Broad coverage and low construction cost: commercial operators' networks already cover the vast majority of populated areas, so the emergency command organization does not need to bear construction costs;
2) Synchronized technology evolution: the ability to directly inherit the technological evolution of public mobile communication networks, quickly benefiting from network-capability improvements brought by 6G,

low-earth-orbit satellite communication, cloud computing, and artificial intelligence, without needing to undertake large-scale dedicated-system upgrades and infrastructure construction on its own;
3) Rich terminal ecosystem: commercial smartphones, tablets, and in-vehicle terminals can all be used directly, without the need to procure dedicated equipment.

However, public-network solutions face several fundamental limitations that make it difficult for them to independently bear mission-critical communication:

1) Risk of network congestion: when a disaster occurs, large numbers of members of the public flood onto the network at once, and commercial networks are prone to overload; even with priority preemption configured, it is difficult to fully guarantee access for emergency communication users;
2) Infrastructure vulnerability: severe earthquakes, floods, and other disasters often damage base-station power supplies and backhaul links, and commercial base stations are typically equipped with only a few hours of backup battery, giving them far lower resilience than dedicated networks;
3) Security and control: commercial operators cannot meet emergency communication's special security-control requirements, such as end-to-end encryption, dynamic frequency reconfiguration, and priority forced preemption;
4) Coverage gaps: commercial networks are designed on a population-density basis, and remote areas, tunnels, and underground spaces may have coverage gaps — precisely the areas where disaster rescue frequently occurs.

2. Dedicated Network Solutions

A dedicated-network solution means building a dedicated communication network, with independent spectrum and infrastructure, specifically for the emergency command organization, without sharing resources with commercial users. Dedicated-network solutions are currently the mainstream choice of most core public-safety agencies and some vertical-industry users worldwide, with notable advantages including:

1) Full control: the emergency command organization can independently determine coverage, frequency planning, priority policy, and security configuration, unconstrained by a commercial operator's business logic;
2) High resilience: dedicated-network base stations are typically equipped with sufficient backup power, reinforced enclosures, and multi-path backhaul, giving them far greater survivability than commercial base stations;
3) Support for mission-critical features: dedicated networks typically support direct mode, dynamic frequency reconfiguration, end-to-end encryption, and key management, among other features;
4) Coverage designed on demand: coverage targets are determined by rescue needs, allowing targeted coverage of remote areas, tunnels, underground spaces, and other commercial-network blind spots.

The main challenge for dedicated-network solutions is the high cost of construction and operation; the economies of scale for dedicated-network equipment are far weaker than for commercial equipment, resulting in a higher per-unit cost.

3. Public-Private Hybrid Solutions

Hybrid public/dedicated solutions combine the high reliability of dedicated networks with the broad coverage and low cost of commercial networks, achieving complementary capabilities through technical integration – one of the important development directions in emergency communication worldwide today. Typical implementation paths include:

1) Network slicing: under 5G Standalone (SA) architecture, an operator can allocate a dedicated network slice for emergency-communication services, providing relatively independent QoS assurance, security policy, and service priority while sharing the same physical infrastructure.
2) MCX over LTE/5G public networks: deploying a mission-critical service platform on a commercial LTE/5G network, where emergency-communication terminals access via public-network base stations, but at the service layer retain dedicated-network characteristics such as Push-to-Talk (PTT) group calling, priority preemption, and end-to-end encryption.
3) Space-air-ground integrated platforms: integrating terrestrial dedicated networks, public mobile communication networks, satellite communication, and other access methods, achieving cross-network coordination

and link switching through a unified dispatch platform, and improving communication-support resilience in complex disaster scenarios.

4) Coordinated multi-mode terminal access: emergency-communication terminals simultaneously support dedicated-network, public-network, and satellite communication standards, with network selection controlled manually or by policy depending on the coverage environment, thereby improving the continuity and adaptability of on-site communication.

Hybrid public/dedicated solutions trade a limited dedicated-network investment for reliable assurance of core capability, while leveraging the scale effects of the commercial ecosystem to lower total cost of ownership.

1.2.3 Classification by the Evolution of the Incident

The third classification dimension for emergency communication is the stage of an emergency's evolution along the time axis. The widely adopted "four-phase model" of disaster management, treats disaster management as a cyclical, continuous process comprising four core phases: mitigation, preparedness, response, and recovery. Emergency communication can accordingly be divided into three categories: emergency communication before an incident occurs, emergency communication after an incident occurs, and emergency communication during the recovery and reconstruction phase.

1. Emergency Communication Before an Incident Occurs

Before an emergency occurs, the public communication network remains fully intact and there is no issue of damaged infrastructure. Demand for emergency communication during this phase mainly falls into three areas: continuous monitoring and early warning of major potential emergencies; day-to-day response to emergencies that recur frequently within a region; and communication support for large-scale events and emergency drills.

The communication system used to support the monitoring and early warning of major emergencies is, in essence, a dedicated data-communication network, whose traffic mainly consists of a large volume of upstream monitoring data supplemented by necessary two-way voice and video traffic; this network should be capable of immediately switching over to support emergency command and control once an incident occurs.

The communication system used to support day-to-day response to regionally recurring emergencies is typified by urban emergency-linkage systems and industry-specific emergency communication systems, whose core

functions are alarm reporting and dispatch. On the reporting side, this relies on public communication networks or industry-dedicated networks feeding into a unified alarm-receiving platform; on the dispatch side, on-site dispatch relies on either public or dedicated networks, while internal command and office coordination rely on local-area networks and business systems. This is the routine law-enforcement and service communication carried out by public agencies or industry-management departments under normal working conditions, providing integrated voice, data, and location communication services for routine tasks such as patrols and law-enforcement dispatch.

Communication for large-scale events and emergency drills is a planned, high-load communication-support scenario, mainly used to support major public events, emergency drills, and cross-regional coordinated training. Traffic peaks for such scenarios are typically predictable, allowing for advance frequency-resource coordination, capacity assessment, and support planning, and allowing capacity expansion and coverage enhancement of key areas through the rapid deployment of temporary infrastructure such as temporary base stations, emergency communication vehicles, and portable broadband systems, so as to meet high-concurrency communication demand during the event.

2. Emergency Communication After an Incident Occurs

After an emergency occurs, fixed communication infrastructure may be wholly or partially damaged, and public communication networks may also lose service capability due to equipment failure, power interruption, or traffic congestion; at this point, various rescue operations become highly dependent on the emergency communication system for support. This phase is where the emergency-communication technology system faces its most concentrated challenges, and it is also the primary application background for the various technical approaches covered later in this book. At the disaster site, a multi-layered communication system covering command organizations, rescue forces, on-site support, and the affected public must be built to support command and dispatch, coordinated operations, information gathering, and public liaison.

(1) **Command-layer communication systems.** Used to support on-site command at the disaster area and cross-regional coordination, this is the core communication hub of the entire rescue operation, carrying voice, video, data, conferencing, and image transmission across multiple services, and maintaining external liaison between the disaster area and higher-level com-

mand organizations. Its typical architecture usually uses HF, VHF/UHF, or trunked radio to support internal communication within the disaster area, and satellite communication, microwave links, or surviving public-network links to achieve long-range backhaul, with emphasis on high reliability, high security, high mobility, and rapid deployability. Typically, a unified on-site emergency command center is set up for a disaster area, with a relatively complete command communication network deployed around it.

(2) **On-site internal communication.** Used to support communication coordination within each rescue team and among different working groups on the ground, this places high demands on the portability, mobility, and environmental adaptability of terminal equipment, typically relying mainly on handheld radios, portable trunking systems, or single-base-station broadband dedicated-network systems to cover a limited on-site working area. When multiple rescue forces enter the disaster area at the same time, differences in the frequency bands, standards, and equipment systems used by different departments often make cross-system interoperability a prominent problem in on-site communication support.

(3) **On-site video and television relay systems.** Responsible for the real-time capture and backhaul of disaster imagery, on-site video, and key-area situational information, providing an intuitive on-site perception capability for the remote command center. Traditional approaches mostly use lightweight satellite TV relay vehicles or portable satellite image-transmission systems, balancing image quality with rapid deployability and mobility. With the development of LTE/5G broadband communication technology, video backpacks, aggregated-transmission terminals, and drone-based real-time image transmission systems are gradually becoming an important supplement to satellite relay.

(4) **On-site emergency communication technical-support systems.** Mainly used to resolve interoperability problems between systems using different frequencies and different standards, bringing the communication equipment carried by different departments and rescue forces into a unified interoperable communication system. Typical implementations include vehicle-mounted mobile communication-support platforms, integrated-communication gateways, and software-defined radio systems, which can enable voice dispatch, cross-network interconnection, and unified access management.

(5) **Self-rescue and distress communication for the affected public.** This category covers the most diverse range of communication means, with the core

objective of enabling trapped members of the public to send distress signals and enabling rescue personnel to quickly obtain their location and status information. Available communication methods include surviving cellular networks, satellite terminals, amateur radio, VoIP systems, portable temporary base stations, drone relays, and positioning tags, among other available facilities and technologies.

(6) **Temporary public communication systems for the affected public.** Mainly used to meet the public's needs for reporting their safety, obtaining rescue information, and maintaining basic social contact, with relatively low requirements for communication quality but usually significant capacity demand. When the public network has not yet completely failed, surviving public-network resources can be prioritized for use; where infrastructure damage is severe, temporary public communication services are typically provided through facilities such as emergency communication vehicles, vehicle-mounted mobile base stations, portable base stations, and satellite backhaul links.

Taken together, these six categories of system reveal three common engineering characteristics of post-incident emergency communication. First, a pronounced supply-demand mismatch: rescue-communication demand rises sharply in a short period, while the supply capability of fixed communication infrastructure drops sharply due to disaster damage; rapidly deploying mobile communication systems is therefore the fundamental way to restore communication capability. Second, prominent needs for concurrent multi-system operation and cross-system interoperability: command, rescue, video-backhaul, and public communication systems of various types often run simultaneously in the same disaster area, and differences in frequency bands, standards, and equipment systems between departments become a key bottleneck constraining overall communication effectiveness — making technical-support systems based on software-defined radio and integrated-communication gateways an indispensable intermediate layer. Third, priority on mobility: all types of systems emphasize being lightweight, rapidly deployable, and simple to operate, so as to adapt to the complex environment and rapid-deployment demands of a disaster area.

3. Emergency Communication During the Recovery Phase

Once emergency rescue is complete, incident response gradually enters the recovery and reconstruction phase. Compared with the initial disaster and peak-rescue phases, the communication system during this phase is char-

acterized by public-network dominance with emergency-network support, and communication pressure and organizational complexity both decrease markedly.

In terms of infrastructure recovery, the public communication network has generally resumed operation and can handle most communication demand during the recovery phase; various monitoring and early-warning systems, regional linkage systems, and communication platforms gradually return to normal operating mode as well. Because some on-site rescue and secondary-disaster response work may still be ongoing in the early part of this phase, some outside support forces and emergency communication systems continue to operate, but their role shifts to a supporting one. At the same time, command and management authority over the emergency communication system is gradually transferred from the temporary emergency-command structure back to the routine responsible department.

This process reflects an important design goal of the emergency communication system: to shorten, as much as possible within limited resources, the duration of high-intensity emergency support, promoting a rapid return of communication capability to normal operation, thereby freeing up mobile communication resources and preserving support capability for future emergencies. Another important task of the recovery phase is a systematic review and assessment of the communication-support effort just carried out — a comprehensive analysis of emergency communication support effectiveness, network coverage, system interoperability, command processes, and resource dispatch is needed, with particular focus on identifying coverage gaps, insufficient heterogeneous-system interoperability, redundant command layers, and equipment-deployment efficiency issues, forming targeted recommendations for improvement to feed into subsequent plan revisions and system development.

1.3 Emergency Communication Standards System

The formation of the emergency communication standards system is the concentrated product of decades of major disasters and emergencies driving the evolution of communication technology. The 1995 Great Hanshin earthquake in Japan, the 2004 Indian Ocean tsunami, and Hurricane Katrina in 2005 — each major event has profoundly exposed the vulnerabilities of existing communication systems in disaster scenarios, in turn prompting standards bodies to place

emergency communication on their agendas and forming a well-structured, interconnected system of international and national standards.

Structurally, current emergency communication standards can be divided into three layers: first, international framework standards represented by the ITU, which define terminology, allocate spectrum, and specify network capability requirements, providing a reference for national standards; second, regional and industry technical standards represented by ETSI/CEPT in Europe and TIA/APCO in the United States, which translate framework-level requirements into quantifiable, testable engineering specifications; and third, national standards represented by the China Communications Standards Association and Japan's ARIB/TTC, which adapt international technical achievements to national disaster characteristics and management systems. 3GPP and IETF, as the core technical standards organizations in the communication field, provide a common protocol foundation for broadband mobile emergency communication and internet-based emergency services, and their outputs are also widely referenced.

1.3.1 International Telecommunication Union

ITU-R, ITU-T, and ITU-D jointly build the top-level framework of international emergency communication standards along three dimensions: spectrum, network, and development assistance. Their standards output takes the form mainly of "Recommendations," "Reports," and "Questions."

1. ITU-R: Spectrum Coordination and PPDR Technical Requirements

ITU-R's emergency communication work centers on the PPDR framework, and its standardization output spans spectrum planning, technical requirements, and application specifications, forming to date a systematic body of documents. The main technical standards relevant to emergency communication are shown in Table 4.

Table 4. ITU-R Documents Related to Emergency Communication

No.	Title	Standard/Document No.
1	Broadcasting means for public warning, disaster mitigation and relief	Question 118-1/6
2	Use of the mobile, amateur and the amateur-satellite services in support of disaster radiocommunications	Question 209-7/5
3	Technical and operational characteristics for systems in the fixed service used for disaster mitigation and relief	Question 248/5
4	Broadcasting-satellite means for public warning, disaster mitigation and relief	Question 290/4
5	Use of satellite and terrestrial broadcast infrastructures for public warning, disaster mitigation and relief	BO.1774/BT.1774
6	Use of International Radio for Disaster Relief frequencies for emergency broadcasts in the High Frequency bands	BS.2107
7	Broadcasting for public warning, disaster mitigation and relief	Report BT.2299
8	Fixed wireless systems for disaster mitigation and relief operations	Recommendation F.1105
9	HF fixed radiocommunications systems	Report F.2061

No.	Title	Standard/Document No.
10	Requirements for high frequency (HF) radiocommunication systems in the fixed service	Report F.2087
11	Disaster communications in the amateur and amateur-satellite services	Recommendation M.1042
12	Global cross-border circulation of radiocommunication equipment for use in emergency and disaster relief situations	Recommendation M.1637
13	Harmonized frequency channel plan for broadband public protection and disaster relief operations at 4 940-4 990 MHz in Regions 2 and 3	Recommendation M.1826
14	Use of mobile-satellite service in disaster response and relief	Recommendation M.1854
15	Radio interface standards for use by public protection and disaster relief operations in accordance with Resolution 646 (Rev.WRC-15)	Recommendation M.2009
16	Frequency arrangements for public protection and disaster relief radiocommunication systems in accordance with Resolution 646 (Rev.WRC-15)	Recommendation M.2015

No.	Title	Standard/Document No.
17	Radiocommunication objectives and requirements for public protection and disaster relief	Report M.2033
18	Role of the amateur and amateur-satellite services in support of disaster mitigation and relief	Report M.2085
19	Use and examples of mobile-satellite service systems for relief operation in the event of natural disasters and similar emergencies	Report M.2149
20	Use of International Mobile Telecommunications for broadband public protection and disaster relief applications	Report M.2291
21	Radiocommunication objectives and requirements for public protection and disaster relief	Report M.2377
22	Spectrum aspects for public protection and disaster relief	Report M.2415
23	Managed by SG05. Emerging usage of the terrestrial component of International Mobile Telecommunication (IMT)	Report M.2441
24	ITU-R studies of disaster prediction, detection, mitigation and relief	Resolution 55-4
25	Public protection and disaster relief (PPDR)	Resolution 646 (Rev.WRC-19)

No.	Title	Standard/Document No.
26	Radiocommunication aspects, including spectrum-management guidelines, for early warning, disaster prediction, detection, mitigation and	
relief operations relating to emergencies and disasters	Resolution 647 (Rev.WRC-19)	
27	Use of remote sensing systems for data collection to be used in the event of natural disasters and similar emergencies	Recommendation RS.1859
28	The essential role and global importance of radio spectrum use for Earth observations and for related applications	Report RS.2178
29	Use of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations	Recommendation S.1001
30	Use and examples of systems in the fixed-satellite service in the event of natural disasters and similar emergencies for warning and relief operations	Report S.2151

On spectrum coordination, Resolution 646 (Rev.WRC-19) is the most authoritative policy document in the PPDR field, requiring administrations to use harmonized frequency bands as far as possible when developing PPDR

frequency plans, so as to promote cross-border interoperability and economies of scale in equipment. ITU-R M.2015 further specifies UHF-band frequency arrangements for PPDR systems, providing a technical reference for national regulators' frequency allocation, while M.1826 sets out a coordinated channel plan for broadband PPDR operation in the 4 940–4 990 MHz band, now applied in both the Asia-Pacific (Region 3) and the Americas (Region 2).

On technical requirements, M.2033 was the earliest systematic requirements document in the PPDR field, the first to give a complete description, from a radiocommunication perspective, of the technical objectives and usage requirements of public protection and disaster relief; it distinguished three categories of operational scenario – day-to-day operations (PP1), major planned/public events (PP2), and disaster relief (DR) – establishing the analytical framework for subsequent PPDR standardization work. Building on it through continuous revision, M.2377-2 now represents the highest level of PPDR technical-requirements standardization: it comprehensively covers narrowband, wideband, and broadband implementation paths, systematically summarizes 17 technical and functional objectives (including multimedia capability, end-to-end encryption, and direct mode), 12 operational objectives, and the full range of operational requirements – priority access, Quality of Service (QoS) grading, reliability, coverage and capacity, interoperability, and security – and it is the most widely cited international document in global PPDR system research and engineering practice. M.2291-1 specifically evaluates the capability of 3GPP LTE/LTE-Advanced systems to support broadband PPDR applications, making the case for introducing commercial IMT technology into public-safety communication and providing standards support for subsequent choices of technical route for national broadband public-safety networks.

On application specifications, BT.1774 sets out the technical framework for using satellite and terrestrial broadcasting infrastructure for public warning, disaster mitigation, and relief, clarifying the technical role of broadcast systems in emergency warning and the associated interface requirements. The F.1105 series specifically sets technical specifications for transportable fixed wireless communication equipment (including satellite stations and mobile base stations) used in disaster relief operations, addressing transportability, rapid deployability, and electromagnetic-compatibility requirements. The M.1042 series focuses on the use of the amateur radio service in disaster communication, emphasizing the value of the amateur-radio community as a supplementary means of communication when public networks fail, while also specifying methods of coordination with professional emergency agencies

under national emergency-plan frameworks.

2. ITU-T: Service Framework and Network Capability Standards

ITU-T's research on emergency communication mainly focuses on emergency-service capability built on public telecommunication networks, with an emphasis on how fixed networks, mobile networks, Next Generation Networks (NGN), the IP Multimedia Subsystem (IMS), IP networks, and future networks can provide reliable information transmission and service assurance to governments, rescue agencies, and the public during disasters, accidents, and public crises. Unlike ITU-R, which focuses on radio spectrum and emergency wireless systems, ITU-T is more concerned with network architecture, service capability, protocol mechanisms, QoS/Quality of Experience (QoE), priority control, and cross-network interoperability. A fairly complete technical system has formed around emergency communication, public warning, disaster-relief communication, NGN/IMS emergency services, and network resilience. The main technical standards relevant to emergency communication are shown in Table 5.

Table 5. ITU-T Documents Related to Emergency Communication

No.	Title	Standard No.
1	Framework of disaster management for disaster relief system	E.100SerSup1
2	International Emergency Preference Scheme (IEPS) for disaster relief operations	E.106
3	Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS	E.107
4	Requirement for disaster relief mobile message service	E.108
5	Requirements for safety confirmation and broadcast message service for disaster relief	E.119
6	Notation for national and international telephone numbers, e-mail addresses and web addresses: Contact information in case of emergency for mobile telephones	E.123 Amendment 1

No.	Title	Standard No.
7	Guidelines to select Emergency Number for public telecommunications networks	E.161.1
8	Guidance with regard to the selection of numbers for helplines for children	E.164 Suppl. 5
9	Framework and requirements for emergency services using civilian unmanned aerial vehicles	F.749.18
10	Requirements and reference framework for emergency rescue systems	F.760.1
11	Guidelines for user interface of first responders in emergency response support systems	F.760.2
12	Metadata for disaster information presentation with human factors	F.760.3
13	Gateway control protocol: Multi-level precedence and pre-emption package	H.248.44
14	Gateway control protocol: Guidelines on the use of the International Emergency Preference Scheme (IEPS) call indicator and priority indicator in ITU-T H.248 profiles	H.248.81
15	Tunnelling of Common Alerting Protocol (CAP) messages in H.323	H.323 Annex M5
16	Call priority designation and country/international network of call origination identification for H.323 priority calls	H.460.4
17	Support for Multi-Level Precedence and Preemption (MLPP) within H.323 systems	H.460.14
18	Message broadcast for H.323 systems	H.460.21
19	Digital signage: Requirements of disaster information services	H.785.0

No.	Title	Standard No.
20	Gateway control protocol: Operation of H.248 with H.225.0, SIP, and ISUP in support of Emergency Telecommunications Service (ETS)/International Emergency Preference Scheme (IEPS)	H.Sup9
21	Gateway control protocol: Priority traffic treatment by ITU-T H.248 gateways	H.Sup12
22	Requirements for preferential telecommunications over IPCablecom networks	J.260
23	Framework for implementing preferential telecommunications in IPCablecom and IPCablecom2 networks	J.261
24	Specifications for authentication in preferential telecommunications over IPCablecom2 networks	J.262
25	Specification for priority in preferential telecommunications over IPCablecom2 networks	J.263
26	Disaster management for improving network resilience and recovery with movable and deployable ICT resource units	L.392
27	Framework of disaster management for network resilience and recovery	L.Sup35
28	Disaster management for outside plant facilities	L.390
29	Disaster management for improving network resilience and recovery with movable and deployable ICT resource units	L.392

No.	Title	Standard No.
30	TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)	M.3350
31	Speech communication requirements for emergency calls originating from vehicles	P.1140
32	Signalling architecture of fast deployment emergency telecommunication networks to be used in a natural disaster	Q.3060
33	Signalling requirements for emergency services in an IP Multimedia Subsystem roaming environment	Q.3647
34	Emergency services for IMT-2000 networks – Requirements for harmonization and convergence	Q.Sup47
35	Signalling requirements to support the International Emergency Preference Scheme (IEPS)	Q.Sup53
36	Signalling requirements to support the emergency telecommunications service (ETS) in IP networks	Q.Sup57
37	Evaluation of signalling protocols to support ITU-T Y.2171 admission control priority levels	Q.Sup61
38	Overview of the work of standards development organizations and other organizations on the emergency telecommunications service	Q.Sup62
39	Signalling protocol mappings in support of the Emergency Telecommunications Service in IP networks	Q.Sup63

No.	Title	Standard No.
40	Technical Report on emergency telecommunication service (ETS) interoperability limitations	Q.Sup68
41	Framework for interconnection between VoLTE-based networks and other networks supporting emergency call	Q.Sup69
42	Signalling requirements for IMS and GSM/UMTS network supporting multi-device emergency telecommunications service	Q.Sup70
43	Signalling requirements for IP multimedia subsystem (IMS) emergency call in support of multiple acces	Q.Sup72
44	Common alerting protocol (CAP 1.1)	X.1303
45	Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks	Y.1271
46	Requirements for Internet of things devices and operation of Internet of things applications during disasters	Y.2074
47	Admission control priority levels in Next Generation Networks	Y.2171
48	Service restoration priority levels in Next Generation Networks	Y.2172
49	Next Generation Networks - Emergency telecommunications - Technical considerations	Y.2205
50	Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)	Y.2705
51	Requirements for Internet of things devices and operation of Internet of things applications during disasters	Y.4102

No.	Title	Standard No.
52	Requirements and capability framework for IoT-based automotive emergency response system	Y.4119
53	Framework of smart evacuation in a disaster or emergency in smart cities and communities	Y.4222
54	Functional framework and requirements for disaster monitoring systems	Y.4226
55	Information and communication technology implementation framework for smart public health emergency management in smart and sustainable cities	Y.4233
56	Minimum set of data structure for automotive emergency response system	Y.4467
57	Minimum set of data transfer protocol for automotive emergency response system	Y.4468
58	Requirements and reference architecture for a smart public health emergency information system	Y.4496
59	Metadata model of sensing capability for disaster monitoring systems	Y.4705
60	ITU-T Y.2200-series - Supplement on the risk analysis service in next generation networks	Y.Sup19
61	Signalling in support of IEPS in ISUP	Q.761 Amd.3, Q.762 Amd.3, Q.763 Amd.4, Q.764 Amd.4
62	Signalling in support of IEPS in BICC	Q.1902.1 Amd.2, Q.1902.2 Amd.3, Q.1902.3 Amd.3, Q.1902.4 Amd.3
63	Signalling in support of IEPS in ATM AAL2 / CBC	Q.1950 Amd.1 Annex G; Q.2630.3 Amd.1
64	Signalling in support of IEPS in B-ISUP	Q.2762 Amd.1, Q.2763 Amd.1, Q.2764 Amd.1
65	Signalling in support of IEPS in DSS2	Q.2931 Amd.5

ITU-T E.106 defines the International Emergency Preference Scheme (IEPS) and is a foundational document in the ITU-T emergency communication standards system. This Recommendation sets out the core mechanism of IEPS: when international circuits suffer reduced capacity, congestion, or service interruption due to a disaster, IEPS users authorized by a national administration can obtain privileged services such as priority dial tone, priority call setup (including priority queuing), and exemption from restrictive network controls (such as call-gapping), thereby ensuring that key disaster-relief communication personnel remain reachable even when communication resources are severely scarce. E.107 builds on E.106 to further establish a national implementation framework and international interconnection mechanism for Emergency Telecommunications Service (ETS). This Recommendation defines ETS as a national-level priority communication service realized over a national public communication network, used to provide authorized users with priority telecommunication service during disasters and emergencies – distinguishing it from IEPS's international-level application. E.107 was the first to introduce the concept of "preferential treatment capability" – the ability to give a particular communication a higher probability of success in network resource allocation and processing – laying the theoretical foundation for the priority scheduling, resource preemption, and service-assurance mechanisms in later emergency communication systems. E.107 also specifies bilateral and multilateral interconnection frameworks, enabling interconnection between countries' national ETS implementations and thereby supporting priority telecommunication service in cross-border disaster relief.

ITU-T Y.1271 is one of the most representative comprehensive emergency communication framework standards in the ITU-T system, and also one of the most widely cited emergency communication Recommendations. It was developed against the backdrop of the profound evolution of public communication networks from traditional circuit switching toward packet switching (IP-based) architectures: traditional circuit-switched networks respond to network overload mainly through "call blocking," while the "best-effort" transmission model of packet-switched networks cannot inherently guarantee priority for emergency communication, making new priority-assurance mechanisms necessary. Y.1271 systematically sets out the basic requirements, key characteristics, and capability framework for emergency communication in both evolving circuit-switched and packet-switched networks, proposing 12 core capability elements. It also distinguishes the differentiated requirements for these capabilities across four communication directions: public-to-authority,

authority-to-authority, authority-to-public, and public-to-public. Y.2205 further extends Y.1271's research to NGN and IMS architectures, focusing on technical paths for achieving priority assurance for emergency communication in an all-IP network environment, including Session Initiation Protocol (SIP) priority-header processing, media-stream preemption mechanisms, and network overload control, providing an important theoretical basis for the subsequent development of 3GPP IMS emergency calling and MCX service specifications.

Y.2705 sets out minimum security requirements for ETS interconnection scenarios, covering signalling integrity protection, minimum security levels for user identity authentication, and key-management mechanisms, complementing the security-capability elements in Y.1271 and together forming the security foundation of the IP-based emergency communication system.

X.1303 specifies a language-independent public warning message format usable for cross-platform, cross-network, and cross-agency exchange of warning information; this protocol has been widely adopted, and is one of the core data-exchange standards for institution-to-public warning communication.

3. ITU-D: Development Assistance and National Planning Guidance

ITU-D is the sector of the ITU dedicated specifically to promoting sustainable social and economic development through information and communication technology (ICT). Unlike ITU-R and ITU-T, which focus mainly on technical-standards development and spectrum coordination, ITU-D places greater emphasis on translating relevant standards and technical capability into emergency communication systems that can actually be deployed and sustainably operated, especially in developing and least-developed countries, working to bridge the capability gap between standards development and engineering implementation. ITU-D therefore plays an important capacity-building and international-assistance role in the global emergency communication system.

ITU-D's work in the emergency communication field mainly spans three areas: disaster-response assistance, policy-planning advisory services, and training and capacity building. First, disaster-response assistance: after a major disaster, ITU-D helps affected countries formulate temporary telecommunication/ICT recovery plans and supports the rapid rebuilding of emergency communication capability. Second, policy-planning advisory services:

through platforms such as the World Telecommunication Development Conference, ITU-D encourages countries to incorporate emergency communication systems into their national ICT development strategies and disaster-risk-management frameworks, assists in developing national emergency communication plans, and helps improve related management mechanisms, spectrum policy, and cross-department coordination systems. Third, training and capacity building: ITU-D has long conducted capacity-building programs for government agencies, regulators, and emergency-management personnel in developing countries, aiming to improve local capability for planning, building, and operating emergency communication. The main research and projects relevant to emergency communication are shown in Table 6.

Table 6. ITU-D Documents Related to Emergency Communication

No.	Title	Year
1	Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations	1998
2	The use of telecommunications/ICTs for disaster risk reduction and management	2017
3	ITU Guidelines for national emergency telecommunication plans	2020
4	Developing a telecommunications/ ICT contingency plan for a pandemic response	2020
5	Utilizing telecommunications and ICTs for disaster risk reduction and management	2021
6	Digital transformation and early warning systems for saving lives	2023
7	Scaling Up Cell Broadcast for Last-mile Early Warning Delivery: Progress, barriers, and enabling mechanisms	2025

An important contribution of ITU-D was leading the development of the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations, whose core provisions require signatory states to reduce or remove regulatory barriers in disaster scenarios, allowing other countries' emergency communication equipment (including radio terminals and satellite stations) to enter and be used without obstruction, and providing entry facilitation for the associated operating personnel.

Another representative ITU-D achievement in emergency communication is the *ITU Guidelines for National Emergency Telecommunication Plans* (NETP), published in 2020 – a systematic planning toolkit compiled by ITU-D drawing

on practical experience from around the world, whose core value lies in integrating ITU-R's spectrum policy with ITU-T's network-capability framework into an operational planning methodology for national governments. The NETP guidelines propose that a complete national emergency communication plan should cover at least six dimensions: the legal and regulatory framework, institutional coordination mechanisms, technology-solution selection, spectrum management, emergency-communication operating procedures, and continuous capacity building. ITU-D has also produced a series of research reports and guidance documents targeting specific emergency communication scenarios.

1.3.2 European Standards System

A distinctive feature of the European emergency communication standardization system is the parallel operation of "technical specification development" and "legal and regulatory constraint": the European Telecommunications Standards Institute (ETSI) is responsible for developing systematic, engineering-oriented technical specifications, while EU legislative bodies convert relevant technical requirements into legally binding obligations for member states through regulations and directives, together forming a complete loop from standards development through industrial implementation to market deployment.

1. ETSI Technical Committee on Emergency Communications (TC EMTEL)

ETSI's dedicated Technical Committee for Emergency Communications (TC EMTEL) is the core body developing European emergency communication standards. Its work covers communication between individuals and authorities, between authorities and individuals, between authorities, and between individuals during emergencies. The main technical standards relevant to emergency communication are shown in Table 7.

Table 7. ETSI Documents Related to Emergency Communication

No.	Title	Standard No.
1	Emergency Communications (EMTEL); Test/verification procedure for emergency calls	ETSI SR 002 777
2	Emergency Communications (EMTEL); Basis of requirements for communication of individuals with authorities/organizations in case of distress (emergency call handling)	ETSI TR 102 180
3	Emergency Communications (EMTEL); Emergency Communications (EMTEL); Collection of European Regulatory Texts and orientations	ETSI TR 102 299
4	Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress	ETSI TR 102 410
5	Analysis of the Short Message Service (SMS) and Cell Broadcast Service (CBS) for Emergency Messaging applications; Emergency Messaging; SMS and CBS	ETSI TR 102 444
6	Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness	ETSI TR 102 445
7	Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities	ETSI TR 102 476
8	Emergency Communications (EMTEL); Analysis of Mobile Device Functionality for PWS	ETSI TR 102 850
9	Emergency Communications (EMTEL); Total Conversation for emergency communications; implementation guidelines	ETSI TR 103 201
10	Emergency Communications (EMTEL); Recommendations for public warning making use of pre-defined libraries	ETSI TR 103 273
11	Emergency Communications (EMTEL); Guidelines for alert message content accessibility	ETSI TR 103 335
12	Emergency Communications (EMTEL); Advanced Mobile Location for emergency calls	ETSI TR 103 393
13	EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations	ETSI TR 103 582

No.	Title	Standard No.
14	Emergency Communications (EMTEL); Main terms and definitions for Emergency Communications	ETSI TR 104 020
15	Emergency Communications (EMTEL); Total Conversation Access to Emergency Services	ETSI TS 101 470
16	Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies	ETSI TS 102 181
17	Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies	ETSI TS 102 182
18	Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service	ETSI TS 102 900
19	Emergency Communications (EMTEL); Pan-European Mobile Emergency Application	ETSI TS 103 478
20	Emergency Communications (EMTEL); Core elements for network independent access to emergency services	ETSI TS 103 479
21	Emergency Communications (EMTEL); Interoperability testing of core elements for network independent access to emergency services	ETSI TS 103 480
22	Emergency Communications (EMTEL); Transporting Handset Location to PSAPs for Emergency Communications - Advanced Mobile Location	ETSI TS 103 625
23	EMTEL; Testing - Conformance test specifications for core elements for network independent access to emergency services (NG112); Part 1: Protocol Implementation Conformance Statement (PICS), Test Suite Structure and Test Purposes (TSS & TP)	ETSI TS 103 650-1
24	EMTEL; Testing - Conformance test specifications for core elements for network independent access to emergency services (NG112); Part 2: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)	ETSI TS 103 650-2
25	Emergency Communications (EMTEL); Emergency Communications (EMTEL); Lightweight Messaging Protocol for Emergency Service Accessibility (LMPE)	ETSI TS 103 698
26	Emergency Communications (EMTEL); PEMEA ESInet Shared Services	ETSI TS 103 755

No.	Title	Standard No.
27	Emergency Communications (EMTEL); PEMEA Instant Message Extension	ETSI TS 103 756
28	Emergency Communications (EMTEL); Testing - Conformance test specifications for Advanced Mobile Location; Test Purposes (TP) for the handsets	ETSI TS 103 825
29	Emergency Communications (EMTEL); PEMEA Real-Time Text Extension	ETSI TS 103 871
30	Emergency Communications (EMTEL); PEMEA Service Discovery Extension	ETSI TS 103 872
31	Emergency Communications (EMTEL); Accessibility and interoperability of emergency communications and for the answering of emergency communications by the public safety answering points (PSAPs) (including to the single European Emergency number 112)	ETSI TS 103 919
32	Emergency Communications (EMTEL); PEMEA Audio Video Extension	ETSI TS 103 945
33	Emergency Communications (EMTEL); PEMEA File Exchange Extension	ETSI TS 104 014

TS 102 181 and TS 102 182 are the two foundational requirements specifications of ETSI TC EMTEL. TS 102 181 takes the perspective of public-protection and disaster-relief agencies, systematically analyzing the communication requirements of police, fire and rescue, and medical-emergency departments during an emergency – including cross-agency voice dispatch, multi-party consultation, secure data sharing, and real-time video transmission – along with quantitative requirements for latency, reliability, and information confidentiality. TS 102 182 instead addresses communication needs between government agencies and the public, focusing on the transmission characteristics of different warning-message categories such as “act-immediately” and “informational” messages, and setting requirements for geographic-coverage precision, message timeliness, multilingual support, and accessible access for people with disabilities – laying the requirements foundation for the later construction of European public-warning systems such as EU-Alert.

TS 102 900 is the core technical specification of the European public-warning system, defining the system requirements, message format, and network implementation mechanism for the European Public Warning System (EU-Alert) based on the Cell Broadcast Service (CBS). This standard selected

CBS as its carrier technology for three main reasons: first, CBS does not require establishing a point-to-point connection – a base station can broadcast directly to all terminals within its coverage area, so it retains high reachability even under network congestion; second, CBS offers strong geographic targeting capability, enabling warnings down to the cell or even sector level, and in the 5G era further supports finer-grained polygon-based area alerting; third, CBS is compatible with 2G through 5G mobile networks, covering the vast majority of existing mobile terminals. In view of Europe's large cross-border mobile population, TS 102 900 also specifies a language-code identification and priority mechanism for multilingual environments, to support roaming users in receiving localized disaster warnings.

TS 103 625 addresses the problem of location accuracy in mobile-terminal emergency calls. Inaccurate call location has long been an important factor constraining rescue-dispatch efficiency. The Advanced Mobile Location (AML) mechanism defined in this standard specifies that when a user dials an emergency number such as 112, the terminal automatically activates Global Navigation Satellite System and Wi-Fi positioning in the background, and sends the resulting high-precision location information to the Public Safety Answering Point via SMS or a data service, significantly improving the positioning accuracy and response efficiency of emergency rescue.

TS 103 479 defines the overall architecture and core interfaces for next-generation emergency communication, aiming to move Europe's 112 emergency-call system from a traditional Public Switched Telephone Network (PSTN) voice model toward a multi-modal IP communication system supporting voice, text, video, and data. This specification defines the interface specifications and functional requirements between the core nodes of the emergency communication network, with an emphasis on resolving cross-network interoperability for VoLTE/VoNR emergency calls, as well as emergency-call routing and addressing mechanisms in roaming scenarios. TS 103 479 is also coordinated with the relevant RFCs from the IETF ECRIT working group, reflecting the deep convergence of the European telecommunication-standards system and the internet-standards system in the field of IP-based emergency communication.

2. EU Emergency Communication Regulations

Article 110 of the European Electronic Communications Code (EECC – Directive (EU) 2018/1972) required member states to establish public-warning capability by 21 June 2022; where a public-warning system is available, operators

providing interpersonal communication services based on mobile numbers must send affected end-users public-warning information about imminent or ongoing major emergencies and disasters. This provision effectively established, in law, the mandatory deployment of mobile public-warning systems such as EU-Alert across Europe. The European Accessibility Act (EAA – Directive (EU) 2019/882) further requires that emergency communication services be accessible to users with disabilities, driving the standardization and engineering deployment of accessible emergency communication technologies such as real-time text and total conversation. By using law and regulation to enforce compliance with technical standards, the EU has enabled a complete loop from standards development to industrial deployment for its public-warning and next-generation emergency communication systems – an important feature distinguishing the European emergency communication system from those of other regions.

1.3.3 3rd Generation Partnership Project (3GPP)

3GPP's standardization work on emergency communication entered a systematic phase of development starting with Release 11. Before that, 3GPP's research on emergency services focused mainly on the single scenario of "emergency calling" – for example, TS 22.011 specified that a terminal should still support emergency-number calling even without a SIM card. Starting with Release 11, 3GPP began treating public safety and public-protection-and-disaster-relief as an independent vertical application domain for systematic design, gradually building a complete emergency communication standards system spanning radio access, the core network, service applications, security mechanisms, and terminal capability. Some of the main technical standards relevant to emergency communication are shown in Table 8.

Table 8. Selected 3GPP Standards Related to Emergency Communication

No.	Title	Standard No.
1	Service accessibility	TS 22.011
2	Service aspects; Service principles	TS 22.101
3	Earthquake and Tsunami Warning System (ETWS) requirements; Stage 1	TS 22.168
4	Mission Critical Push to Talk (MCPTT); Stage 1	TS 22.179
5	Public Warning System (PWS) requirements	TS 22.268
6	Mission Critical (MC) video	TS 22.281
7	Mission Critical (MC) data	TS 22.282
8	Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1	TS 22.346
9	Feasibility study for Proximity Services (ProSe)	TR 22.803
10	Study on non-voice emergency services	TR 22.871
11	Feasibility study on Mission Critical (MC) data communications	TR 22.880
12	Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety	TR 22.897
13	Transferring of emergency call data	TR 22.967
14	Study for requirements for a Public Warning System (PWS) service	TR 22.968
15	Feasibility study on enhancements of Public Warning System (PWS)	TR 22.969
16	Technical realization of Cell Broadcast Service (CBS)	TS 23.041
17	IP Multimedia Subsystem (IMS) emergency sessions	TS 23.167
18	Common functional architecture to support mission critical services; Stage 2	TS 23.280
19	Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2	TS 23.281
20	Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2	TS 23.282
21	Mission Critical Communication Interworking with Land Mobile Radio Systems	TS 23.283
22	Mission Critical services over 5G System; Stage 2	TS 23.289
23	Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2	TS 23.379
24	5G System; Multicast/Broadcast Service Transport Services; Stage 3	TS 29.518

The MCPTT (Mission Critical Push-to-Talk) standard introduced by 3GPP in Release 13 is a milestone in its public-safety and emergency communication standardization work. MCPTT solved a problem that had long constrained the use of LTE in public safety: although LTE offers broadband data capability, traditional cellular voice-call setup latency typically ran 1–3 seconds, which could not meet command organizations' need for low-latency PTT communication. By introducing a floor-control mechanism, MCPTT achieves low-latency group-call communication over LTE networks — after a user presses the PTT button, the system can complete the floor-request and notification process within a very short time, with response performance approaching that of traditional narrowband trunking systems such as TETRA and P25. To meet on-scene command needs, MCPTT also supports a priority-preemption mechanism, allowing a high-priority user to forcibly interrupt a lower-priority user's transmission, so that an incident commander can immediately take control of communication resources. In terms of service capability, MCPTT supports private calls, group calls, broadcast calls, and emergency calls, and supports end-to-end media encryption based on SRTP as well as user-identity authentication based on the 3GPP Generic Authentication Architecture, meeting public safety's requirements for security and reliability. Release 14 further extended this into the Mission Critical Data (MCData) and Mission Critical Video (MCVideo) standards, which follow MCPTT's priority-control and security framework and respectively support instant messaging, file transfer, location sharing, and real-time video. Together, MCPTT, MCData, and MCVideo make up the MCX (Mission Critical eXchange) mission-critical communication system, marking 3GPP's evolution from a single voice-dispatch system into a broadband public-safety communication platform that integrates voice, data, and video. This system was subsequently incorporated into ITU-R Recommendation M.2009 as one of the broadband radio-interface technology families applicable to public protection and disaster relief.

The Public Warning System (PWS) is another important direction of 3GPP's emergency communication work. TS 22.268 specifies the service requirements for PWS, requiring the system to be able to broadcast warnings to all terminals in a specific geographic area during emergencies such as earthquakes and tsunamis, and to do so reliably regardless of how congested the network is (i.e., delivery must remain reliable even under network overload). TS 23.041 specifies the concrete implementation of cell-broadcast technology, defining the trigger interfaces between base stations and core-network nodes, and the message formats and parameters for four regional implementations: the

Earthquake and Tsunami Warning System (ETWS), the U.S. Wireless Emergency Alerts (WEA/CMAS), EU-Alert, and Korea's KPAS. In 5G NR, TS 29.518 additionally introduces a new N50 interface, defining an HTTP/2-based service-based interface between the cell-broadcast control function and the 5G Access and Mobility Management Function, enabling 5G NR networks to natively support second-level, precisely polygon-targeted public warning, advancing the geographic precision and trigger speed of CBS to a new level.

1.3.4 Internet Engineering Task Force (IETF)

The IETF is the core organization for internet technical-standards development worldwide, founded in 1985 as an open international technical standards body. Unlike the ITU, which focuses on spectrum management and service frameworks, or 3GPP, which focuses on the mobile-communication protocol system, the IETF's research focus in emergency communication is resolving the key problems of location, discovery, routing, security, and congestion control that arise when emergency services run over the open, IP-based internet. Its output forms an important protocol foundation for next-generation emergency-call systems (NG911/NG112) and VoIP-based emergency communication. Some of the main technical standards relevant to emergency communication are shown in Table 9.

Table 9. Selected IETF Standards Related to Emergency Communication

No.	Title	Standard No.
1	General Requirements for Emergency Telecommunication Service (ETS)	RFC 3689
2	IP Telephony Requirements for Emergency Telecommunication Service (ETS)	RFC 3690
3	Communications Resource Priority for the Session Initiation Protocol (SIP)	RFC 4412
4	Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite	RFC 4542
5	Requirements for Emergency Context Resolution with Internet Technologies	RFC 5012
6	A Uniform Resource Name (URN) for Emergency and Other Well-Known Services	RFC 5031
7	Security Threats and Requirements for Emergency Call Marking and Mapping	RFC 5069

No.	Title	Standard No.
8	LoST: A Location-to-Service Translation Protocol	RFC 5222
9	Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)	RFC 5223
10	HTTP-Enabled Location Delivery (HELD)	RFC 5985
11	Framework for Emergency Calling Using Internet Multimedia	RFC 6443
12	Best Current Practice for Communications Services in Support of Emergency Calling	RFC 6881
13	Public Safety Answering Point (PSAP) Callback	RFC 7090
14	Additional Data Related to an Emergency Call	RFC 7852
15	Next-Generation Pan-European eCall	RFC 8147
16	Non-interactive Emergency Calls	RFC 8876

With the widespread adoption of VoIP and internet multimedia communication, the traditional PSTN-based E911/E112 emergency-call system faces a fundamental challenge. Traditional telephone networks rely on a static binding between a fixed phone number and a geographic location, allowing an emergency call to be automatically routed to the nearest Public Safety Answering Point (PSAP); in an internet environment, however, there is no natural mapping between an IP address and a user's actual geographic location, and users may also access the internet via mobile terminals, softphones, or roaming networks – all of which cause traditional fixed-location-based emergency-call routing mechanisms to fail.

To address this, the IETF began systematic research on internet-based emergency communication around 2004 and formed the ECRIT (Emergency Context Resolution with Internet Technologies) working group, dedicated to studying emergency-service location and routing in the internet environment. ECRIT's scope spans requirements analysis, system architecture, location acquisition, call routing, service discovery, security mechanisms, and threat modeling, with the goal of rebuilding, within an open IP network environment, a "location-aware" emergency-calling capability similar to traditional E911/E112, providing standardized protocol support for the NG911/NG112 system. RFC 5012 is the foundational document of this body of work, systematically laying out, in the form of a requirements document, the full range of technical challenges in realizing emergency services over the internet – including the acquisition and delivery of location information, PSAP discovery and selection, special handling of anonymous and unauthenticated users, and end-to-end

routing coordination across multi-operator network environments. RFC 5031 defines the Uniform Resource Name for emergency services, specifying a standardized way to identify emergency-call service types, enabling a SIP client to initiate an emergency call using only a standardized service URI, without needing to know the destination PSAP's address at all. RFC 5222 and RFC 5223 together specify the mapping mechanism between location information and emergency-service access points – the Location-to-Service Translation (LoST) protocol – solving the "location-dependent routing" problem for IP-based emergency calls. RFC 6443 provides a complete end-to-end reference framework for emergency calling using internet multimedia, integrating the requirements of RFC 5012 with protocol standards such as RFC 5031 and RFC 5222. RFC 4412 specifies the mechanism for handling communications resource priority within SIP, an important standard for realizing a function similar to traditional circuit-switched networks' "priority preemption" over IP networks.

In recent years, the IETF has continued to expand the scope of emergency-communication-related standards as technology develops. For connected-vehicle emergency scenarios, RFC 8147 and subsequent documents specify an IP-based in-vehicle emergency call (eCall over IP) system, addressing the protocol problem of a connected vehicle automatically sending a standardized minimum data set to a PSAP after an accident. For non-interactive emergency calling, RFC 8876 specifies a one-way emergency-notification mechanism that does not require establishing a two-way media session. For WebRTC-based emergency communication scenarios, the IETF DISPATCH working group is researching how to achieve LoST service discovery and PSAP routing in browser-initiated real-time communication. This body of work shows that IETF emergency-communication standardization is continuing to extend from traditional VoIP into IoT, connected vehicles, and WebRTC and other emerging scenarios.

1.3.5 Alliance for Telecommunications Industry Solutions (ATIS)

ATIS is an ICT industry standards organization accredited by the American National Standards Institute. Its emergency communication work covers three areas: first, standards for the security, availability, and recoverability of emergency communication services; second, architecture and interface specifications for Next Generation 911 (NG911) systems; and third, standardization of Wireless Emergency Alerts (WEA/CMAS) technology. To advance

cross-network-type emergency interconnection issues in a concentrated way, ATIS has also established the Emergency Services Interconnection Forum (ESIF), dedicated to interconnection research spanning wireline, wireless, cable, satellite, internet, and emergency-services networks – the core coordination platform for achieving cooperation among various types of U.S. communication infrastructure in emergency scenarios. Some of the main technical standards relevant to emergency communication are shown in Table 10.

Table 10. Selected ATIS Standards Related to Emergency Communication

No.	Title	Standard No.
1	Availability & Restorability Aspects of Emergency Telecommunications Service (ETS)	ATIS-0100004
2	Overview of Standards in Support of Emergency Telecommunications Service (ETS)	ATIS-0100009
3	Disaster Roaming Guide and Resources	ATIS-0100054
4	Request for Assistance Interface (RFAI) Specification	ATIS-0500019
5	Applying Common IMS to NG9-1-1 Networks	ATIS-0500023
6	ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture	ATIS-0500032
7	ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection	ATIS-0500036
8	Overview of how an IMS Originating Network Interfaces to an E9-1-1 or NG9-1-1 System	ATIS-0500037
9	Commercial Mobile Alert Services (CMAS) via GSM/UMTS Cell Broadcast Service Specification	ATIS-0700006
10	CMAS via EPS Public Warning System Specification	ATIS-0700010
11	ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination	ATIS-0700015
12	Location Accuracy Improvements for Emergency Calls	ATIS-0700028
13	Enhanced Wireless Emergency Alert (eWEA) Mobile Device Behavior (MDB) Specification (A Revised Version of J-STD-100)	ATIS-0700036
14	Civic and Geodetic Location Conveyance in Support of Emergency Calling	ATIS-0700052
15	Support of Emergency Telecommunications Service (ETS) in IP Networks	ATIS-1000010

No.	Title	Standard No.
16	Emergency Telecommunications Service (ETS): Core Network Security Requirements	ATIS-1000055
17	Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Network (NGN)	ATIS-1000057
18	Emergency Telecommunications Service Wireline Access Requirements	ATIS-1000059
19	Emergency Telecommunications Service (ETS) Roadmap	ATIS-1000070
20	Joint ATIS/TIA CMAS Mobile Device Behavior Specification	J-STD-100

In the standardization of Emergency Telecommunications Service (ETS), ATIS has continuously produced a series of engineering specifications for ETS implementation since 2006. ATIS-0100009 provides a technical overview of the standards system supporting ETS, mapping ITU-T E.106 and E.107 against North American network-implementation practice, and identifying 18 ETS functional requirements together with the corresponding signalling and transport protocol structures — a foundational reference document for ETS deployment in North America. ATIS-0100004 focuses on ETS availability and recoverability requirements, specifying, from a network-architecture perspective, the redundancy and automatic-recovery capability that ETS network nodes should possess in the face of equipment failure, transmission interruption, and disaster impact, and giving quantitative availability targets. ATIS-1000055 sets detailed core-network security requirements for ETS, covering access authentication, signalling protection, media-stream encryption, and security auditing, with particular emphasis on the special requirements for user-identity authentication and SIP signalling security in NGN (IMS) environments. ATIS-1000059 focuses on ETS implementation requirements on the wireline access-network side, specifying the technical mechanism by which IP-based wireline access networks provide priority access for ETS users under overload and disaster conditions, addressing the engineering problem of how wireline operators implement ETS priority access in emergency scenarios. ATIS-1000070, as the ETS roadmap document, systematically lays out the technical path for ETS's evolution from traditional PSTN toward NGN/IMS, comparatively analyzing the standardization maturity of each stage, and providing a reference framework for operators planning the evolution of their emergency-communication IT infrastructure.

In the area of Next Generation 911 (NG911) and NGN emergency calling, ATIS

has carried out systematic work through the ESIF forum and various work items. ATIS's research on NGN (IMS) emergency-call handling details how SIP/IMS networks process emergency calls originating from fixed and mobile terminals, including emergency session identification, PSAP routing selection, IMS priority handling, and billing exemption; its results are concentrated in ATIS-0700015, which directly supports the North American standardization of the U.S. NG911 i3 architecture. On the question of NG911 location, ATIS has researched mechanisms for delivering high-precision caller location to the PSAP in IMS/LTE networks, including deployment of the HELD protocol, North American adaptation of Advanced Mobile Location, and engineering approaches to enhancing indoor positioning accuracy; the related results are concentrated mainly in the ATIS NG911 and location-enhancement series of specifications, coordinated technically with ETSI TS 103 625.

In Wireless Emergency Alerts (WEA) standardization, ATIS has taken primary responsibility for developing technical specifications for the U.S. Commercial Mobile Alert Service (CMAS). In 2008, ATIS jointly published J-STD-100 with TIA, specifying the system architecture and interface protocols by which FEMA's Integrated Public Alert and Warning System distributes public-warning information to user terminals via commercial mobile-operator networks. This standards family is based on the cell-broadcast technology defined in 3GPP TS 23.041, specifying the complete flow of message delivery from a FEMA alert-aggregation point through the operator network to the terminal, as well as terminal display and audio-alert handling rules for different message types. ATIS has continued to update the WEA/CMAS standards since then: ATIS-0700006 specifies the implementation of CMAS over GSM/UMTS networks, and ATIS-0700010 specifies the implementation of the public-warning system based on EPS (LTE packet system). ATIS has also published the WEA 3.0 Mobile Device Behavior (MDB) specification, providing an engineering baseline for enhanced geo-targeting capability in terminal implementations.

1.4 Current Status of Emergency Communication Development

1.4.1 Current Status in Japan

Japan is a country prone to frequent earthquake disasters, compounded by tsunami, typhoon, and volcanic threats. Under continuous disaster pressure,

Japan has gradually built the most technically integrated national-level emergency communication system in the world. Japan's emergency communication system uses the Central Disaster Prevention Radio Network as its national backbone, disaster-prevention administrative radio networks at each level as the local terminus, and J-Alert as the nationwide unified warning-trigger mechanism, forming a multi-layered dedicated disaster-prevention radio communication system. As shown in Figure 1, multiple dedicated networks – the Central Disaster Prevention Radio Network, ministry-specific dedicated communication networks, the fire and disaster-prevention radio network, prefectural disaster-prevention administrative radio networks, and municipal disaster-prevention administrative radio networks – together form the nationwide disaster-prevention radio network. Each level of network operates independently while coordinating under a unified command system when a disaster occurs.

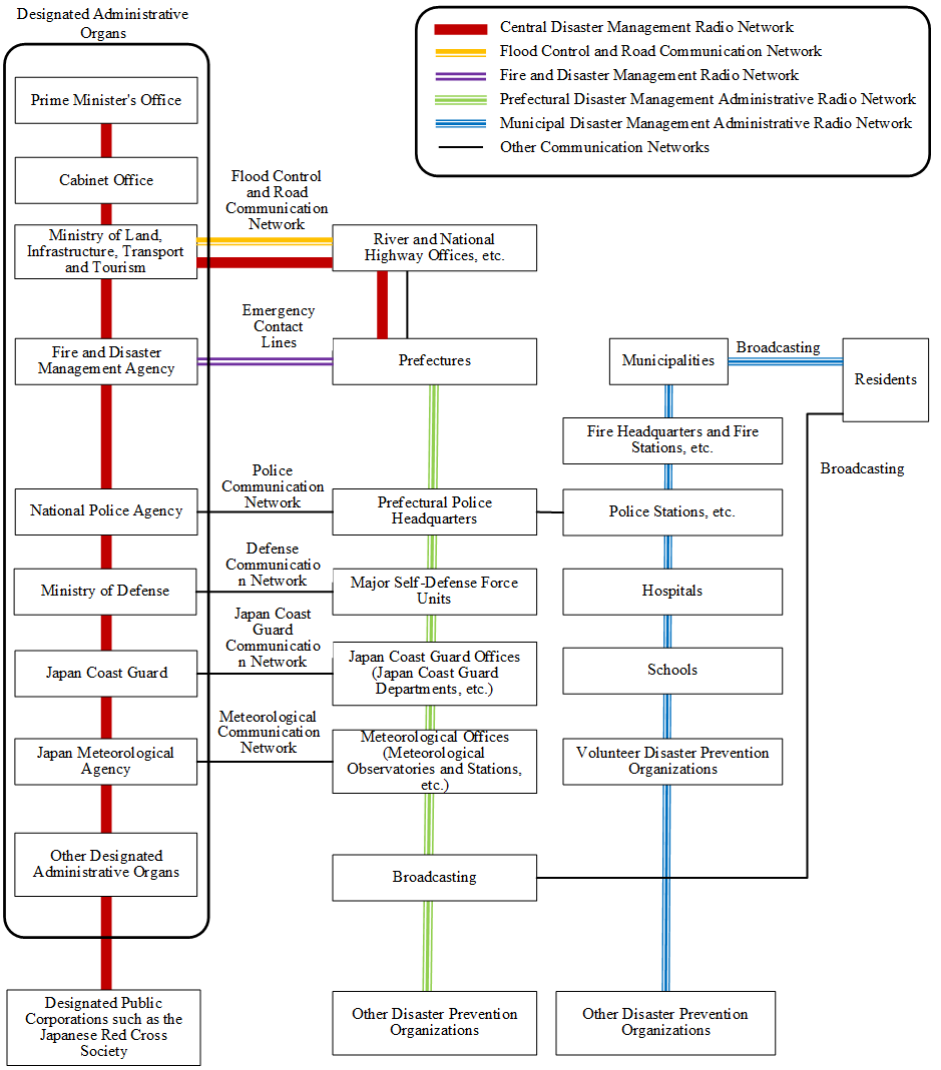


Figure 1. Japan's Disaster Prevention Radio Network

1. Central Disaster Prevention Radio Network

The Central Disaster Prevention Radio Network is operated by Japan's Cabinet Office and is the core hub of the nation's highest-level emergency communication, ensuring uninterrupted voice, fax, and data communication between the Prime Minister's Office, the Cabinet Office, the various ministries, and the prefectures during a major disaster. The network uses communication satellites as its primary backbone, with terrestrial dedicated lines as backup, giving it a high degree of resilience. Organizationally, Japan's Central Disaster Prevention Council is the highest decision-making body for disaster

prevention, exercising nationwide command and coordination through the Central Disaster Prevention Radio Network. Depending on the severity of the emergency, command is divided into three tiers: general or relatively major incidents are handled by the disaster response headquarters of the municipality or prefecture; major and particularly major incidents are directly commanded by a Cabinet-established Extreme Disaster Management Headquarters, at which point the Central Disaster Prevention Radio Network becomes the communication backbone for the highest level of national emergency command.

The core function of the Central Disaster Prevention Radio Network is to ensure communication among the Prime Minister's Office, designated administrative agencies, designated public institutions, the 47 prefectural governments, and the five ordinance-designated cities of the greater Tokyo area during a large-scale disaster, and, through this network, to aggregate and share information on disaster conditions and response status. Construction of the network dates back to 1978; after more than 40 years of sustained investment and iterative upgrades, it has formed a multi-link redundant communication system, as shown in Figure 2.

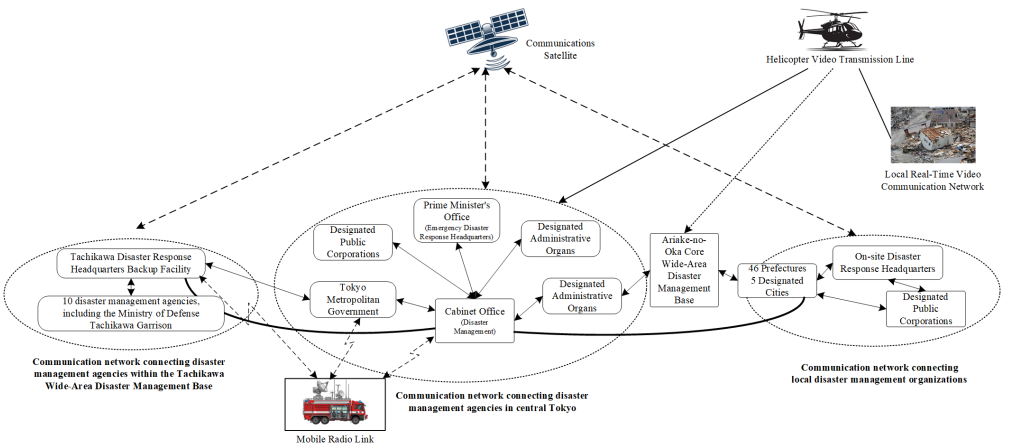


Figure 2. Structure of Japan's Central Disaster Prevention Radio Network

In terms of network topology and functional positioning, Japan's Central Disaster Prevention Radio Network carries out four core communication missions.

First, ensuring interconnection among disaster-prevention-related agencies. In central Tokyo, 7.5 GHz and 38 GHz terrestrial microwave links connect

the Prime Minister's Office, central ministries, designated public institutions, and the Tokyo Metropolitan Government, carrying voice, fax, disaster video, video conferencing, and LAN data, among other traffic types; designated public institutions outside central Tokyo connect to the backbone network mainly via satellite links. All 46 prefectures connect to the central government via the dedicated terrestrial microwave network for flood-control roads administered by the Ministry of Land, Infrastructure, Transport and Tourism (MLIT), together with commercial-operator leased lines; high-risk areas such as those threatened by a Tokai earthquake also connect, in parallel, to an MLIT dedicated fiber network as backup, improving link redundancy and disaster resilience.

Second, ensuring forward communication support for on-site disaster response headquarters. Once a disaster occurs, a temporarily established on-site disaster response headquarters can open a temporary satellite link with the government's Extreme Disaster Management Headquarters via a mobile satellite ground station, achieving efficient information exchange between the disaster site and the central command. Such mobile satellite ground stations are pre-positioned at multiple locations across Japan and can be rapidly deployed to an affected area after a disaster, quickly setting up channels for disaster video backhaul, video conferencing, voice, and fax.

Third, ensuring stable backbone communication between the central government and the prefectures. In addition to terrestrial microwave links and commercial-operator leased lines, Japan's Cabinet Office maintains a dedicated disaster-information-sharing communication facility carrying disaster-video sharing and cross-region video conferencing between the central government and prefectures, with the main link carried over operator leased lines; for high-risk priority areas, an MLIT dedicated fiber network is deployed in parallel as a redundant backup channel, further strengthening reliability under extreme conditions.

Fourth, ensuring emergency command and liaison capability after a disaster strikes. Command personnel for disaster response at every level are uniformly equipped with vehicle-mounted, backpack-mounted, and handheld radio terminals, along with dedicated emergency-liaison mobile phones and portable satellite terminals. Among these, the emergency-liaison terminals can interlock with the Japan Meteorological Agency's warning system to automatically push emergency assembly instructions once a disaster warning is issued; portable satellite terminals serve as a fallback means of communication after

ground public networks fail, ensuring that command-personnel communication is not interrupted and the command chain is not broken in the early stages of a disaster.

At the level of disaster-information processing and sharing, the Central Disaster Prevention Radio Network provides the underlying communication infrastructure for the Comprehensive Disaster Information System. Based on seismic-intensity monitoring data, this system overlays multiple categories of information – disaster-loss estimates, lifeline-service outages, river hydrological monitoring, real-time disaster conditions, evacuation shelters, and disaster medical facilities – displayed visually in map layers, including seismic-intensity distribution estimates, traffic-control information, and residential-damage information layers, as well as satellite remote-sensing imagery layers provided by the Japan Aerospace Exploration Agency (JAXA), supporting the government in quickly assessing the disaster situation and making efficient, scientifically informed emergency decisions. The Central Disaster Prevention Radio Network also carries out nationwide real-time disaster-video sharing: aerial footage from disaster-prevention helicopters operated by the National Police Agency, the Fire and Disaster Management Agency, MLIT, the Japan Coast Guard, and the Ministry of Defense, among others, is aggregated at the Cabinet Office over each agency's own dedicated communication network, then distributed to all connected disaster-prevention-related agencies through the Central Disaster Prevention Radio Network's video-sharing system. In addition, the national Extreme Disaster Management Headquarters can hold remote video conferences with the on-site disaster response headquarters, allowing the Prime Minister (or the minister in charge of disaster prevention) to consult directly with the governor of the affected prefecture and the head of the on-site headquarters on the disaster situation and response measures.

Operationally, the Central Disaster Prevention Radio Network runs on a 24/7 basis, with real-time monitoring of all network links through a monitoring interface and regular functional inspections to maintain long-term stable availability. Network reliability is assured mainly through two measures: first, a fully redundant network architecture, under which the system can automatically switch to a detour route if any network node or link fails, without affecting normal operation of the network as a whole; second, an uninterruptible power-supply mechanism, under which, in the event of a mains-power outage, battery packs and backup generators take over to keep communication services running. For business-continuity assurance, the system strictly follows the Cabinet Office's business-continuity plan requirements: if the Cabinet Office's

main site in central Tokyo suffers a major failure, communication-control core capability can be migrated to backup facilities at the Tachikawa Wide-Area Disaster Prevention Base's disaster response headquarters; core disaster-prevention data such as the Comprehensive Disaster Information System and shared service directories are also backed up off-site at the Tachikawa base at the same time, forming a primary/backup dual-center architecture that achieves business continuity and disaster-recovery resilience under extreme disaster conditions.

2. Disaster Prevention Administrative Radio Network

The Disaster Prevention Administrative Radio Network is a dedicated local disaster-prevention radio system, independent of the Central Disaster Prevention Radio Network, covering the prefectural and municipal levels – it is also the "last mile" infrastructure that delivers national-level warning information to the general public at the grassroots level. At the prefectural level, the prefectural Disaster Prevention Administrative Radio Network handles coordinated communication among government departments within the jurisdiction: horizontally connecting the prefectural police headquarters, the coast guard, the meteorological department, the main force of the Self-Defense Forces, and various disaster-prevention-related units; vertically connecting municipal governments with grassroots emergency-response bodies such as fire stations. At the municipal level, the Disaster Prevention Administrative Radio Network takes two main forms: one is a one-way broadcast mode, using outdoor loudspeakers and wired household receivers to simultaneously broadcast warnings and disaster notices to residents, which can also be linked with broadcast and television operators for joint release; the other provides two-way intercom communication, supporting on-site command and dispatch and information exchange between frontline rescue personnel and the municipal disaster response headquarters. In recent years, Japan's disaster-prevention administrative radio system has been undergoing a comprehensive upgrade from analog to digital IP-based architecture, migrating the backbone links of the disaster-prevention administrative radio network onto IP infrastructure, to improve information-processing capability, remote operations-and-maintenance efficiency, and reliability of interlock with other disaster-prevention business systems such as the J-Alert automatic trigger devices.

3. Nationwide Instantaneous Alert System (J-Alert)

J-Alert was built and put into operation in 2007 by Japan's Fire and Disaster Management Agency, under the Ministry of Internal Affairs and Communica-

tions. It is the core national-level emergency-warning platform, capable of pushing urgent information simultaneously to every municipality nationwide and to the public within seconds; it also serves as the rapid warning-trigger hub within Japan's multi-layered disaster-prevention radio system. Every municipality in Japan has now completed deployment of J-Alert automatic trigger facilities. Its operational flow is as follows: the Cabinet Secretariat, the Japan Meteorological Agency, and other bodies generate urgent warning information, which the Fire and Disaster Management Agency distributes via communication satellite to J-Alert automatic trigger devices pre-positioned at each municipality; the device then automatically activates the local disaster-prevention administrative radio simulcast system, playing the warning tone and message through outdoor broadcast terminals, while simultaneously triggering NHK to interrupt television broadcasting with the emergency warning, and pushing regional warning text messages via mobile-operator networks. This cell-broadcast function follows the 3GPP TS 23.041 ETWS international standard.

1.4.2 Current Status in the United States

1. National Emergency Communications Plan (NECP)

The NECP is developed and updated by the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security, and it is the highest-level strategic guidance document in U.S. emergency communication. The current effective version is the 2019 edition; a NECP summary document published by CISA in March 2024 confirmed that this version remains in effect, and it reviews current implementation progress and priorities.

The national vision established by the 2019 NECP is "to enable the Nation's emergency response community to communicate and share information in real time, securely, and across communications technologies, for all levels of government, disciplines, and jurisdictions and agencies, and impacted individuals affected by any threat or hazard." The NECP is organized around six strategic goals: governance and leadership, planning and procedures, training, exercises, and evaluation, communications coordination, technology and infrastructure, and cybersecurity. Through the annual SAFECOM Guidance (FY2025 edition), the NECP translates these strategic goals into compliance requirements for federal grant funding, steering state investment toward systems that follow the NECP technical roadmap.

2. First Responder Network Authority (FirstNet)

FirstNet is a nationwide broadband infrastructure built in the United States specifically for first responders (police, fire, and EMS). FirstNet uses a commercial network as its physical carrier, achieving an exclusive experience for public-safety users while sharing commercial infrastructure through dedicated spectrum, priority-preemption mechanisms, and a public-safety-specific network slice – delivering reliability higher than typical commercial service at a lower cost than building an independent dedicated network. The network uses the FCC-licensed 700 MHz Band 14 public-safety-dedicated spectrum, based on 3GPP LTE/5G standards, providing users with always-on priority access and preemption capability. During periods of extreme network congestion, the system automatically releases commercial-user resources to prioritize the transmission of rescue instructions and critical data. FirstNet has completed its initial network build and is now in a deep 5G evolution phase; public-safety users can operate not only on Band 14 but also, with preemption rights, on AT&T's full-band commercial 5G links. FirstNet is also integrating direct-to-device satellite connectivity and high-altitude platform capability, to close ground-network coverage gaps in scenarios such as forest firefighting and wilderness rescue.

1.4.3 Current Status in Europe

Europe's emergency communication system is built on the widespread deployment of dedicated TETRA networks as its technical foundation, while an EU regulatory framework has also driven the establishment of a multi-country public-warning system. Member states' dedicated-network technical routes are highly unified, while public warning has been driven toward EU-Alert deployment through the EECC regulation.

1. Germany's Digital Trunked Radio Network (BOSnet)

BOSnet is the largest TETRA public-safety dedicated network in the world, built and operated by the Federal Agency for Public Safety Digital Radio (BDBOS). BOSnet operates in the 380–395 MHz band using TDMA technology, providing a complete set of public-safety communication functions including encrypted voice calling, priority dispatch, and direct mode, with shared access supported for police, fire and rescue, emergency medical services, technical relief, and other public-safety agencies. As of 2024, BOSnet has deployed more than 5,000 base stations, with a core network comprising over 60

switching nodes and more than 1.2 million registered terminals. In terms of its construction model, BOSnet is built and operated centrally by BDBOS and shared jointly by the federal states, forming an operating model of a single shared network with unified management and shared costs.

2. France's Public-Safety Networks and the FR-Alert Warning System

France's dedicated public-safety communication system consists of multiple networks serving different response agencies. ACROPOL (Automatisation des Communications Radioélectriques Opérationnelles de la Police) is the TETRA trunked network used by the national police and the gendarmerie, covering urban and rural areas nationwide; ANTARES (Adaptation Nationale des Transmissions Aux Risques Et aux Secours) is the dedicated wireless trunking network for fire and emergency medical rescue services, providing voice dispatch and data-transmission capability; RUBIS is the gendarmerie's independent communication network. Together these three dedicated networks form the communication infrastructure of France's public-safety agencies. As demand for multimedia emergency communication grows, the French Ministry of the Interior has begun planning an evolution toward hybrid public/dedicated broadband networks, exploring the addition of dedicated security mechanisms over commercial 4G/5G networks to carry broadband video and data services that the existing dedicated networks cannot support.

FR-Alert is France's nationwide public-warning system, established under Article 110 of the European Electronic Communications Code (EECC, Directive 2018/1972/EU). Led by the French Ministry of the Interior, it was formally deployed across mainland France (including overseas departments) in June 2022, making France one of the first countries in Europe to complete deployment of a cell-broadcast public-warning system. FR-Alert uses two complementary technical approaches: first, cell broadcast over 4G/5G networks, pushing warning notifications via radio waves to all compatible terminals within coverage, typically completed within seconds – triggering a distinct alert tone even if the phone is on silent mode, and requiring no app installation or account registration in advance; second, location-based SMS, covering all terminals from 2G through 5G, with somewhat slower delivery but broader terminal compatibility. FR-Alert can be used for four categories of major hazard scenario – natural disasters, industrial accidents, public health incidents, and security threats – with warning-area precision down to the base-station level, and issuance authority held by the Prime Minister or the relevant prefect.

Chapter References

[1] ITU-R. *M.2377-2 Radiocommunication objectives and requirements for public protection and disaster relief.* Geneva: ITU, 2023.

[2] ITU-R. *M.2033 Radiocommunication objectives and requirements for public protection and disaster relief.* Geneva: ITU, 2003.

[3] ITU-T. *Y.1271 Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks.* Geneva: ITU, 2014.

[4] ITU-T. *Y.2205 Next Generation Networks – Emergency telecommunications – Technical considerations.* Geneva: ITU, 2011.

Chapter 2: Emergency Communication System Requirements

Emergency communication systems are critical infrastructure that underpins public protection and disaster relief (PPDR) operations. When responding to sudden-onset incidents, efficient and reliable communication support has a direct bearing on the coordination efficiency of response forces, the real-time responsiveness of command decision-making, and the ultimate success of the emergency response. Emergency communication, however, faces special challenges that conventional commercial communication networks do not: the system must remain available in extreme environments, support peak traffic loads several times higher than everyday levels, ensure cross-agency, cross-region, and even cross-border coordination and interoperability, and maintain basic communication capability even when infrastructure is partially or completely destroyed. These challenges drive the design philosophy, technology choices, and requirements definition of emergency communication systems. Drawing on the relevant emergency communication standards, this chapter systematically presents the architecture and requirements framework for emergency communication systems, including the technical, functional, and operational objectives of emergency communication systems; typical application scenarios and their corresponding service requirements; and emergency communication user requirements.

2.1 Emergency Communication System Objectives and Requirements

The design and construction of an emergency communication system must be grounded in a clearly defined set of objectives and a requirements framework. The ITU-R M.2377 series of Recommendations systematically establishes objectives and requirements for public protection and disaster relief (PPDR) radiocommunication, providing an international reference for the planning and construction of national emergency communication systems. Following ITU-R Recommendation M.2377-2, this book divides emergency communication

system objectives and requirements into three tiers: technical and functional objectives, operational objectives, and operational requirements.

2.1.1 Technical and Functional Objectives

Technical and functional objectives define the core capabilities an emergency communication system must possess, spanning communication integration, security assurance, equipment ruggedness, coverage capability, interoperability, and other dimensions.

1. Multimedia Communication Integration

Emergency communication systems must support integrated voice, data, and image communication, which is a foundational requirement for multimedia command and dispatch. QoS requirements differ significantly across service types: voice communication requires low latency and high reliability, with typical coding rates of 8–13 kbps; real-time video requires high bandwidth (e.g., 720p video requires 2–4 Mbps) and relatively low latency; and data transmission tolerates higher latency but requires a low bit error rate. From a technical implementation standpoint, an IP-based converged communication architecture is the mainstream technical path for achieving multimedia integration.

2. End-to-End Security Assurance

The information carried by emergency communication systems may include operational deployments, personnel locations, tactical decisions, and other sensitive content, requiring protection against information leakage, tampering, and unauthorized access. End-to-end encryption is the primary technical means of achieving communication security, requiring that data be encrypted at the sending end and decrypted at the receiving end, with the data remaining in ciphertext throughout intermediate transmission and storage. Introducing security mechanisms increases system latency and computational overhead, so low-latency applications must balance security strength against latency performance.

3. Adaptability to Extreme Environments

Emergency communication equipment typically must operate continuously and stably in complex, harsh environments, with use cases potentially involving high or low temperatures, high humidity, low air pressure, dust, strong vibration, and drop impacts. Such equipment therefore generally requires a high degree of environmental adaptability, including a high level of ingress

protection (IP rating), shock and vibration resistance, and the ability to keep working normally across a wide temperature range and under strong electromagnetic interference. However, ruggedization measures that strengthen environmental adaptability often come with a marked increase in equipment weight, size, and cost, so engineering practice requires a comprehensive trade-off among reliability, mobility, and economy.

4. Wide-Area Coverage and Coverage of Shielded/Enclosed Spaces

The locations where emergencies occur are typically highly unpredictable, placing high demands on the coverage capability of emergency communication networks. The system must cover not only cities, suburbs, rural areas, mountainous regions, and maritime areas, but also maintain basic communication capability when infrastructure is damaged or has failed entirely. In major disaster relief scenarios in particular, fixed communication facilities may be severely damaged and conventional base stations may be unable to function, so temporary means of communication – such as satellite communication, drone-based aerial relay, vehicle-mounted mobile base stations, and portable ad hoc networks – are often needed to rapidly restore coverage.

At the same time, many emergencies occur in complex shielded spaces, such as building interiors, underground tunnels, mines, and underground utility corridors. These environments significantly attenuate and block wireless signal propagation and readily create coverage blind spots, placing higher demands on an emergency communication system's penetration capability, indoor coverage capability, and networking capability in complex environments.

In addition, user density on emergency communication networks typically exhibits pronounced spatiotemporal non-uniformity. Under everyday operating conditions, the number of concurrent users in a single cell or local area may be only a few dozen; however, after a major incident occurs, large numbers of rescue personnel, government staff, and members of the public converge on the same area within a short period, simultaneously generating command-and-dispatch, on-scene backhaul, and public communication traffic, and the instantaneous user population and traffic volume in a local area can grow sharply. This kind of sudden, high-density access can readily cause radio-channel congestion, intensified contention for network resources, and degraded service quality, so emergency communication networks need strong capacity elasticity, priority scheduling, and rapid expansion capability to ensure that critical services remain stable under high-load conditions.

5. Multi-Network Interoperability

Emergency response typically involves multiple agencies, which may use dedicated communication networks of different standards (such as PDT, TETRA, or ad hoc networks) or rely on public networks. Achieving efficient coordination requires resolving interconnection issues between heterogeneous networks. The current mainstream interoperability approach is to deploy a dedicated gateway device that connects to multiple heterogeneous networks simultaneously and performs protocol conversion at the application layer or network layer. 3GPP introduced mission-critical communication standards in Release 13, defining an LTE-based mission-critical push-to-talk service and providing a unified interface for interoperability among equipment from different vendors.

6. Rapid Call Setup Capability

Emergency communication is characterized by low latency, high concurrency, and group coordination. Push-to-talk (PTT) is the most representative service mode: once a user presses the PTT button, the system must complete call setup within an extremely short time. Per the requirements of ITU-R M.2377-2, mission-critical voice services generally require call setup latency to be kept under 500 ms, and end-to-end voice or data transmission latency under 1 s. Group calling is one of the most essential service forms in emergency communication, implementing a "one speaks, many receive simultaneously" communication mode to meet the needs of on-scene command and coordinated operations. Because traditional point-to-point communication is poorly suited to large-scale group scenarios, emergency communication systems typically use mechanisms such as multicast to improve transmission efficiency, and reduce call setup latency through group pre-configuration and priority management, thereby ensuring real-time performance and reliability for large-scale coordinated communication.

7. Location Services and Situational Awareness

During emergency response, knowing the real-time location of rescue personnel, vehicles, and key resources is an important foundation for effective command and dispatch. Emergency communication systems therefore generally need continuous, reliable positioning capability to support situational awareness and resource management in complex environments. Outdoors, positioning is typically achieved via GNSS technology, which can meet the high-precision positioning needs of personnel and equipment; in-

doors, underground, or in environments where satellite signals are obstructed, base-station-assisted positioning, short-range wireless positioning, and multi-source fusion positioning are typically used to improve positioning availability and accuracy in complex environments. For three-dimensional scenarios such as high-rise building fires or underground-space rescue, horizontal position alone is often insufficient to support effective dispatch, so vertical position information – such as floor height – is also needed. This capability typically relies on barometric sensors, three-dimensional positioning, or multi-source fusion positioning to improve positioning accuracy and rescue efficiency in complex spatial environments.

8. High Spectral Efficiency and Dynamic Spectrum Management

Emergency communication systems typically operate in lower frequency bands such as VHF/UHF, which offer strong diffraction, long propagation distance, and good penetration – characteristics well suited to wide-area coverage and on-scene communication in complex environments. At the same time, however, the spectrum available for emergency communication is generally limited while service demand continues to grow, so spectrum scarcity remains a key constraint in the construction of emergency communication systems.

To improve the utilization efficiency of limited spectrum resources, modern emergency communication systems continue to introduce high-spectral-efficiency technologies, including higher-order modulation, multi-antenna technology, carrier aggregation, and dynamic spectrum access, to increase system capacity and data transmission capability. Narrowband trunking systems emphasize coverage capability and highly reliable voice communication, while broadband systems use higher spectral efficiency to support broadband services such as video backhaul and data sharing.

At the same time, advances in software-defined radio (SDR) technology are giving emergency communication equipment increasing multi-mode, multi-band, and dynamic reconfiguration capability. By configuring radio functions in software, the same hardware platform can flexibly switch among different communication schemes and access modes according to on-scene conditions, enabling converged access to trunked communication, broadband mobile communication, satellite communication, and other networks – improving communication adaptability and resource-utilization efficiency in complex disaster scenarios.

9. Network Resilience and Self-Healing Capability

Emergency communication networks may face a range of failure risks during sudden-onset incidents, including infrastructure damage caused by disasters such as earthquakes and floods, base-station failures triggered by extended power outages, loss of backhaul connectivity due to fiber or microwave link interruptions, and security threats such as cyberattacks and physical equipment destruction. Emergency communication systems therefore place greater emphasis on network survivability and operational resilience than ordinary public communication networks.

To sustain operation under extreme conditions, emergency communication networks typically employ multi-tier redundancy and disaster-recovery design. At the access layer, deploying multiple sites in key areas improves coverage reliability; at the core-network layer, active/standby architectures and disaster-recovery mechanisms ensure the continuity of core services; and at the transport layer, a mix of fiber, microwave, satellite, and other backhaul methods enables link backup and automatic switchover, reducing the impact of single points of failure on the overall network.

At the same time, modern mobile communication systems are progressively introducing self-organizing network technology, using mechanisms such as automatic configuration, automatic optimization, and automatic recovery to improve the network's ability to adapt to complex environmental changes. For example, when some base stations fail, surrounding base stations can automatically adjust their coverage parameters to mitigate local coverage gaps and capacity pressure.

For the extreme case in which the core network becomes unreachable during a disaster, mobile communication systems have also introduced "isolated-island operation" capability, whereby a base station that has lost its connection to the core network can still maintain basic local communication service within a limited range. The Isolated E-UTRAN Operation for Public Safety (IOPS) mechanism introduced by 3GPP in Release 13 is an important example designed for public-safety scenarios; its objective is to preserve basic voice and data communication for on-scene users even when the core network is unreachable.

10. Low Power Consumption and Extended Battery Life

Emergency communication terminals typically need to operate continuously in long-duration, high-intensity task environments – for example,

continuous on-scene rescue, inspection, or duty tasks lasting several hours or even more than ten hours – while handheld device battery capacity and carried energy supply are limited. If a terminal remains in a high-power-consumption state for extended periods, such as continuous transmission, frequent data transfer, or prolonged high-brightness display, it will struggle to meet the sustained-operation requirements of emergency scenarios. Low-power design and energy-management capability are therefore important engineering metrics for emergency communication terminals.

To extend device battery life, modern mobile communication systems widely employ energy-saving mechanisms, including periodic sleep, adaptive wake-up, deep standby, and dynamic transmit-power control, reducing terminal power consumption while preserving communication reachability. Among these, discontinuous reception and its enhancements reduce power consumption during a terminal's idle state, while adaptive power control dynamically adjusts transmit power according to channel conditions, avoiding unnecessary energy consumption. For long-term unattended deployments – such as environmental monitoring terminals, border surveillance nodes, and forest-fire early-warning sensors – solar, wind, and other energy-harvesting technologies can also be combined to enable long-term, low-maintenance, or even maintenance-free operation, improving the system's ability to sustain support in remote and complex environments.

2.1.2 Operational Objectives

Operational objectives focus mainly on the long-term sustainable operation of an emergency communication system. Beyond technical performance, they also involve construction cost, operation and maintenance, organizational management, policy and regulation, and resource assurance. These non-technical factors directly affect the system's construction model, adoption, and long-term operational effectiveness, and are an important safeguard for the sustained, stable functioning of the emergency communication system.

1. Cost Acceptability

The cost of an emergency communication system covers not only the initial construction investment in infrastructure such as base stations, the core network, and terminals, but also the full life-cycle cost of operation and maintenance, system upgrades, and equipment retirement. The operational phase

involves long-term expenditures such as power supply, site and equipment-room leasing, spectrum occupation, and routine operations and maintenance; the maintenance phase covers equipment replacement, software upgrades, fault repair, and technical support. As communication technology continues to evolve, the system must also bear the cost of generational upgrades and retrofits — for example, the transition from traditional narrowband trunking to broadband mobile communication systems. In addition, decommissioning and disposal of retired equipment also incur costs. International engineering practice generally shows that the long-term operation and maintenance cost of an emergency communication system typically exceeds its initial construction investment, making full life-cycle cost control an important issue in system planning.

Different countries and industries have taken different paths to system construction based on their own management systems, communication industry base, and public-safety needs. One approach is to build an independent dedicated network, invested in and operated primarily by government, which offers strong controllability and security but comes with higher construction and maintenance costs. Another approach is to rely on commercial mobile communication networks, providing assurance to emergency users through mechanisms such as priority access and dedicated network slicing; the advantage here is the ability to share in the scale effects and technological progress of public networks, but this approach depends more heavily on public-network availability during emergencies. In recent years, an increasing number of countries have begun exploring a "public-private hybrid" model, in which commercial networks provide the primary service under everyday conditions, while dedicated systems provide critical assurance capability during major disasters or public-network failures — balancing economy, technological currency, and reliability.

2. Interoperability and Standardization

Interoperability is not only an important technical metric for emergency communication systems but also a key factor influencing construction and operational efficiency. From an operational perspective, good interoperability improves procurement flexibility, reduces dependence on a single vendor, and avoids vendor lock-in, thereby lowering construction and maintenance costs through multi-vendor competition. Interoperability is also directly tied to cross-region coordination capability. When an incident affects multiple administrative regions or requires joint handling by multiple departments,

whether different regions and different systems can achieve rapid interconnection directly affects the efficiency of unified command and coordinated dispatch. Likewise, in international rescue scenarios, whether communication equipment brought by external rescue forces can quickly connect to the local emergency communication system is an important measure of the system's openness and compatibility.

From an industry-development standpoint, adopting open standards and standardized technology systems helps form a large-scale industrial ecosystem, lowering the cost of terminal and network equipment. The development of global mobile communication systems has shown that the higher the degree of standardization, the more mature the industry chain, and the lower equipment and operations-and-maintenance costs tend to be. By comparison, closed, proprietary systems may offer certain customization advantages in specific scenarios, but they often suffer from limited industry scale, higher equipment prices, and constrained future evolution. Modern emergency communication systems therefore generally favor international or regional standards to improve openness, compatibility, and long-term sustainability.

3. Spectrum Management and Coordination

Countries vary considerably in how they allocate spectrum resources for emergency communication, primarily through dedicated bands, shared bands, or dynamic allocation. The dedicated-band model allocates independent spectrum resources for emergency communication, ensuring a high degree of independence and interference resistance, but the spectrum tends to be underutilized outside of emergencies. The shared-band model has emergency communication and public communication systems share the same spectrum, using priority mechanisms to guarantee emergency users' communication needs; this improves spectrum utilization efficiency but places higher demands on interference coordination and resource management. The dynamic-allocation model emphasizes flexible scheduling of spectrum resources, using the spectrum for public services under normal conditions and switching it to emergency use through management or technical means once an incident occurs.

Because radio signals propagate across regional boundaries, border areas also face cross-region and cross-border frequency interference issues. The ITU Radio Regulations therefore require countries to conduct frequency coordination in border areas to reduce mutual interference and ensure the normal operation of radio services.

4. Training and Capacity Building

Modern emergency communication systems integrate broadband mobile communication, multi-antenna technology, network slicing, multimedia dispatch, and other advanced technologies, and are markedly more complex than traditional two-way radio systems. Without systematic training, frontline personnel may struggle to operate equipment quickly and accurately under high-pressure, complex conditions, undermining the effectiveness of emergency communication support. A well-developed training system and a routine exercise mechanism have therefore become important components of emergency communication system development.

Training systems are typically designed in layers according to different job responsibilities. Terminal-operation training for frontline rescue personnel focuses on mastering basic communication functions and standardized operating procedures, ensuring that equipment can be used quickly and accurately in emergencies; training for command-and-dispatch personnel emphasizes dispatch organization, resource coordination, and cross-department collaboration capability; and training for technical maintenance personnel focuses more on professional competencies such as network planning, system configuration, fault handling, and operational optimization.

Beyond routine training, live exercises are also an important means of testing system reliability and coordination capability. Exercises typically cover scenarios such as large-scale natural disasters, complex sudden-onset incidents, and damaged communication systems, and are used to verify the rapid-deployment capability of temporary communication systems, joint multi-department command capability, and the system's ability to sustain operation under complex conditions.

5. Policy and Regulatory Support

During sudden-onset incidents and network congestion, emergency communication users typically need high-priority communication assurance to ensure that command, dispatch, and rescue operations can continue uninterrupted. Many countries have therefore established specific provisions, at the level of law, regulation, and communication-sector oversight, for priority access and resource assurance for emergency communication.

At the network-operation level, operators typically need to establish a priority-assurance mechanism for emergency communication – through priority access, resource reservation, and priority service scheduling – to im-

prove the reachability of emergency users under high-load conditions. At the management level, spectrum for emergency communication is typically planned separately to reduce frequency conflicts with other radio services; in key areas, measures such as frequency coordination, transmit-power limits, and protection of the radio environment may also be used to reduce the risk of interference to emergency communication systems from external radio equipment, thereby maintaining the stable operation of critical communication links.

6. Sustainability and Technology Evolution

The pace of communication-technology evolution typically outstrips the construction and renewal cycle of emergency communication systems. Public mobile communication networks generally undergo a generational upgrade roughly once every decade, while emergency communication systems – owing to their large construction scale, long operational life, and high reliability requirements – tend to lag behind. Consequently, many emergency communication systems worldwide are still built on narrowband trunking technologies such as TETRA and PDT, even as public communication networks have moved into 5G and beyond.

To reduce the risk of obsolescence caused by generational technology shifts, emergency communication systems generally need to give full consideration to technology-evolution capability at the design stage – for example, supporting remote software upgrades, compatibility with multiple communication schemes, and modular architecture – to extend system life and protect existing investment. Globally, emergency communication is continuing to evolve toward broadband, IP-based, and converged architectures. In terms of service capability, systems are expanding from traditional narrowband voice trunking to high-definition video, real-time data, and multimedia collaboration; in terms of network architecture, they are shifting from traditional circuit switching toward fully IP-based packet switching; and in terms of construction model, they are evolving from fully independent dedicated networks toward a model of "public-network carriage with dedicated-network assurance" and public-private convergence.

2.1.3 Operational Requirements

Operational requirements translate the technical and functional objectives into concrete, quantifiable metrics for actual operation, covering network

performance, service quality, security policy, and other measurable indicators.

1. Priority Access and Preemption Mechanisms

Different users and services on an emergency communication system carry different levels of importance, requiring a tiered priority mechanism that gives priority to critical communication services when the network is congested or resources are constrained. A typical priority hierarchy generally includes, at the highest level, emergency distress calls and command-center all-network broadcasts; next, task instructions and mission-critical communication from on-scene commanders; then, general dispatch and operational communication; and, at the lowest level, non-real-time data transmission or background services.

Priority access means that, when network resources are constrained, higher-priority users can preferentially obtain radio channels, transmission bandwidth, or core-network processing resources, improving the connection success rate for critical services. On public mobile communication networks, this is typically implemented through service priority, access class, and resource reservation; on dedicated trunking systems, priority calling and priority dispatch are often natively supported by the system.

Preemption is the mechanism by which, when network resources are insufficient, a higher-priority service forcibly interrupts a lower-priority service and takes over its communication resources to ensure uninterrupted mission-critical communication. Because preemption directly affects ongoing communication, the triggering conditions and policy generally must be tightly controlled — for example, triggering preemption only when the network is severely congested and a high-priority service cannot otherwise be established; preferentially interrupting low-priority data services before considering low-priority voice services; and typically notifying the preempted user with an interruption indication and automatically attempting to re-establish the connection once resources become available.

2. Grade of Service and Quality of Service

An emergency communication system must not only be able to communicate, but must also maintain stable, predictable communication performance under complex environments and high-load conditions. System design therefore generally attends to two dimensions: Grade of Service (GoS) and Quality of Service (QoS).

GoS primarily describes the network's access capability and call-

establishment performance, reflecting whether users "can gain access" and "can get through." Its core metrics typically include call-completion rate, call-setup latency, and dropped-call rate. In mission-critical communication scenarios, for example, the system typically requires an extremely high call-completion success rate and as short a PTT call-setup time as possible, while also minimizing the probability of abnormal interruption during communication to ensure a continuous, stable command link.

QoS, by contrast, primarily describes transmission quality after a call has been established, reflecting whether the user's actual communication experience meets service requirements. Different service types are sensitive to QoS metrics in different ways: voice services are more sensitive to latency and jitter, video services place higher demands on throughput and continuity, and data services generally focus more on reliability and integrity. Common QoS metrics include end-to-end latency, packet loss rate, latency jitter, and service throughput.

To meet the differentiated needs of different services, emergency communication systems typically employ a layered QoS assurance mechanism. First, data flows are classified by service type and priority, mapping voice, video, and data services to different QoS classes. Second, at the network-scheduling level, a differentiated resource-allocation strategy is used, prioritizing low-latency transmission for real-time services such as mission-critical voice while applying fair scheduling to non-real-time services. When network congestion occurs, congestion-control and queue-management mechanisms prioritize high-priority services and limit or drop low-priority traffic.

3. Reliability and Availability

Emergency communication systems support disaster relief, on-scene command, and mission-critical communication, so their availability requirements are generally far higher than those of ordinary commercial communication networks. For a public mobile communication network, a brief, localized outage typically only affects user experience; for an emergency communication system, however, a communication failure can directly affect rescue efficiency and even cause serious consequences. High reliability and high availability are therefore always among the core objectives of emergency communication system design. To improve availability, emergency communication networks typically adopt multi-tier redundancy and disaster-recovery design. At the equipment level, core equipment often uses dual hot-standby or N+1 backup mechanisms, automatically switching to backup equipment when the primary

equipment fails; at the network level, multi-link, multi-route design avoids single points of failure — for example, deploying fiber, microwave, and satellite backhaul links simultaneously so they can back each other up; and at the core-system level, geographically dispersed disaster recovery and multi-data-center deployment are commonly used, so that if one node fails, other nodes can continue to carry the service. Modern IP-based emergency communication systems also emphasize rapid-recovery capability, minimizing perceptible service interruption during system switchover or local-fault recovery.

4. Coverage Requirements

Emergency communication networks must provide communication assurance across a wide range of complex geographic environments — urban, rural, mountainous, maritime, and underground — so their coverage design is typically more complex than that of ordinary commercial networks and places greater emphasis on reachability and continuity under extreme conditions.

Coverage approaches differ significantly by scenario. In dense urban environments, where buildings are closely packed and blockage is severe, coverage quality is typically improved through dense base-station deployment, indoor coverage systems, and distributed antenna systems; in suburban and rural areas, wide-area coverage is emphasized, typically achieved through elevated sites and high-power macro base stations for long-range communication; mountainous environments, with their pronounced terrain variation, readily produce radio shadow zones and require site placement optimized for terrain conditions, supplemented by high-point sites and microwave relay to strengthen coverage continuity; and maritime areas, tunnels, and underground spaces often require dedicated coverage techniques such as coastal base stations, shipborne platforms, leaky feeder cable, or distributed antenna systems.

Beyond conventional fixed infrastructure, emergency communication systems must also consider temporary coverage capability under disaster conditions. When ground base stations are damaged or communication infrastructure is disrupted, mobile means — satellite communication, vehicle-mounted base stations, portable base stations, and drone relay platforms — are typically needed to rapidly restore local coverage, forming an emergency-support system that combines fixed networks with mobile systems.

5. Interoperability Requirements

Interoperability is one of the most essential and practically challenging capabilities of an emergency communication system. Incident response typically

involves coordination across multiple levels, multiple departments, and multiple technology schemes; if different systems cannot communicate effectively with one another, no matter how complete each system's individual functions are, it will be difficult to form a unified, efficient emergency response.

Organizationally, interoperability comprises both vertical and horizontal interoperability. Vertical interoperability refers to interconnection between emergency command authorities at different levels – the national, provincial, municipal, county, and on-scene command-post levels – with the core goal of achieving unified command and tiered dispatch, ensuring that instructions from higher levels can be issued quickly and that on-scene information can be relayed back in real time. Horizontal interoperability refers to coordinated communication capability between different departments at the same level – for example, joint operations at the same scene by police, fire, medical, transportation, and power authorities. Because these departments have long used different communication systems and technology schemes, achieving interoperability across different frequencies and standards has consistently been a prominent engineering challenge. In major incidents, a unified dispatch platform is often also needed to achieve cross-department resource coordination and centralized command.

As broadband and IP-based technologies advance, the scope of interoperability has expanded from traditional voice interconnection to comprehensive interconnection encompassing data, video, positioning, and service platforms.

6. Security Requirements

While carrying out critical command and rescue missions, emergency communication systems also face a higher level of security risk. Their security architecture generally needs to cover full-stack protection across the physical, network, transport, and application layers, combined with strict key-management and audit mechanisms, to ensure the system remains reliable and trustworthy in complex adversarial environments.

2.2 Typical Emergency Communication Application Scenarios and Service Requirements

ITU-R M.2377-2 divides emergency communication service capability into three tiers by data rate – narrowband, wideband, and broadband – each corresponding to different application scenarios and technical implementation

paths, providing an important reference framework for emergency communication requirements analysis and network planning. Narrowband services primarily support mission-critical voice communication and low-speed data transmission, emphasizing reliable access and dispatch efficiency; broadband services build on this by introducing image, video, and situational-data transmission capability to strengthen on-scene awareness and coordinated command; and broadband services extend further to high-definition video backhaul, remote control, and intelligent-application support, enabling comprehensive information fusion and decision support for complex scenarios.

2.2.1 Narrowband Application Scenarios

Narrowband emergency communication systems primarily carry voice communication and low-speed data services. They offer wide coverage, strong penetration, low power consumption, and long terminal standby time, and remain the primary means of public-safety communication in most countries worldwide today. [Table 11]](#tbl-2-11) lists typical narrowband emergency communication applications.

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Voice	Point-to-point	Selective calling and addressing	High	High	High
	One-to-many	Dispatch and group communication	High	High	High

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
	Direct/Direct Mode Operation	Infrastructure-free, short-range portable-to-portable group communication	High	High	High
	Push-to-talk (PTT)	Push-to-talk	High	High	High
	Instant access to voice channel	Push-to-talk with selective priority access	High	High	High
	Telephone interconnect	Two-way voice calling with wireline terminals	High	High	Medium
		Dispatcher console terminal	High	High	High
		Multi-select calling	High	High	High
	Computer-Aided Dispatch (CAD)	Computer-aided dispatch	High	High	High

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
	Security	Voice encryption/scrambling	High	High	Medium
Fax	Point-to-point	Status, short messages	Low	Low	High
	Emergency alert	Pressing an emergency button triggers an alert to a talk group or dispatcher	High	High	High
	Security	Data encryption/scrambling	High	High	High
	One-to-many (broadcast)	Initial dispatch alert (e.g., address, incident status)	Low	Low	High
Messaging	Point-to-point	Status, short message, short email	High	High	High

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
	One-to-many (broadcast)	Initial dispatch alert (e.g., address, incident status)	High	High	High
Safety	Priority/instant access	Person-down alert button	High	High	High
	Emergency alert	Pressing an emergency button triggers an alert to a talk group or dispatcher	High	High	High
	Emergency call	Priority voice call triggered by an emergency button	High	High	High
Location/Telemetry	Location status	Latitude/longitude information	High	Medium	High
	Sensor data	Vehicle telemetry/status	High	High	Medium

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
		On-scene electrocardiogram (EKG)	High	High	Medium
		Environmental information, including sensor data on air quality, temperature, pollution, radiation level, etc.	Medium	Medium	Medium
Database interaction (minimal record size)	Form-based record query	Access to vehicle license-plate records	High	High	Medium
		Access to criminal records/missing-person records	High	High	Medium

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
		Computer-aided dispatch direct to on-scene resources	Medium	Medium	Low
	Form-based incident reporting	Submitting an on-scene report	High	High	High

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

By service type, narrowband emergency communication traffic falls mainly into three categories: voice communication, short-data communication, and emergency alerting.

1. Voice Communication

Unlike public mobile communication, which centers on individual point-to-point calling, voice services in emergency scenarios place greater emphasis on group coordination, low latency, and high reliability, manifesting mainly as group calling, push-to-talk, direct-mode communication, and priority control.

(1) Group calling is the most representative service form. In public-safety and disaster-relief operations, commanders typically need to issue unified instructions to multiple on-scene personnel simultaneously, so the system must provide efficient one-to-many communication capability. Compared with traditional point-to-point communication, group calling significantly improves command efficiency and reduces the consumption of radio channel resources.

(2) Push-to-talk embodies the strict real-time requirements of emergency communication. After a user presses the PTT button, the system must complete link setup and floor (talk-permission) assignment within an extremely

short time.

(3) When infrastructure is damaged or network coverage is inadequate, the system must also support direct mode. In this mode, terminals can communicate directly with one another without going through a base station or core network, maintaining basic on-scene contact in complex environments such as building interiors, underground spaces, and mountainous areas. Direct-mode communication is generally regarded as the last line of defense for communication support at a disaster scene.

In addition, narrowband PPDR systems generally have priority access and preemption mechanisms. When network resources are constrained or congestion occurs, the system can prioritize the communication needs of high-priority users and emergency calls, interrupting lower-priority services when necessary to free resources for mission-critical communication — this priority mechanism is one of the important features distinguishing mission-critical communication from ordinary commercial communication.

2. Short-Data Communication

Beyond voice services, narrowband emergency communication systems also support low-speed data communication for transmitting status information, brief text, location data, and basic service queries. Such traffic is typically small in volume with moderate real-time requirements, but plays an important supporting role in emergency command and dispatch. Because narrowband systems have limited bandwidth, their data services are typically characterized by highly reliable, small-packet transmission.

(1) Status messaging is one of the most common data services. The system typically defines a set of standard status codes in advance, allowing on-scene personnel to quickly report their current status via the terminal. Compared with voice reporting, status messages consume fewer resources and transmit more efficiently, easing channel load during periods of heavy traffic.

(2) Short messaging provides more flexible text communication capability. Similar to SMS on public mobile networks, short messaging on emergency communication systems typically supports point-to-point sending, group broadcast, priority marking, and encrypted transmission, and can be used for dispatch notices, on-scene briefings, task instructions, and other brief messages. In some scenarios, short messaging also serves as an important supplement when voice communication is constrained.

(3) Location-information transmission is also an important part of nar-

rowband data service. On-scene terminals can periodically report location information to the command center, enabling real-time positioning and track tracking of personnel, vehicles, and equipment. Dispatchers can combine this with an electronic map to understand the distribution of on-scene forces, improving resource-dispatch and coordination efficiency. Beyond GNSS-based outdoor positioning, indoor or underground environments can also use base-station-assisted positioning, wireless ranging, and tag-based sensing to achieve location awareness.

Narrowband systems can also support basic data-query services; because of the limited data rate of narrowband systems, such services are typically presented as text, tables, or simplified graphics, rather than carrying high-bandwidth content such as complex images or video.

3. Emergency Alerting

Emergency alerting is one of the important characteristics of emergency communication systems, and an important way in which mission-critical communication differs from ordinary commercial communication. When frontline personnel face personal danger or a sudden emergency, they can quickly trigger an alerting mechanism via an emergency button on the terminal, obtaining a response from the command center and nearby rescue forces in the shortest possible time. Once triggered, the system typically automatically sends an emergency alert to the command center and preset users or groups, enabling commanders to quickly assess the on-scene situation and organize support. At the same time, the system can automatically establish an emergency voice link with the dispatch center, allowing commanders to monitor the on-scene environment and developments in real time, improving on-scene response efficiency.

Because emergency alerts typically correspond to high-risk incidents, related traffic generally uses the highest-priority transmission mechanism. When the network is congested or resources are constrained, the system can use priority access and resource-preemption mechanisms to prioritize the reliable transmission of alert traffic, ensuring that critical distress information reaches its destination in time. Some emergency communication systems also support covert alerting, in which the terminal does not produce a noticeable audible or visual indication while triggering the alert, avoiding exposing the act of alerting. Such mechanisms are important in high-risk scenarios, helping to improve the safety of on-scene personnel.

2.2.2 Wideband Application Scenarios

Wideband emergency communication systems support the full range of narrowband services while extending multimedia data capability, allowing on-scene personnel to access remote servers, transmit images, and send back video clips – providing richer information support for emergency decision-making. Table 12 lists typical wideband emergency communication applications.

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Messaging	Email, potentially with attachments	Routine email messages	Medium	Medium	Low
Privacy	Security	Data encryption/scrambling	High	High	High
Data direct/direct mode communication	Direct terminal-to-terminal communication requiring no additional infrastructure	Direct handheld-to-handheld, on-scene local communication	High	High	High
Database interaction (medium record size)	Form and record query	Access to medical records	High	High	Medium

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
		List of identified persons/missing persons	High	High	High
		Computer-aided dispatch direct to on-scene resources	High	Medium	Low
		Geographic Information System (GIS)	High	High	High
Text/file transfer	Data transfer	Submitting a report from an incident scene	Medium	Medium	Medium
		Criminal-records-management system information	Medium	Medium	Low
		Downloading legal information	Medium	Medium	Low

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Image transfer	Download/upload of compressed still images	Biometric identification (fingerprint, facial recognition)	High	High	Medium
		Identity photo (license-plate recognition)	High	High	Medium
		Building layout diagram	High	High	High
Telemetry	Location status and sensor data	Vehicle status	High	High	High
Over-the-Air Programming (OTAP)	Over-the-air programming	Programming a user device over the air	High	High	High
Security	Priority access	Critical care	High	High	High
Video	Download/upload of compressed video	Video clip	Medium	Low	Low

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
		Patient monitoring (may require a dedicated link)	Medium	Medium	Medium
		Live video feed of an ongoing incident	High	High	Medium
Interactive	Position determination	Two-way communication system	High	High	Medium
	Interactive location data	Interactive location data	High	High	High

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

As broadband mobile communication technology advances, emergency communication systems are no longer confined to traditional voice dispatch and low-speed data transmission, but are progressively gaining the ability to carry multimedia and data-intensive services. Compared with narrowband systems, wideband emergency communication supports higher data rates and richer service forms, meeting the higher bandwidth and latency demands of real-time database access, computer-aided dispatch, image and video transmission, and remote terminal management – significantly improving on-scene information gathering, situational awareness, and coordinated command.

1. Database Access and Computer-Aided Dispatch

Wideband emergency communication networks give on-scene personnel real-time access to back-end databases and business systems, extending

emergency response from traditional voice dispatch toward data-driven, visualized coordination and improving on-scene information-gathering efficiency and command decision-making. In medical emergency scenarios, for example, paramedics can use mobile terminals to access patient information in real time — including medical history, allergy history, and medication records — informing on-scene first aid and transport decisions; in fire-rescue scenarios, on-scene personnel can retrieve building floor plans, fire-protection-system layouts, and hazardous-material locations to optimize rescue routes and response plans; and in search-and-rescue operations, comparing personal characteristics found on scene against a missing-persons database can speed up identification.

Computer-aided dispatch (CAD) systems are an important part of modern emergency command, pushing incident type, location, task priority, response requirements, and personnel-assignment information directly to on-scene terminals for digital task delivery. Compared with traditional voice dispatch, CAD reduces omissions and misunderstandings in information transfer and improves cross-department coordination efficiency.

Geographic Information Systems (GIS) provide spatial-visualization support for emergency command. By combining location information with an electronic map, a GIS can display the location and status of on-scene personnel, vehicles, and equipment in real time, while overlaying key facility information such as hospitals, fire stations, shelters, and hazard sources — assisting commanders with resource allocation, route planning, and situational analysis. GIS has increasingly become one of the core support platforms for modern emergency communication command systems.

2. Image Transmission

Wideband emergency communication systems support the transmission of still images and picture data, giving on-scene personnel a more intuitive way to obtain, share, and analyze information. Compared with narrowband systems, which can carry only text and low-speed data, wideband networks support the real-time upload and download of higher-resolution images, significantly improving on-scene evidence collection, identity verification, and decision support.

One important application of image transmission is biometric identification. In law-enforcement and border-inspection scenarios, on-scene personnel can use portable terminals to capture fingerprint, facial, or iris biometric data

and upload it over the wireless network to a back-end database for rapid matching, enabling identity confirmation and screening of persons of interest. As AI-based recognition technology advances, image transmission has become an important foundation for mobile identity verification. In document-verification scenarios, on-scene terminals can photograph identification documents, driver's licenses, or vehicle license plates and, combined with back-end optical character recognition and database lookup, quickly verify personnel and vehicle information – reducing manual data entry and improving law-enforcement efficiency and accuracy.

Image transmission is also widely used for on-scene evidence collection and remote collaboration. Criminal investigators, accident investigators, or disaster-assessment personnel can transmit on-scene photos in real time to a rear command center or specialized technical department for expert remote analysis, supporting on-scene response. In major cases and complex disaster scenarios, this collaboration model of on-scene collection paired with rear-area analysis can effectively improve response efficiency.

In addition, wideband networks can support the transmission of building-structure diagrams, equipment-layout diagrams, and 3D models. Before entering a complex environment, professional rescue teams can obtain structural information about the target area in advance to develop action plans, plan rescue routes, and conduct tactical rehearsals, improving operational safety and coordination efficiency.

3. Video Transmission

Building on their higher data-transmission capability, wideband emergency communication systems can support video services, providing more intuitive information support for on-scene situational awareness and remote collaboration. Because of network-bandwidth and radio-resource constraints, such systems typically support the transmission of compressed video clips or low-bit-rate video services rather than continuous, large-scale high-definition video streaming.

One important application of video transmission is on-scene video evidence collection. For example, video clips captured by body-worn cameras, in-vehicle recording devices, or on-scene mobile terminals can be uploaded over the wideband network to a back-end system for storage, analysis, and evidentiary retention. This helps improve the efficiency of incident investigation, law-enforcement oversight, and accident review.

In medical emergency scenarios, video service can also support remote medical collaboration. Cameras and vital-sign monitoring equipment aboard an ambulance can transmit patient status information to a hospital, allowing remote specialists to understand the patient's condition in advance and provide remote guidance during on-scene first aid and transport. Because medical video traffic has stringent real-time and reliability requirements, practical deployments typically employ dedicated service assurance or priority mechanisms to reduce the impact of network congestion on service quality.

In addition, on-scene commanders can capture video of disaster scenes, accident areas, or key targets via mobile video terminals and send the compressed video back to the rear command center, providing an intuitive basis for remote situational assessment and command decisions. Compared with voice reporting alone, video information reflects the on-scene environment, disaster scale, and resource deployment more comprehensively, making it an increasingly important service form in modern wideband emergency communication.

4. Over-The-Air Programming (OTAP)

OTAP refers to remotely upgrading terminal software, configuring parameters, and updating functionality over a wireless communication network. Because PPDR terminals are numerous and widely distributed, manually maintaining them one by one is costly and slow, and struggles to meet the need for rapid, unified updates – making OTAP an important operations-and-maintenance capability of modern emergency communication systems.

The most common OTAP application is terminal software upgrading. The system can remotely fix software defects, optimize performance, or add new service functions over the wireless network, extending terminal life and improving system maintainability. Compared with traditional factory-return upgrades, OTAP significantly reduces equipment downtime and on-scene maintenance workload.

OTAP can also be used to remotely update terminal configuration parameters. For example, in response to organizational changes, changing task requirements, or network-optimization needs, the system can dynamically modify a terminal's frequency parameters, channel configuration, group information, and priority policy, ensuring consistency across large numbers of terminal configurations.

For security management, OTAP is also widely used to update encryption

keys and security parameters. The system can periodically push new authentication credentials or encryption keys to terminals, reducing the security risk associated with long-term key use and improving overall system security.

As wideband PPDR systems gain stronger data-carrying capability, OTAP can also support remote distribution of applications and service components – such as dynamically loading electronic maps, form templates, and on-scene law-enforcement applications – expanding terminal service capability.

2.2.3 Broadband Application Scenarios

Broadband emergency communication supports all narrowband and wideband services while also carrying advanced applications such as high-definition real-time video, remote robotic control, multimedia conferencing, and big-data analytics. Table 13 summarizes typical applications of broadband emergency communication systems.

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Direct-mode operation for video and data	Infrastructure-free direct video and data communication between units	Direct handheld-to-handheld, on-scene local command and control	High	High	High
Privacy	Security	Data encryption/scrambling	High	High	High

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Database access	Intranet/Internet access	Querying building architectural drawings, hazardous-material locations	High	High	High
	Web browsing	Browsing an emergency communication organization directory to look up phone numbers	Medium	Medium	Low
Robotic control	Real-time remote control of robotic equipment	Hazardous-material recovery robots, imaging/video robots	High	High	Medium

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Video	Video streaming, live video feed, download/upload of video clips, video conferencing	Wireless clip-on camera video communication used by firefighters inside a building	High	High	High
		Image- or video-assisted remote medical support	High	High	High
		Monitoring of an incident scene via fixed or remotely controlled robotic equipment	High	High	Medium
		Assessing a crime/-fire/flood scene from an aerial platform	High	High	Medium

Application	Functional Charac-teristic	Example	PP(1)	PP(2)	DR
		Multi-scene video dispatch	Low	High	High
		Multicasting multi-media from a base station to multiple users within a given area (e.g., point-to-multipoint/broadcast)	Low	High	High
		One-to-one, one-to-many video confer-encing, etc.	Low	High	High
		Encrypted video stream-ing	Medium	Medium	Medium

Application	Functional Characteristic	Example	PP(1)	PP(2)	DR
Real-time multimedia intelligence	Real-time optimization of video or other multimedia content	Optimizing allocated bandwidth to support multiple video streams	High	High	High
Imagery	Download/upload of high-resolution imagery	Downloading earth-observation satellite imagery	Low	Low	Medium
		Real-time medical imaging	Medium	Medium	Medium

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

Building on all narrowband and wideband services, broadband emergency communication achieves a qualitative leap in video communication capability.

1. Real-Time High-Definition Video

Real-time high-definition video is one of the most representative services of broadband emergency communication systems and an important technical means of enhancing the visualization capability of emergency command. Compared with traditional voice reporting, high-definition video conveys the on-scene environment, personnel status, and the unfolding of events more directly, significantly improving the accuracy and timeliness of command decisions. For example, rescue personnel can use helmet cameras or body-worn cameras to send a first-person view of the scene back to the rear command center in real time, letting commanders directly observe the on-scene environment, task execution, and changing risks, and improving remote

situational awareness and coordinated command. Drones, helicopters, and other aerial platforms can carry high-definition cameras to conduct aerial patrols and real-time video backhaul over disaster areas, traffic-accident scenes, or large-event venues, providing a macro-level view to support damage assessment, personnel search, traffic control, and security monitoring. In key areas, at major events, or in border-control scenarios, fixed cameras and vehicle-mounted camera systems can be deployed for continuous video surveillance, combined with intelligent analysis to automatically detect and warn of abnormal behavior, crowd gathering, or security risks. In remote areas or at disaster scenes, on-scene medical personnel can establish remote collaboration with rear-area medical experts via real-time video, supporting injury assessment, first-aid guidance, and remote consultation.

2. Remote Robotic Control

In high-risk environments, using remotely controlled robots in place of personnel can significantly reduce the risk of casualties during rescue and response operations. With advances in broadband communication, low-latency transmission, and intelligent control technology, robots have increasingly become important equipment in modern emergency communication systems. Rescue personnel remotely operate robots via wireless links to approach a target and perform tasks such as reconnaissance, retrieval, relocation, or disposal. Robots are typically equipped with high-definition cameras, robotic arms, and various sensing devices, and require real-time transmission of video, control commands, and status information, placing high demands on communication latency and reliability.

3. Video Conferencing and Multimedia Collaboration

Broadband emergency communication systems can support multi-party high-definition video conferencing and multimedia collaboration applications, providing important support for joint command across regions and departments. Compared with traditional voice dispatch, multimedia collaboration enables the simultaneous sharing of images, video, maps, documents, and other information, improving coordinated decision-making and command efficiency in complex incidents.

An on-scene command post can establish real-time video conferencing with the rear command center, specialized technical teams, and others, sharing on-scene footage, electronic maps, monitoring data, and emergency plans to support rapid assessment of the developing situation and coordinated

response. In major disasters or comprehensive sudden-onset incidents, multiple departments – police, fire, medical, transportation, environmental protection, and others – often need to respond jointly, and a video-conferencing system can support real-time, multi-department coordination, reducing layers of information transfer and improving unified command and resource-coordination efficiency. When complex technical issues arise on scene, subject-matter experts can be brought in via the video-collaboration system to remotely view the situation and provide professional guidance.

In major disasters or large-scale incidents, emergency communication networks often need to carry large volumes of high-definition video, audio, and multimedia data streams simultaneously, placing enormous pressure on wireless bandwidth and network processing capability. To maintain the continuity and transmission quality of critical services, broadband emergency communication systems typically need to combine intelligent video processing with dynamic resource scheduling to optimize bandwidth and prioritize multimedia services.

2.2.4 Trends in Service Requirement Development

Emergency communication application requirements are trending from narrowband toward broadband, from voice-only toward multimedia, and from traditional communication toward intelligent collaboration; the underlying technology base is likewise evolving from relatively independent dedicated communication networks toward a converged, intelligent, broadband emergency information infrastructure.

(1) Evolution from narrowband toward wideband and broadband. Emergency communication systems are evolving from narrowband trunking represented by TETRA and PDT toward wideband and broadband systems based on LTE and 5G. Narrowband systems will continue to carry mission-critical voice, group calling, and basic data services for some time to come, while broadband systems primarily carry video, multimedia data, and intelligent applications; the long-term coexistence and coordinated operation of both types of systems will be the mainstream pattern going forward.

(2) Evolution from voice-dominant toward video- and multimedia-dominant. Traditional emergency communication has centered on voice dispatch, but as broadband network capability improves, the importance of high-definition video, image transmission, and multimedia collaboration

continues to grow. Video information conveys on-scene conditions more directly and is increasingly becoming an important information source for emergency command, damage assessment, and remote collaboration.

(3) Evolution from information transmission toward intelligent analysis. Traditional emergency communication systems have mainly served an information-relay function, but the introduction of AI and edge computing is progressively giving communication networks real-time analysis and intelligent decision-support capability. For example, real-time recognition and analysis of video, image, and sensor data can automatically detect abnormal events, generate alerts, and support decision-making – improving emergency-response efficiency and situational awareness.

(4) Evolution from a single network toward multi-network convergence. Future emergency communication systems will place greater emphasis on coordination and convergence – between public and dedicated networks, between terrestrial and satellite networks, and between narrowband and broadband systems. Multi-mode, multi-band terminals and a unified dispatch platform can automatically select the most suitable access method based on network conditions, ensuring communication continuity and service reliability in complex or degraded network environments, and improving the robustness and survivability of the overall system.

2.3 Emergency Communication User Requirements Analysis

User requirements are the fundamental basis for planning, designing, and building emergency communication systems. During the handling of a sudden-onset incident, different response agencies have markedly different communication needs owing to differences in mission, working environment, and operational process – spanning both the routine communication needs of day-to-day public-safety operations and the special communication capabilities required under major disasters and sudden-onset incidents. Drawing on ITU-R M.2377-2 and reflecting the developing characteristics of emergency communication services, this book divides emergency communication user requirements into three categories: general requirements, broadband emergency communication requirements, and localized communication service requirements. General requirements address the basic communication capability needed across all emergency communication scenarios; broadband

emergency communication requirements focus on video, multimedia, and intelligent broadband service capability; and localized communication service requirements address the differentiated needs of different countries, regions, and industries with respect to institutional context, environment, and application scenario.

2.3.1 General Requirements

General requirements are the baseline capabilities that narrowband, wideband, and broadband emergency communication systems must all satisfy, spanning system design, security, cost-effectiveness, electromagnetic compatibility, operational control, coverage quality, grade of service, and interoperability, among other dimensions. Table 14 summarizes eight categories of general user requirements for emergency communication systems.

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
System	Support and integration of multiple service applications	Integrating multiple service applications (e.g., voice and low/medium-speed data) over a high-speed network, serving localized areas of intense activity	High	High
	Concurrent use of multiple service applications	Voice and data	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Multicast and unicast service		
		Real-time instant messaging		
		Mobile office functionality		
		VPN service		
		Telemetry		
		Remote control		
		Terminal positioning		
	Priority access	Tiered management of high- and low-priority service under heavy-traffic conditions, with traffic-peak shaving	High	High
		Accommodating increased traffic load during major operations and emergencies	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Dedicated frequency, or equivalent high-priority access to other systems	High	High
	Grade of service	Appropriate grade of service	High	High
	Quality of service	Quality of service	High	High
		Reduced response latency for establishing direct network links and retrieving information at a disaster scene, together with rapid authentication and verification of user identity and network permissions	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Reliability	Stable, reliable, and highly damage-resistant operating platform	High	High
		Stable, easy-to-operate management system	High	High
		Damage-resistant, reliable service carriage	High	High
		High availability	High	High
		Localized communication service, e.g., isolated-island base-station operation, relay-mode operation, Direct Mode Operation (DMO), device-to-device (D2D) direct communication	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Coverage	Full coverage across the emergency communication system's jurisdiction and operational area	High	High
		Full signal coverage of the jurisdiction and operational area for emergency response agencies at the national, provincial/-municipal, and local levels	High	High
		Dedicated systems capable of carrying peak service load and accommodating large fluctuations in traffic volume	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Improved system capacity in public-safety emergency and disaster-relief scenarios through techniques such as network reconfiguration and rapid activation of direct mode at high frequency	High	High
		Independently deployable portable base-station sites to support local on-scene networking	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Mobile sites capable of operating in either standalone-network or wide-area-network mode, to extend coverage and increase system capacity	High	High
		Air-to-ground communication	High	High
		Vehicle-mounted relay equipment (narrowband, wideband) for local-area signal coverage and gap-filling for portable-site networking	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Reliable indoor and outdoor coverage throughout, including bidirectional power amplifiers	High	High
		Full coverage of remote areas, underground spaces, and hard-to-reach areas, equipped with bidirectional amplifiers	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Appropriate redundancy to maintain service operation in the event of equipment or infrastructure failure, supporting independent, self-sufficient site operation and maintenance	High	High
	Capability	Rapid, dynamic system reconfiguration	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Communication control functions including centralized dispatch, access-permission control, dispatch talk-group configuration, service-priority setting, and forced-insertion preemption	High	High
		Robust, efficient operations-and-maintenance system supporting status monitoring and dynamic reconfiguration	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Internet Protocol compatibility (system-wide compatibility or interface-level compatibility)	Medium	Medium
		Highly reliable equipment, spanning hardware, software, and operations and maintenance	High	High
		Portable terminal equipment (supporting communication and transmission while mobile)	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Specialized-function communication equipment featuring high-volume audio output, compatibility with dedicated accessories (e.g., professional microphones), glove-friendly operation, adaptability to harsh environments, and long battery life	High	High
		Rapid call setup, supporting one-touch push-to-talk instant group calling	High	High
		Location services	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Air-to-ground and maritime communication, and control of uncrewed devices	Medium	High
		One-touch broadcast, group calling, and air-to-ground communication, able to issue announcements and rapidly establish sessions to all or selected talk groups	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Infrastructure-free direct terminal communication (direct mode, off-network two-way radio), compatible with vehicle-mounted relay equipment	High	High
		Emergency alerting: pressing an emergency button sends an alert to a talk group or dispatch console	High	High
		Emergency calling: pressing an emergency button initiates a high-priority voice call	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Audio/video call recording and monitoring, retaining audio/video call records for forensic tracing, security control, and after-action review	High	High
		Talk-group merging: combining multiple talk groups into a unified, system-wide call	High	High
		Interconnection with different tiers of the public network as needed	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Security-related requirements	End-to-end encrypted communication, supporting encrypted voice and data transmission for terminal interconnection, dispatch, and group calling	High	High	Low
Cost-related	Open standards	High	High	High
	Cost-effective solutions and supporting applications	High	High	High
	A fully competitive market for equipment and terminal supply	High	High	High
	Reduced scale of fixed network infrastructure deployment, leveraging equipment commonality and ubiquity	High	High	Low

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Electromagnetic compatibility	Emergency communication system operation in compliance with national electromagnetic-compatibility standards	High	High	High
Practical application	Application scenario	Support for practical application of emergency communication across all environments	High	High
		Deployable by public or private operators to support emergency and disaster-relief communication service	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Rapid deployment of systems and equipment, adaptable to major hazards, large events, and disaster emergencies (e.g., major fires, sporting events, peacekeeping missions)	High	High
		Two-way information exchange between frontline on-scene units and control centers and specialized analysis centers	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Further safeguarding personnel operational safety through improved communication effectiveness	High	High
	Compatibility	End-to-end direct interconnection	High	High
		Compatibility with existing public emergency communication networks (e.g., trunked two-way radio networks)	High	High
	Interoperability	Intra-system interoperability: support for shared use of network channels and/or talk groups	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
		Inter-system interoperability: promoting common functionality and interoperability capability across different systems	High	High
		Coordinated tactical communication among on-scene commanders from multiple emergency agencies	High	High
Spectrum use and management	Spectrum sharing with other terrestrial mobile-communication users	Low	Low	Medium
	Access to adaptable spectrum resources (narrowband, wideband, broadband channels)	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Minimizing interference to emergency and disaster-relief communication systems	High	High	High
	Improving spectrum-utilization efficiency	Medium	Medium	Medium
	Appropriately set channel spacing between mobile-station and base-station frequencies	Medium	Medium	Medium
Compliance	Compliance with applicable national laws and regulations	High	High	High
	Frequency coordination in border areas	High	High	Medium

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Cross-border coverage capability for emergency communication systems (contingent on bilateral agreements)	Medium	Medium	Medium
	Flexible activation of other service systems at major emergency scenes (e.g., HF, satellite, amateur radio)	Medium	High	High
	Adherence to the principles of the Tampere Convention	Low	Low	Medium
Overall planning	Reduced dependence on external resources (e.g., power, batteries, fuel, antennas)	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	On-demand availability of ready-to-use equipment (through inventory or facilitated access to larger equipment pools)	High	High	High
	Provision of national, provincial, and local (e.g., municipal) level systems	High	High	Medium

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Pre-coordination and pre-planning activities (e.g., designating specific channels for use during disaster-relief operations – not as a permanent dedicated assignment, but with priority use when needed)	High	High	High
	Maintaining accurate and detailed information accessible to emergency communication users in the field	Medium	Medium	Medium

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

1. System Requirements

System requirements primarily reflect the capabilities an emergency communication network must have with respect to coverage, basic functionality, service carriage, and operational assurance. An emergency communication

system should provide continuous, stable communication support throughout its jurisdiction, ensuring the network functions normally across different times, weather conditions, and incident scenarios, without a significant drop in service capability due to day/night variation, severe weather, or special periods. Compared with ordinary commercial communication networks, emergency communication networks place greater emphasis on reachability and service continuity under extreme conditions.

Emergency communication traffic is markedly bursty and uneven. Under everyday conditions, network traffic may be relatively low, but during a major disaster, large event, or mass-gathering incident, traffic volume and the number of user connections in a local area can grow sharply within a short period. Emergency communication systems therefore need the capacity to absorb sudden high-load scenarios, reserving sufficient network resources for critical services so that core services continue to operate normally even amid large swings in demand. Compared with commercial networks, which plan capacity mainly around average traffic, emergency communication networks place greater emphasis on assuring peak traffic and extreme scenarios.

During emergency response, a system often needs to carry voice dispatch, video backhaul, data query, and location reporting simultaneously, so it must support concurrent multi-service transmission and be able to flexibly adapt to different service types and rate requirements. Priority access and preemption are important features distinguishing emergency communication systems from public communication networks: the system should reserve critical resources for high-priority users and, when the network is congested, proactively compress or interrupt lower-priority services to prioritize the reliability of command dispatch and emergency communication. Grade-of-service assurance requires the system to meet high-reliability communication requirements on key metrics such as call-setup success rate, access latency, and dropped-call rate. At the same time, full coverage is one of the core requirements of an emergency communication system — not only conventional outdoor coverage, but also deep indoor coverage, underground-space coverage, and communication in remote rural or mountainous areas, ensuring that rescue personnel maintain stable communication in every environment. To meet the need for rapid response to sudden-onset incidents, the system should also support rapid link setup and rapid authentication, minimizing call-setup and terminal-access time so that lengthy authentication and access procedures do not hinder on-scene response. Quality-of-service requirements focus on the communication performance actually experienced by users, an

important indicator of service experience and operational usability. Compared with operational requirements, which emphasize network organization and resource-scheduling capability, quality-of-service requirements focus more on concrete performance measures such as latency, connection success rate, stability, and service continuity during communication.

In addition, in major disasters or when infrastructure has been damaged, emergency communication systems also need rapid-recovery and elastic-expansion capability, using mobile assets such as emergency communication vehicles, portable base stations, and drone relay platforms to quickly restore local coverage in the disaster area and increase on-scene communication capacity, keeping rescue units interconnected. Direct-mode operation allows terminals to communicate directly without relying on network infrastructure, serving as an important fallback when a base station fails or the network is disrupted. Vehicle-mounted or portable relay equipment can also serve as coverage-extension nodes, rapidly deployed at temporary command posts, forward rescue positions, and other key areas to provide local signal enhancement and relay. This kind of communication, with a degree of self-organizing and decentralized character, is important for on-scene communication support in mountain rescue, underground-space incidents, tunnel emergencies, and areas with severely damaged infrastructure.

2. Security Requirements

The information carried by emergency communication systems typically involves personnel safety, operational deployment, on-scene situational data, and other sensitive business data, so communication security requirements are correspondingly high. End-to-end encryption is the key technical means of ensuring communication confidentiality; it should keep voice, video, and data services protected throughout the entire transmission process, preventing eavesdropping, interception, or tampering by unauthorized parties. At the same time, terminals and the network should establish a mutual-authentication mechanism to prevent unauthorized terminal access, rogue-base-station spoofing, and identity impersonation, ensuring trusted network access and controlled identity.

Beyond protecting communication content, emergency communication systems also need robust access control, permission management, and security-audit capability, applying tiered management to different agencies' and users' network-access permissions and scope of service use, and recording and tracing key operations to strengthen overall system security. For critical

infrastructure and core nodes, measures such as firewalls, intrusion detection, link encryption, and key management should also be applied to strengthen resistance to cyberattacks and malicious destruction.

In routine public-safety operations and major-event security scenarios, security requirements are typically high-priority, since the relevant tasks often involve law-enforcement coordination, crowd control, VIP protection, and other highly sensitive missions requiring strong communication confidentiality and system trustworthiness. In major disaster-relief scenarios, by contrast, where multiple departments, social organizations, and even international rescue forces often need to participate jointly, the system places greater emphasis on rapid access and wide-area interconnection, requiring a balance between security and reachability so that overly complex encryption and authentication procedures do not hamper cross-agency coordination efficiency. Even in an open rescue environment, however, an emergency communication system still needs the necessary security protections to prevent malicious interference, unauthorized access, and tampering with critical information.

3. Cost Requirements

Cost-effectiveness is an important constraint on the long-term, stable operation of an emergency communication system. Emergency communication networks typically have long construction cycles, wide coverage, and large numbers of devices, and their cost includes not only network construction and equipment procurement but also subsequent operation and maintenance, system upgrades, spectrum use, and personnel training. Under the premise of meeting reliability and security requirements, controlling the system's full life-cycle cost is therefore an important issue in emergency communication system construction.

Adopting open standards and internationally common technology systems is an important way to lower construction and operating costs. Standardization creates a large-scale industrial ecosystem, promotes multi-vendor equipment compatibility and market competition, and thereby lowers equipment-procurement and maintenance costs while avoiding vendor lock-in caused by closed, proprietary technology. The system should also have good backward compatibility and sustainable evolution capability, allowing old and new systems to coexist and interoperate over the long term, achieving technological evolution through smooth upgrades and avoiding forced network-wide rebuilds driven by technology renewal.

Diversifying equipment and the supply chain is likewise an important safeguard for cost control and supply security. Supporting equipment access from multiple vendors reduces dependence on any single supplier and strengthens the system's stability and sustainability amid supply-chain volatility or geopolitical risk. In addition, emergency communication systems need to support multiple types of terminal equipment – handheld terminals, vehicle-mounted terminals, individual-soldier equipment, command terminals, and drone-mounted communication terminals – to meet different mission-scenario needs. Terminal equipment should be cost-controlled while meeting reliability, ruggedization, and specialized-function requirements, avoiding the high cost of large-scale deployment caused by overly complex designs.

4. Electromagnetic Compatibility Requirements

Emergency communication systems typically operate in a complex electromagnetic environment dense with spectrum resources and populated by multiple coexisting wireless systems, so electromagnetic compatibility (EMC) performance directly affects network stability and reliability. System equipment must meet relevant EMC standards and regulatory requirements, passing certification testing for electromagnetic radiation, conducted emissions, and interference resistance – both to avoid causing harmful interference to other lawful radio services and to ensure the equipment itself can operate stably and continuously in a complex electromagnetic environment.

Electromagnetic compatibility issues arising from the coexistence of multiple networks, standards, and devices are especially prominent in emergency communication scenarios. Within a single emergency command structure, narrowband trunking systems, wideband dedicated networks, satellite communication, HF communication, and public-network access systems are often deployed simultaneously; different bands and standards require unified coordination in frequency planning, spatial isolation, and transmit-power control to reduce the impact of intermodulation interference, adjacent-channel interference, and receiver blocking on communication quality.

In major-event security and disaster-relief scenarios, large numbers of communication devices may be densely deployed within a limited space – for example, in a temporary command post, an emergency communication vehicle, or a mobile command platform – where high-density concurrent operation of wireless equipment readily produces a complex electromagnetic coupling environment. Reasonable antenna layout, RF isolation, filtering, and power

control are therefore needed to strengthen the system's overall interference resistance and ensure that critical-service communication remains reliable under intense electromagnetic conditions.

5. Operational Requirements

Operational requirements focus mainly on an emergency communication system's service-assurance capability, network stability, and dispatch-control capability during actual operation, and are an important measure of the system's practical, field-ready performance. Emergency communication traffic typically demands strong real-time performance and high reliability, with push-to-talk (PTT) being one of the most essential characteristics of trunked communication. The system should be able to establish a communication link quickly after a user initiates a call, completing voice transmission within an extremely short time to meet the real-time needs of on-scene coordination and command dispatch.

Network load in emergency scenarios is often bursty and highly concentrated. During a major disaster, mass incident, or large-event security operation, a large number of users may access the network simultaneously within a short period, frequently initiating group calls and data services. The system therefore needs strong high-load carrying capacity, maintaining basic communication capability for critical services under extreme concurrency and avoiding overall service failure due to network congestion. At the same time, the system should maintain a high call-setup success rate and service availability, ensuring that key users and important services can access the network stably even in complex environments.

Under disaster conditions, some communication infrastructure may fail due to power outages, transmission-link interruption, or equipment damage, so the system also needs strong service continuity and fault-recovery capability. Through core-network redundancy, automatic link switchover, coordinated base-station coverage backfill, and rapid deployment of mobile communication assets, basic communication service can be maintained even when part of the network is damaged, improving overall system resilience.

Interoperability is one of the key requirements in building an emergency communication system and an important foundation for cross-department, cross-region coordinated response. Compared with ordinary commercial communication networks, emergency communication often involves coordination across multiple agencies, multiple networks, and different technology

schemes, so interoperability capability affects not only whether communication is possible but also directly influences the efficiency of unified command and coordinated operations. Interoperability requirements cover not only interconnection between networks but also compatibility and coordination across different standards, different bands, and different generations of systems.

In addition, emergency communication systems need flexible, efficient communication management and dispatch-control capability, including dynamic group-call management, priority control, cross-system coordination, dynamic resource allocation, and service rerouting under fault conditions. Through real-time control of communication resources and business processes, dispatchers can quickly adjust the communication organization according to on-scene conditions, improving the efficiency of emergency command and coordinated response.

6. Spectral Efficiency Requirements

Spectrum is one of the most essential and scarcest resources for any wireless communication system. Although emergency communication systems typically have dedicated bands or priority spectrum-use rights, the allocable bandwidth is limited while service types and user numbers continue to grow, so the system still needs to improve spectrum-utilization efficiency as much as possible, achieving greater network capacity, wider coverage, and higher data-carrying capability within limited bandwidth. Improving spectral efficiency generally requires a combination of wireless-technology measures. For example, higher-order modulation and coding improve data-transmission capability per unit of bandwidth; multi-antenna technology and spatial multiplexing improve system capacity and transmission rate within the same spectrum resources; and cell splitting, heterogeneous networking, and frequency reuse improve the spatial reuse efficiency of spectrum. In addition, dynamic spectrum access and spectrum sharing are increasingly important directions for improving spectrum utilization – while preserving emergency communication's priority-use rights, idle spectrum resources can be shared with other services under non-emergency conditions, reducing the problem of chronically low utilization of dedicated spectrum.

7. Compliance Requirements

Compliance requirements are an important foundation for the construction and operation of an emergency communication system, ensuring the

system meets national laws and regulations, international rules, and industry standards with respect to frequency use, equipment deployment, network operation, and information security, while also enabling cross-region, cross-industry, and even cross-border coordination. Compliance affects not only whether the system can operate legally but also directly influences the network's long-term sustainability and international-cooperation capability.

Compliance with national laws and regulations is a basic precondition for building and operating an emergency communication system. Countries generally maintain strict regulatory regimes covering radio-frequency use, equipment type approval, electromagnetic compatibility, electromagnetic-radiation protection, network security, and data security. During the planning, construction, deployment, and operation of an emergency communication system, these regulatory requirements must be met to ensure lawful, compliant network operation and to avoid causing harmful interference to other radio services. Because emergency communication carries public-safety responsibilities, its compliance requirements are generally stricter than those of ordinary commercial communication systems.

Frequency coordination is also an important part of compliance requirements, particularly in border areas or cross-region coordination scenarios, where an emergency communication system's spectrum may become coupled with that of a neighboring region or country. Without unified planning and coordination, this can readily produce cross-border co-channel or adjacent-channel interference that disrupts normal operation. When deploying emergency communication networks in border areas, frequency coordination is therefore typically carried out under international radio regulations and bilateral or multilateral coordination mechanisms, reasonably planning frequency-use schemes and transmission parameters to keep all parties' communication systems operating stably.

In addition, compliance requirements also include adherence to emergency communication technical standards and industry norms. Adopting international or regional common standards improves system compatibility, interoperability, and industry-chain maturity, providing a technical foundation for cross-department coordination and international joint rescue operations. At the same time, network security, data protection, and personal-privacy requirements must also be satisfied to ensure the emergency communication system operates securely, reliably, and controllably in complex environments.

8. Overall Planning Requirements

Overall planning requirements focus mainly on the overall coordination, long-term sustainability, and assurance capability of emergency communication system construction under extreme conditions, emphasizing that network operation, resource assurance, disaster response, and future evolution be fully considered at the planning and design stage, so the system does not become destabilized by over-reliance on any single external condition.

Improving the system's ability to operate independently and reducing dependence on external factors in critical areas is an important principle for strengthening an emergency communication system's damage resistance and sustained-support capability. After a major disaster or extreme event, commercial power, transportation, fuel supply, and public communication infrastructure may all be damaged simultaneously; if the system relies too heavily on external resources, its overall communication capability will rapidly degrade. Emergency communication systems therefore need a degree of self-sufficiency in energy, transport, siting, and core-network functions.

For power assurance, systems generally need extended backup power and diverse energy sources — high-capacity batteries, mobile generators, and auxiliary sources such as solar and wind power — to reduce dependence on the commercial grid and ensure sustained operation during extended outages. Necessary fuel reserves and emergency resupply mechanisms are also needed to keep emergency generators running throughout a disaster.

In terms of network architecture, emergency communication systems should strengthen localized operating capability wherever possible — for example, by building local core networks, edge-computing nodes, and regional service platforms — to reduce reliance on remote, centralized data centers and long-distance transmission links. When external backhaul links are disrupted, the local network can still maintain critical services, preserving basic voice dispatch and data communication.

In addition, equipment and infrastructure planning must fully account for overall reliability and maintainability. Integrated equipment design, redundant configuration of key components, and mobile-deployment capability, for example, improve the system's survivability and rapid-recovery capability in harsh environments. Overall planning is not simply a network-construction issue — it involves the coordinated design of energy assurance, resource reserves, operations and maintenance, and emergency plans, and is an important foundation for building a highly reliable emergency communication system.

2.3.2 Broadband Emergency Communication Requirements

Broadbandemergency communication requirements build on the general requirements to define enhanced capabilities for broadband multimedia application scenarios. As emergency communication evolves from narrowband voice toward broadband multimedia, services such as real-time video backhaul, high-definition image transmission, geographic-information-system applications, and large-capacity database queries place higher demands on network bandwidth, latency, and security. Table 15 summarizes user requirements for broadband emergency communication.

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Multi-service fusion and collaborative use	Converging voice, data, video, and other services over a high-speed network to meet communication needs in high-load on-scene operational areas	High	High	Medium
	On-scene video transmission	High	High	Medium
Quality of Service (QoS)	Support for a range of priority service levels	High	High	High
	Guaranteed throughput	High	High	High
	Rapid session setup	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Coverage	Maximizing frequency-reuse efficiency in the radio access network	High	High	Medium
	Vehicle-mounted broadband relay equipment for signal coverage of local areas and mobile sites	High	High	High
Capability	System-level network management and control capability	Medium	High	High
	Basic network self-healing capability, rapidly restoring service and returning to redundant operation	High	High	High
	Packet data transmission capability	High	High	High
	Rapid deployment capability for base-station facilities and terminal equipment	Low	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Seamless coverage via network handover, sustaining stable communication links for stationary use and for mobility up to 120 km/h within 95% of the coverage area	High	High	High
	Unified common air interface across the mobile broadband network	High	High	High
	Rated transmit power of 0.25 W EIRP (24 dBm) for mobile and portable equipment; in rural scenarios, portable equipment transmit power not to exceed 3 W EIRP (34.8 dBm)	Low	Low	Low

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Support	Round-the-clock operations-and-maintenance assurance for fixed equipment and user terminals	High	High	High
	24/7, year-round staffing at the network operations-and-maintenance center	High	High	High
	Round-the-clock operations-and-maintenance mode with on-demand on-scene support to keep the network stable and available, together with a 7×24 customer-service hotline for issue handling and technical assistance at any time	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Reliability and adaptability	Adaptability to extreme natural and electromagnetic environments; the network should not experience functional failure under conditions such as weather disasters, operational vibration, seismic activity, electromagnetic interference/electrostatic discharge, or abnormal power supply	High	Medium	Low

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Fixed, mobile, and terminal equipment able to adapt to a range of natural-environment conditions; the physical facilities supporting network equipment should comply with applicable standards for surge suppression, grounding, and electromagnetic-pulse protection	High	High	High
	Highly robust network architecture	High	High	High
	Network self-management capability	High	High	High
	Establishment and coordination of business-continuity plans	High	High	High
	Elastic service-provisioning capability	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	High-availability design, e.g., link or equipment diversity, redundant deployment, automatic fault-switchover protection, and backup operating procedures	High	High	High
	Network and operational testing to confirm that, after a fault interruption, data and call-processing functions can be restored within a prede-termined, assured time	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The above measures should ensure that the emergency communica-tion broadband network achieves at least the robustness level of current public-safety land-mobile radio systems	High	High	High
Availability	Service-availability metrics should not be computed on the assumption that a single service area may experience a prolonged outage	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Power assurance via battery backup and/or standby generation, with redundant backhaul links deployed between the radio access network and the core network and between base stations; base-station towers should have strong wind resistance, with a long-term system-availability target of up to 99.995%	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Each network element should have extremely high reliability (e.g., 99.999%) and reduce mean time to repair (MTTR) through adequate spare-parts supply and convenient maintenance support; system operation should remain uninterrupted even during maintenance windows	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Redundant equipment and network elements should automatically detect failures in the active component and automatically switch over to take on the service upon primary-equipment failure, ensuring service continuity	High	High	High
	Service-availability metrics should not be computed on the assumption that a single service area may experience a prolonged outage	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Security	Support for end-to-end encryption. The network should provide cryptographic protection mechanisms ensuring that communication content can be decrypted only by authorized recipients, including encrypting data on all wireless links	High	High	Low
	Support for domestic (national) cryptographic algorithms	High	High	Low
	Encryption mechanisms should support both point-to-point and point-to-multipoint communication	High	High	Low

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The network should support periodic renewal of terminal keys, and should be able to switch service encryption keys without requiring terminal re-authentication or interrupting service	High	High	High
	The network should provide integrity-protection mechanisms to ensure received data has not been tampered with in transit	High	High	Low
	Only users and/or devices explicitly authorized by the emergency communica-tion management authority may access public-safety services and applications	High	High	Medium

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The network should require all terminals attempting to connect to complete identity authentication before obtaining network resources. Each terminal should have a unique identifier, and the authentication mechanism should provide high-confidence identity verification – e.g., via public-key cryptography – without requiring user interaction	High	High	Medium
	Terminal authentication service should use open standard protocols	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	To prevent attacks from malicious terminals or rogue base stations, the authentication mechanism should support mutual authentication, whereby the terminal proves its identity to the network and the network also proves its legitimacy to the terminal	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Each emergency communication management authority should be able, as needed, to further enable user-identity authentication on top of terminal authentication. When user authentication is enabled, the network should verify user identity before authorizing access	High	High	High
	For agencies that enable user authentication, the network should support sequential multi-user authentication and switching on the same terminal	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Support for system authorization management, allowing each agency to control its own authorization policy via a management interface	High	High	High
	For agencies that enable user authentication, user-account addition, removal, and permission management should be supported via a management interface (e.g., a web management portal)	High	High	High
	For agencies requiring user-identity verification, the network should support a single device completing sequential authentication of multiple users	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The network should have an independent emergency communication core network	High	High	High
	Support for third-party key-management systems	Low	Low	Low
	The network should log all device and user access attempts, along with authentication, authorization, and permission-change operations	High	High	High
	Support for over-the-air key updates	Low	Low	Low
	The network should support a configurable connection-timeout mechanism to limit continuous terminal-connection duration	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The network should support an idle-timeout mechanism that automatically disconnects terminals with no traffic for an extended period	High	High	High
	Each emergency communica-tion management authority should be able to independently configure timeout and idle parameters for its own terminals	High	High	High
	Each agency should also be able to manually force termination of its own terminals' network access and active sessions via a management interface	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	The network should have attack-detection capability, able to detect and alert on abnormal behavior and potential security attacks	High	High	High
Requirements for preventing unauthorized terminal use	Devices must support the network's device-authentication protocol, with each device configured with a unique identifier; identity verification uses highly reliable methods such as public-key cryptography, requiring no manual operation	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Mutual authentication is used to prevent illegitimate terminals and rogue base stations from gaining access; the terminal verifies its identity to the network and the network also authenticates itself to the terminal, with the terminal barred from accessing the public emergency communica-tion network if network authentication fails	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Each emergency agency may independently choose whether to enable user-access authentication; if enabled, users must complete identity verification before they can use terminal services or invoke network resources	High	High	High
	Devices support complete data wiping, following industry standards for multi-pass overwriting of storage media to destroy all data on the device	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Devices have built-in local data encryption; retrieving decrypted data requires user-identity verification	High	High	High
Cost	Elastically scalable system	Low	High	Medium
	Open system architecture	High	High	High
	Support for public and private operators to independently or jointly build and deploy emergency communica-tion service	High	High	Medium

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
Interoperability	Interoperability and interconnection with narrowband trunking communication systems, including interfaces between RF subsystems and supplementary dispatch-console interfaces for voice and supplementary services	High	High	High
	Interoperability with other broadband systems	High	High	High
	Interoperability with satellite communication systems	High	High	High
	Interconnection with various information systems	High	High	High
	Configuration with standard interfaces for connecting to other communication systems	High	High	High

User Requirement	Specific Requirement	PP(1)	PP(2)	DR
	Application interfaces conforming to common standard specifications	High	High	High
	Tiered inter-connection with public telecommuni-cation networks such as fixed and mobile networks, as needed	Medium	Medium	Medium
Spectrum use and management	Dynamic spectrum allocation	High	High	High
	Sufficient available spectrum resources configured, providing a broadband channel that meets the maximum uplink rate	High	High	High
	Flexible allocation of uplink/down-link bandwidth and rate	High	High	High

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

Broadband emergency communication requirements build on the general requirements, defining enhanced capabilities aimed at multimedia services and broadband application scenarios. Unlike traditional narrowband trunking systems, which primarily carry voice dispatch and low-speed data, broadband emergency communication systems are based on an IP packet-switched architecture and use cellular broadband technologies such as LTE and 5G, supporting real-time video backhaul, high-definition image transmission, geographic-information-system applications, large-capacity database access, and multimedia collaborative command – significantly improving on-scene situational awareness and overall command capability.

The introduction of broadband and IP-based technology also exposes emergency communication systems to a more complex network environment and technical challenges. On one hand, because broadband networks are highly integrated with the wider internet, the system must guard against cyberattacks, malicious intrusion, data theft, denial-of-service attacks, and other network-security threats, in addition to fulfilling traditional wireless-communication functions, requiring a more comprehensive network-security and access-control mechanism. On the other hand, voice, video, image, and data services differ significantly in their requirements for latency, bandwidth, packet loss, and reliability, requiring a fine-grained QoS mechanism for traffic classification, priority scheduling, and dynamic resource allocation to ensure mission-critical services remain reliably assured even when the network is congested.

In addition, the network scale, equipment count, and system complexity of broadband emergency communication systems are all significantly higher than those of traditional narrowband systems. Unified operation and maintenance of large numbers of base stations, the core network, edge nodes, and multiple types of terminals places higher demands on network-management capability. Systems typically need remote operation and maintenance, centralized monitoring, self-healing, and over-the-air upgrade capability to reduce maintenance cost and improve operational efficiency.

Broadband systems also have more pronounced spectrum demands. High-definition video, real-time multimedia, and large-capacity data services significantly increase the load on wireless links, while spectrum available for emergency communication is typically limited – requiring carrier aggregation, multi-antenna technology, dynamic spectrum sharing, and heterogeneous networking to improve spectrum-utilization efficiency and system capacity,

meeting the demand for concurrent multi-service transmission within limited spectrum.

Interoperability and coordination with commercial 4G/5G networks is also an important characteristic that distinguishes broadband emergency communication from traditional narrowband trunking systems. Broadband emergency communication typically adopts a technology base similar to commercial cellular networks and can achieve coordinated operation through dedicated networks, priority access to public networks, network slicing, or hybrid networking, ensuring the reliability of mission-critical services while fully leveraging the broad coverage and mature industrial ecosystem of commercial networks.

At the same time, technologies such as airborne base stations, satellite-communication backhaul, and space-air-ground integrated networking are increasingly becoming important components of the broadband emergency communication system. When ground backhaul links are disrupted or disaster-area communication infrastructure is severely damaged, satellite links can establish a connection to external networks, and aerial platforms such as drones, tethered balloons, and helicopters carrying temporary base stations can be used to rapidly restore coverage and communication access in the disaster area – improving the system's ability to sustain communication support under extreme conditions.

2.3.3 Localized Communication Service Requirements

Localized communication service refers to technical mechanisms – direct terminal-to-terminal communication, isolated-island base-station operation, or relay mode – that provide local-area communication capability when base-station coverage is limited or infrastructure has failed. Table 16 summarizes user requirements for localized communication service.

Localized Communication Service	Attribute	D2D/DMO (Isolated)	Isolated Base Station – Connected to Core Network	Isolated Base Station – Isolated from Core Network	Relay Mode – Connected to Core Network	Relay Mode – Isolated from Core Network
Voice	Person-to-person	High	High	High	High	High
	One-to-many	High	High	High	High	High
	Push-to-talk	High	High	High	High	High
	Priority	High	High	High	High	High
	Encryption	High	High	High	High	High
	Emergency PTT	High	High	High	High	High
Multimedia (Voice+Video+Data)	Person-to-person	High	High	High	High	High
	One-to-many	High	High	High	High	High
	One-touch multimedia	High	High	High	High	High
	Priority	High	High	High	High	High
	Encryption	High	High	High	High	High
	Real-time video	High	High	High	High	High

Localized Communication Service	Attribute	D2D/DMO (Isolated)	Isolated Base Station – Connected to Core Network	Isolated Base Station – Isolated from Core Network	Relay Mode – Connected to Core Network	Relay Mode – Isolated from Core Network
Text messaging/instant messaging	Person-to-person	High	High	High	High	High
	Emergency alert	High	High	High	High	High
	One-to-many	High	High	High	High	High
Multimedia messaging/instant messaging content	Point-to-point	High	High	High	High	High
	One-to-many	High	High	High	High	High
	Standard-definition audio/video	High	High	High	High	High
	High-definition audio/video	Medium	High	High	Medium	Medium

Localized Communication Service	Attribute	D2D/DMO (Isolated)	Isolated Base Station – Connected to Core Network	Isolated Base Station – Isolated from Core Network	Relay Mode – Connected to Core Network	Relay Mode – Isolated from Core Network
	Presence/status awareness	High	High	High	High	High
Database interaction	(n/a)	High	Low	High	(n/a)	(n/a)
Location	Interactive location data	High	High	High	High	High
File transfer	(n/a)	High	High	High	High	High
Client/server architecture applications	(n/a)	High	Low	High	(n/a)	(n/a)
Peer-to-peer-architecture applications	(n/a)	High	High	High	High	High

Localized Communication Service	Attribute	D2D/DMO (Isolated)	Isolated Base Station – Connected to Core Network	Isolated Base Station – Isolated from Core Network	Relay Mode – Connected to Core Network	Relay Mode – Isolated from Core Network
Other requirements	Over-the-air software/firmware/hardware upgrade	(n/a)	Medium	(n/a)	Medium	(n/a)
	Online update of geographic-information maps	(n/a)	Medium	(n/a)	Medium	(n/a)
	Automatic telemetry-data collection	(n/a)	Medium	(n/a)	Medium	(n/a)
	Ad hoc hotspot networking in disaster/incident areas	High	High	High	High	High

Localized Communication Service	Attribute	D2D/DMO (Isolated)	Isolated Base Station – Connected to Core Network	Isolated Base Station – Isolated from Core Network	Relay Mode – Connected to Core Network	Relay Mode – Isolated from Core Network
	Emergency alerting and group paging	High	High	High	High	High

Note: PP(1) denotes day-to-day operations, PP(2) denotes a major incident/public event, and DR denotes disaster relief.

Localized communication service requirements reflect an emergency communication system's damage resistance, self-organizing capability, and sustained-support capability under extreme conditions; their core objective is to preserve, at minimum, critical communication capability even when infrastructure is partially or entirely lost. Unlike a traditional cellular network, which relies on a centralized "terminal–base station–core network" architecture, localized communication places greater emphasis on decentralization, survivability, and on-scene self-sufficiency, making it one of the key features distinguishing emergency communication from ordinary public communication networks.

Such requirements stem primarily from the special nature of disaster and emergency scenarios. Earthquakes, floods, typhoons, and other disasters, for example, can cause base-station power loss, transmission-link interruption, or core-network failure; rescue personnel entering underground spaces, tunnels, or building interiors may lose normal cellular coverage; and mountainous, maritime, and desert areas may inherently lack well-developed communication infrastructure. In these situations, communication approaches that depend on a fixed network architecture struggle to keep working, making localized

communication mechanisms essential for sustaining on-scene coordination and command capability.

Localized communication service is typically implemented through several technical mechanisms. First, Device-to-Device (D2D) communication, or Direct Mode Operation (DMO), allows terminals to establish a communication link directly, bypassing the base station, enabling point-to-point or point-to-multipoint communication when the network has failed or coverage is absent – the most fundamental fallback communication method for on-scene personnel. Second, isolated-island operating mode allows a base station that has lost its connection to the core network to continue operating independently on local resources, providing basic voice dispatch, short-message, and data-communication capability to users within its coverage area, thereby sustaining communication service in a local area. Third, relay mode can use dedicated relay equipment, vehicle-mounted platforms, or even ordinary terminals as relay nodes to extend wireless coverage or connect isolated communication areas, achieving interconnection between different local networks.

These mechanisms can operate either independently or in coordination with one another, together forming the localized support system that sustains an emergency communication system under extreme conditions. Through this decentralized, self-organizing communication capability, an emergency communication network can maintain the continuity of critical communication services even when infrastructure is damaged, backhaul is interrupted, or coverage is missing – providing a last line of communication support for on-scene rescue and emergency response.

References

[1] ITU-R. M.2377-2 Radiocommunication objectives and requirements for public protection and disaster relief [R]. Geneva: ITU, 2023.

[2] ITU-R. M.2033 Radiocommunication objectives and requirements for public protection and disaster relief [R]. Geneva: ITU, 2003.

[3] ITU-T. Y.1271 Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks [S]. Geneva: ITU, 2014.

[4] 3GPP. TS 22.179 Mission Critical Push to Talk (MCPTT) over LTE; Stage 1 [S]. Sophia Antipolis: 3GPP, 2020.

Chapter 3: Emergency Communication System Architecture

The engineering realization of an emergency communication system is, in essence, a complex problem of system-of-systems design. This chapter proceeds from the architectural level, systematically analyzing the logical organization of the functional components within an emergency communication system, the networking modes used at different geographic scales and mission phases, the way space-ground integrated communication architectures are constructed, the mechanisms for interconnection and interoperability among heterogeneous communication systems, and the supporting role that plans and drills play in the reliable operation of the overall system. The chapter first establishes a layered reference model for emergency communication systems, providing a unified framework for positioning the functions of various communication components and for system-level analysis — this forms the basis for understanding everything that follows. Building on this foundation, the chapter systematically analyzes emergency communication networking modes, dividing them by coverage range and application scenario into three basic types — wide-area relay, on-site regional relay, and on-site access — and analyzes the applicable scenarios and selection principles for each type of technical approach. The chapter then turns to the long-standing engineering challenge of heterogeneous network interoperability, systematically presenting the technical paths toward multi-system collaborative communication from the perspectives of standardization frameworks, engineering implementation techniques, and public–private network convergence mechanisms. Finally, from the perspective of institutionalized management and capability building, the chapter introduces the structure and drafting methodology of communication support emergency plans, the mechanisms for drill evaluation and continuous improvement, and further analyzes the impact of digital technologies on the evolution of emergency plan management and drill practice.

3.1 Emergency Communication Command Reference Model

The emergency communication command reference model establishes the basic hierarchical structure, core functional elements, and their interrelationships for an emergency communication command system, forming a unified abstract framework for describing the emergency communication command system as a whole. Establishing such a reference model serves two purposes. On one hand, it provides a common thread for technical research, allowing work in wireless communication, computer networks, Geographic Information Systems (GIS), data fusion, and other technology domains to be positioned and related within a single framework. On the other hand, it provides a common point of reference for system construction, giving different levels of government and different departments a shared functional vocabulary when planning and building emergency communication command systems. In addition, the reference model helps reveal the dependencies among the various components of the system and their shared capability requirements, making it possible to identify capability gaps and critical bottlenecks from a system-wide perspective.

3.1.1 Characteristics of Emergency Communication Command

Compared with other information systems, emergency communication command systems have clear distinguishing characteristics in their application scenarios, system organization, and operating mechanisms. Because they are oriented toward the handling of sudden-onset incidents – a highly dynamic and uncertain environment – their design must not only meet communication and command requirements under complex conditions, but must also adapt to multi-department coordination, interoperability among heterogeneous systems, and rapid reconfiguration of resources.

(1) **Diversity of application requirements.** Sudden-onset incidents are complex in type, and highly uncertain in terms of when and where they occur, their nature, and their severity, so the functional requirements placed on the emergency communication command system differ markedly from scenario to scenario. In most general incidents, dedicated (private) networks and public communication networks typically operate side by side; in large-scale disaster scenarios where public network infrastructure has been severely damaged, the

private network often has to independently carry the entire communication load of the response; and in scenarios such as security support for major events or individual emergency calls for help, the public network becomes the primary provider of communication services. The operating mode and emphasis of the same system can vary considerably across these different scenarios, so the system must possess a high degree of flexibility, adaptability, and configurability.

(2) **Heterogeneity of system composition.** Responding to a sudden-onset incident typically involves coordinated action among multiple departments – public security, fire and rescue, medical services, transportation, electric power, and others – and because each department has followed its own historical development path and has its own operational requirements, they often adopt different technical standards and communication protocols, resulting in strong specialization and compatibility differences among systems. At the same time, information and communication technology evolves rapidly, so old and new systems coexist over extended periods. For example, at the same disaster site, the fire department might use a TETRA system, the public security department a PDT trunking system, and medical rescue teams might rely on public 4G/5G terminals, with no direct interoperability among these systems. This state of heterogeneous coexistence is a reality that emergency communication command systems must confront over the long term.

(3) **Virtuality of system resources.** Major sudden-onset incidents often require the rapid on-site construction of a temporary, dedicated emergency communication network, but such private networks are typically constrained in coverage, scale of resources, and usage authority, and cannot fully substitute for the basic communication capability of the public network. They must therefore be used in coordination with public network resources, including public networks in unaffected areas, public networks partially restored after a disaster, and satellite links, among other resources. With the development of cloud computing, Network Function Virtualization (NFV), and Software Defined Networking (SDN), the emergency communication command system is increasingly taking the form of a "virtualized system" built collaboratively across public networks, private networks, and multiple data centers, in order to meet the demands of rapid deployment and elastic resource scheduling.

(4) **Coupling between technical performance and management mechanisms.** Because of the high degree of system heterogeneity and the complexity of resource sourcing, an emergency communication command system

depends not only on the communication technology itself, but also heavily on organizational management, laws and regulations, and operating mechanisms working in concert. Frequency coordination, cross-department dispatching, permission control, and security management under different scenarios all need to be guaranteed through corresponding management systems and institutional rules. Consequently, the overall capability of an emergency communication command system is not determined by the technical system alone – policy and regulation, operating mechanisms, security systems, and organizational management are equally indispensable components.

3.1.2 Operational Process of Emergency Communication Command

The operational process of an emergency communication command system can be abstracted as a closed-loop process centered on the flow of information, in which four stages – information collection, information transfer, information processing, and command execution – are linked together to form the basic operating cycle of emergency communication command.

1. Information Collection

Information collection is the starting point of the emergency communication command process; its core task is to comprehensively sense and acquire, in real time, the situation at the disaster site. What is collected typically includes environmental data, voice, video imagery, target location information, and the aggregation of multi-source data, among other things, with the goal of giving commanders a complete and accurate picture of the on-site situation so that they can promptly grasp key information such as the geographic and meteorological conditions in the affected area, how the disaster is developing, the distribution of rescue forces, the status of resource dispatch, and the progress of response actions.

As sensor technology and the Internet of Things have advanced, the sources of information for an emergency communication command system are no longer limited to manual reporting, but have progressively expanded to a wide range of intelligent terminals and sensing devices. Sensors, RFID tags, cameras, drones, and various IoT terminals can automatically perform status monitoring, environmental sensing, anomaly detection, and alarm reporting, forming a "people–objects–environment" collaborative sensing system. This shift has significantly improved the system's real-time sensing capability and level of

automation, but it has also raised the bar for communication bandwidth, data processing capability, and information fusion efficiency.

2. Information Transfer

Information transfer plays the crucial role of connecting on-site sensing with rear-echelon command; its main functions are the real-time uploading of on-site information and the rapid delivery of command orders. The foundation for this process is an emergency communication network built jointly from satellite communication, trunked communication, public mobile communication, HF (shortwave) communication, ad hoc networking, and other technologies.

In sudden-onset incident scenarios, the main challenge facing information transfer is that basic communication infrastructure may be damaged or even completely disabled, while the site still needs continuous, reliable transmission of voice, data, imagery, and video and other services. How to maintain stable communication links under complex conditions, and how to improve network survivability and service assurance capability, therefore become core problems in the design of emergency communication systems.

In terms of access methods, emergency communication includes both wired access methods such as fiber-optic cable and copper cable, and wireless access methods such as satellite, broadband wireless, trunked communication, and ad hoc networking. Wired communication offers high capacity and high stability, but is vulnerable to damage in a disaster environment and lacks deployment flexibility; wireless communication offers strong mobility, rapid deployment, and adaptability to complex environments, making it the primary access method in emergency scenarios.

3. Information Processing

Information processing is the core stage in which the various types of information from an emergency site are analyzed, organized, and turned into decision support; it includes data storage, computational analysis, visualization, situational assessment, and decision assistance.

GIS is an important underlying platform for emergency command information processing. By visualizing terrain, personnel locations, equipment status, and spatial relationships, GIS helps commanders quickly build spatial awareness of the site, improving the efficiency of damage assessment, resource dispatch, risk assessment, and coordinated command.

At the same time, data fusion technology can correlate and comprehensively process information arriving from different sensors, different communication links, and different business systems; by exploiting the complementarity of multiple sources, it improves the accuracy and reliability of situational awareness. Compared with any single information source, the result of multi-source fusion more fully reflects the true state of the site, providing more reliable intelligence support for command decisions.

4. Command Execution

Command execution is the final stage in which the emergency communication command system converts decisions into on-site action. The various response departments and on-site rescue forces carry out coordinated action according to the dispatch orders issued by the command system, achieving unified organization and task control of rescue resources, until the response mission is complete.

Command instructions can be delivered in a variety of forms – voice, text, imagery, video – with different information-carrying forms used in different operational scenarios to meet requirements for timeliness and accuracy. During command execution, on-site feedback information again flows back to the command center through the information-collection link, forming a closed-loop operating mechanism of sensing, transmission, processing, execution, and feedback that enables continuous, dynamic adjustment and optimization of the response process.

3.1.3 Facility, Capability, and Support: The Three-Plane Architecture

Emergency Communication Command: Technology, Systems, and Applications (Chen Shanzhi et al., Publishing House of Electronics Industry, 2013) proposes dividing the emergency communication command reference model into a Facility Plane, a Capability Plane, and a Support Plane, describing the system from the three dimensions of physical composition, emergency capability, and management support, respectively, as shown in Figure 4.

Figure 3. Emergency Communication Command Reference Model

1. Facility Plane

The Facility Plane describes the physical composition of the emergency communication command system and its functional layering. Functionally, it can be divided into three layers – the access and information-collection layer, the communication network layer, and the service and application layer – which connect with one another to form the complete emergency communication command infrastructure system.

The access and information-collection layer sits at the bottom of the Facility Plane and is mainly responsible for the access and sensing of the various users, devices, and on-site information sources. What connects to it includes commanders, professional rescue personnel, and members of the public, as well as devices such as sensors, RFID tags, and cameras. The services carried by the system span voice, data, imagery, and video, and can be divided into real-time and non-real-time services according to their latency requirements. Given the need for deployment flexibility and the complexity of the disaster environment, this layer is predominantly wireless – trunked communication, satellite communication, broadband mobile communication, ad hoc networking – supplemented as necessary by wired access.

The communication network layer sits in the middle of the Facility Plane and is responsible for carrying information and interconnecting networks, covering both on-site communication within the affected area and wide-area communication between the site and the rear command center. By networking scope and function, it can be further divided into three forms: wide-area relay networking, on-site regional networking, and on-site access networking. The wide-area relay network mainly provides long-distance communication between the affected area and the remote command center; the on-site regional network is responsible for covering coordinated communication among the various rescue units within the affected area; and the on-site access network provides access capability to individual terminals and end users. Together, these three types of network form the complete emergency communication network system. Within this layer, private and public networks typically operate in coordination: the private network emphasizes highly reliable, high-priority on-site command and dispatch capability, while the public network plays a complementary role in wide-area coverage, capacity support, and public communication services – the two complement each other's strengths.

The service and application layer sits at the top of the Facility Plane

and directly provides emergency communication and command services to different user groups. By service target, it can be divided into services for commanders, services for professional response personnel, and services for the public. Command-level services mainly involve formulating response plans, resource dispatch, and coordinated control; services for professional personnel mainly include on-site monitoring data, positioning information, imagery/video, and action orders; and public services include emergency calls for help, self-rescue guidance, disaster notification, and "safe and well" reporting. From a functional perspective, services can be further divided into communication services, command services, and positioning services. With the development of broadband mobile communication technology, emergency communication command services are evolving from traditional narrowband voice toward broadband multimedia – high-definition video conferencing, broadband trunked communication, and multimedia collaborative dispatch have become important components of modern emergency command systems.

2. Capability Plane

The Capability Plane describes the core capability attributes that different facilities and systems must jointly possess in an emergency scenario, which can be summarized as four key capabilities: reachability, interconnection and interoperability, prioritization, and intelligence.

Reachability refers to the level at which the system can continuously provide communication capability across different times, different locations, and different user relationships; its goal is to avoid, as far as possible, information isolation caused by network outages during a sudden-onset incident. Achieving reachability presupposes that the communication network has strong survivability, including redundant network topology, damage-resistant routing, and automatic recovery mechanisms.

Interconnection and interoperability is one of the most challenging capabilities to achieve in the construction of an emergency communication system. Because different departments have long used different frequency bands, different standards, and equipment from different vendors, direct coordination among the various communication systems is often difficult. In actual emergency response, interoperability is needed at the level of terminals, networks, and business systems in order to support cross-department coordinated command and joint action. Interoperability problems generally involve three levels – terminal access, network interconnection, and business data exchange – and

are among the issues that consume the most resources and carry the highest technical complexity in emergency communication engineering.

Prioritization capability refers to the system's ability, under conditions of constrained resources or network congestion, to give priority assurance to important users and critical services; it mainly covers priority access and priority transmission. Priority access ensures that commanders and rescue personnel can preferentially obtain a communication channel, while priority transmission improves the level of transmission assurance for critical business data. Dedicated trunked communication systems today generally have mature prioritization mechanisms already in place, while prioritization capability in the public network mainly relies on emergency priority service mechanisms and QoS policies.

Intelligence capability refers to the introduction of automation and intelligent technologies into the processes of information collection, situational analysis, and decision assistance. At present, GIS-assisted decision systems, intelligent video analytics, and expert systems have become important tools supporting emergency command. As artificial intelligence, wireless sensor networks, and cloud computing continue to develop, future emergency communication command systems will further raise the level of automation and intelligence in areas such as intelligent sensing, target recognition, multi-source data fusion, situational assessment, and decision assistance, thereby improving the efficiency of emergency response and the accuracy of decision-making.

3. Support Plane

The Support Plane reflects the dependence of the emergency communication command system on policy and regulation, organizational management, and security mechanisms; its core role is to provide the institutional and management support needed for the Facility Plane and Capability Plane to operate effectively. The existence of the Support Plane makes clear that emergency communication command is not only a communication-technology problem but also a problem of organizational coordination and operational management.

Policy and regulation form the institutional foundation on which the emergency communication command system operates, mainly specifying the organizational structure, operating mechanisms, division of responsibilities, resource assurance, and oversight requirements for emergency communication.

Because management systems and emergency response systems differ across countries and industries, their policy and regulatory frameworks also differ markedly.

System management is mainly oriented toward the unified scheduling and operational maintenance of emergency communication network and business resources, with "integration of peacetime and wartime operations, coordinated linkage" as its core concept. In normal times, the system is in a state of monitoring, maintenance, and drilling; once a sudden-onset incident occurs, it can rapidly switch into emergency operating mode, dynamically scheduling and optimizing the allocation of communication resources. System management typically covers resource-scheduling management, system configuration management, fault management, and performance management, among other areas, with the goal of achieving efficient, coordinated use of communication resources under complex conditions.

Security mechanisms safeguard the stable operation of the system across multiple dimensions – physical security, network security, business security, and disaster-recovery backup. This includes access control for emergency command sites, encryption of classified communications, protection against network vulnerabilities, identity authentication and access control, and local and off-site backup of critical facilities and data. The security assurance of an emergency communication system depends not only on technical measures, but also requires strict organizational management and operating rules to work in concert – combining technology with management is the basic prerequisite for keeping the system secure and reliable.

3.2 Layered Reference Model of Emergency Communication Systems

The functional composition of an emergency communication system is highly complex and heterogeneous, spanning multiple technical layers from end sensors, wireless access links, and wide-area transmission backbones, all the way to command and dispatch platforms and business support systems. In order to describe this complex system in an orderly way at the theoretical level, and to provide a unified analytical framework for system design, interoperability assessment, and the definition of standardized interfaces, it is necessary to draw on a layered reference model to abstract and formalize the

functional architecture of the emergency communication system. Drawing on the functional practice of emergency communication command systems, this book divides the layered reference model of an emergency communication system into four functional layers – the perception and access layer, the transmission and networking layer, the platform and data layer, and the service and application layer. Vertical interaction between layers is achieved through standardized interfaces, and horizontal coordination among different components within the same layer is achieved through unified protocols, as shown in Figure 5.

Figure 4. Layered Reference Model of Emergency Communication Systems

The four-layer structure above embodies a bottom-up functional progression from physical sensing to business decision-making: the bottom layer provides physical connectivity and data-collection capability, the middle layers achieve reliable signal transmission and network organization, the upper layer completes data processing and business orchestration, and ultimately the application layer supports the execution of the various emergency command services.

3.2.1 Perception and Access Layer

The perception and access layer is the interface between the emergency communication system and the physical world; its main function is to convert the raw signals from the various on-site information sources into digital signals suitable for upper-layer transmission, and to provide communication access capability to on-site terminals. Its functional elements mainly include the following.

(1) **Terminal access.** This includes wireless communication terminals held by on-site rescue personnel – handheld radios, trunking terminals, portable satellite terminals, HF stations – as well as mobile communication platforms such as emergency communication vehicles and portable cellular base stations. These terminals access the on-site communication network through an air interface, forming the outermost nodes of on-site communication.

(2) **Sensing and collection.** This includes various environmental sensors, wireless sensor network nodes, and image/video capture devices. Sensing devices access the network via low-power wireless protocols, Wi-Fi, Bluetooth, or cellular IoT, uploading collected data to the platform and data layer.

(3) **Access protocols and standardization.** The perception and access layer supports the coexistence of multiple air-interface standards, including Wireless Local Area Network (WLAN), HF, PDT, B-TrunC, and LTE/5G. Terminals of each standard are brought under unified system management through a common access-authentication mechanism and QoS policy.

3.2.2 Transmission and Networking Layer

The transmission and networking layer is responsible for establishing a reliable information-transmission channel between the perception and access layer and the platform and data layer, and for using network-organization techniques to solve problems such as on-site coverage, multi-network interconnection, and link redundancy. Its functional elements mainly include the following.

(1) **Wide-area transmission links.** These use satellite communication, public mobile communication networks (4G/5G), dedicated fiber-optic networks, or microwave relay to achieve remote data transmission between the on-site command node and the fixed rear command center. The bandwidth, latency, and reliability of the wide-area link directly determine how real-time front-to-rear command coordination can be.

(2) **On-site networking technologies.** Wireless mesh ad hoc networks, broadband wireless access, or trunked communication infrastructure achieve interconnection among multiple nodes within the on-site coverage area. In scenarios where infrastructure has been severely damaged, the wireless ad hoc network – which can dynamically form a network without needing fixed infrastructure – becomes an important supplement to on-site access networking.

(3) **Network redundancy and link protection.** The transmission and networking layer must design redundancy mechanisms against single points of failure, link congestion, and channel interference. Typical approaches include automatic primary/backup link switchover, multipath transmission, load balancing, and priority queue scheduling, to ensure the continuity of emergency communication services under extreme conditions.

3.2.3 Platform and Data Layer

The platform and data layer sits at the core of the layered architecture. It receives raw data from the transmission and networking layer and provides unified data access and service support to the business applications above it. Its functional elements mainly include the following.

(1) **Converged communication gateway.** This achieves convergence and interoperability of voice, video, and data services across heterogeneous networks – public mobile communication networks, dedicated trunked networks, satellite communication networks, and HF communication networks – masking the underlying differences in standards and presenting a unified communication service interface to upper-layer applications. The converged communication gateway is the key technical node for achieving cross-system interoperability, and the design of its standardized interfaces is decisive for enabling multi-vendor equipment to work together.

(2) **Data aggregation and processing.** Heterogeneous data streams from multiple sensors and multiple networks are aggregated, format-converted, and preliminarily processed to form a unified data model. Depending on the level of abstraction of the output, data fusion can be divided into three levels – data-level fusion, feature-level fusion, and decision-level fusion – corresponding respectively to the merging of raw signals, feature extraction, and comprehensive assessment.

(3) **Storage and management.** The audio recordings, video footage, geographic data, and text logs produced during emergency command operations must be persistently stored locally or in the cloud, and must support after-the-fact review and case analysis. The storage system must have primary/backup disaster-recovery capability to meet the high data-reliability requirements of emergency scenarios.

3.2.4 Service and Application Layer

The service and application layer is the functional layer of the emergency communication system that directly faces commanders and rescue personnel; building on the services provided by the platform and data layer, it implements the various emergency command business functions. Its core functional modules include the following.

(1) **Command and dispatch.** This provides multi-party voice conferencing, PTT group calling, floor-control preemption and forced disconnect/interrupt, and other trunking dispatch functions, as well as GIS-based visualized resource dispatch capability; it is the core operating interface for emergency command.

(2) **Situational awareness and decision assistance.** Drawing on the GIS system, intelligent video analytics system, and expert knowledge base, this presents commanders with the dynamic evolution of the disaster situation, and automatically generates or recommends response plans through the intelligent decision-assistance system to support emergency decision-making.

(3) **Public warning and information release.** Disaster warnings and emergency announcements are released to the public through channels such as cell broadcast, SMS, and mobile internet applications, enabling the flow of information from government agencies to the public.

(4) **Simulation drills and evaluation.** This includes digital management of emergency plans, tabletop drill systems, and live-exercise evaluation platforms, used for routine training, plan validation, and drill-effectiveness evaluation — an important supporting mechanism for the continuous improvement of the emergency communication system.

It should be noted that the layer boundaries above are logical divisions in a functional sense, not strict physical separation. In engineering practice, the same piece of physical equipment may carry out functions belonging to multiple layers at once — for example, an emergency communication vehicle may include a mobile base station belonging to the access layer, while also integrating a satellite backhaul link belonging to the transmission layer, and possibly even carrying converged-communication-gateway software belonging to the platform layer. Furthermore, as SDN and NFV technologies are progressively introduced into emergency communication, the dynamic recombination and flexible deployment of functions across layers will become an important direction for the future evolution of these systems.

3.3 Emergency Communication Networking Modes

An emergency communication networking mode refers to the systematic method of selecting and deploying the appropriate communication technology and network topology, during the response to a sudden-onset incident, for a given coverage requirement and organizational level. Unlike conventional

communication networks, whose capacity planning centers mainly around fixed infrastructure, the primary constraints facing emergency communication networking are time pressure and infrastructure uncertainty – that is, the need to rebuild coverage and restore command links in the shortest possible time, on the premise that infrastructure may have been damaged and that the public network may be severely congested or completely down. Emergency communication networking is therefore highly scenario-dependent and technically heterogeneous, and cannot rely on a single technical approach to solve every problem.

Viewed along the time dimension of how an incident unfolds, emergency communication networking generally goes through three phases. In the early stage of a sudden-onset incident, the public communication network is often hit hardest, so deployment speed is the top priority – means that depend little on existing infrastructure, such as portable satellite and HF equipment, are used to establish basic front-to-rear communication at the earliest possible moment. As response forces continue to converge on the scene, the networking must cover a wider area and aggregate more access systems, so bandwidth requirements rise significantly. In the mid-to-late stage of the response, as the public network is progressively restored, interoperability between the various emergency dedicated networks and the public network becomes the main issue. These three phases call for very different networking requirements, which is precisely why multiple networking modes are deployed in parallel.

Viewed along the spatial dimension of geographic coverage, the network-connectivity requirements of a typical emergency communication scenario can be divided into three distinct scales: the wide-area scale, covering the long-distance communication link between the site and the fixed rear command center (typically spanning tens to hundreds of kilometers); the intermediate scale, covering the interconnection of multiple access systems across a large on-site area (typically with a radius exceeding 10 km); and the end scale, covering the direct access of response personnel within a single work area (a typical work area has a coverage radius of 1–5 km). Corresponding to these three scales, emergency communication networking modes can be divided into three basic types – wide-area relay networking, on-site regional relay networking, and on-site access networking – as shown in Figure 6.

Figure 5. Relationship Among the Three Emergency Communication Networking Modes

The three networking modes are functionally complementary and, logically, form a bottom-up hierarchical network system: on-site access networking covers the outermost tier, providing access for on-site rescue personnel; on-site regional relay networking sits in the middle, aggregating and interconnecting multiple access networks; and wide-area relay networking sits at the top, maintaining the wide-area channel between the site and the rear. In practice, when a sudden-onset incident covers a relatively small geographic radius, the regional relay tier can be omitted, with the access network connecting directly to the wide-area relay. Table 17 compares the main characteristics of the three networking modes.

Networking mode	Typical range	Core function	Typical technologies	Core requirements
Wide-area relay networking	Tens to hundreds of km	Connects the site to the rear command center	Satellite communication, public network, dedicated fiber network, HF	Wide coverage, damage resistance
On-site regional relay networking	Radius > 5 km	Aggregation and interconnection of multiple access networks	Microwave, wireless ad hoc network, UAV relay	Bandwidth, flexibility

Networking mode	Typical range	Core function	Typical technologies	Core requirements
On-site access networking	Radius 1–5 km	Access for on-site rescue personnel	Trunked communication, wireless ad hoc network, broadband wireless access	Rapid deployment, mobility

3.3.1 Wide-Area Relay Networking

The core task of wide-area relay networking is to establish a stable wide-area communication link between the mobile emergency command platform at the site of a sudden-onset incident and the fixed emergency command platform in the rear, supporting vertical connectivity and information exchange between the levels of the emergency command system, while also providing a transmission channel for horizontal coordination among peer dedicated command systems. The quality of the wide-area relay link directly determines how real-time front-to-rear coordinated command can be; it is the critical link at the top of the entire emergency communication system, and its loss would leave the site as an information island.

1. Main Technical Approaches

Table 18 lists the main technical approaches available for wide-area relay networking.

Technical approach	Bandwidth, latency	Portability	Deployment speed	Networking flexibility	Infrastructure dependence
GEO communication satellite	Medium (tens of Mbit/s, latency ~200–300 ms)	Medium	Fast	Medium	Low
LEO communication satellite	Medium (tens of Mbit/s, latency ~20–30 ms)	Excellent	Fast	High	Low
Microwave communication	Medium (tens to hundreds of Mbit/s)	Medium	Medium	Poor	Medium
HF (shortwave) communication	Low (≤ tens of kbit/s)	Excellent	Fast	Poor	Low
Public 4G/5G network	High (tens to hundreds of Mbit/s)	Excellent	Fast	Excellent	High
Dedicated fiber-optic network	High (backbone can reach Gbit/s)	Poor	Slow	Poor	High

(1) **Satellite communication.** Because it depends little on ground infrastructure and its coverage is not constrained by geography, satellite communication is the most fundamental means of wide-area relay networking, and is often

the only available wide-area link in scenarios such as earthquakes and floods where ground facilities have suffered widespread damage. Traditional Very Small Aperture Terminal (VSAT) systems use Geostationary Earth Orbit (GEO) satellites; a single station typically offers under 2 Mbit/s of bandwidth with a one-way propagation delay of roughly 270 ms, which struggles to meet the needs of latency-sensitive services such as real-time video. With the development of High-Throughput Satellite (HTS) technology, Ku/Ka-band high-throughput systems can raise the throughput of a single gateway station to the hundreds-of-Gbit/s range, with per-user bandwidth reaching tens of Mbit/s, substantially increasing the satellite bandwidth available at an emergency site. In recent years, Low Earth Orbit (LEO) broadband satellite systems typified by Starlink have entered practical use; at an orbital altitude of roughly 550 km, they offer a propagation delay of only 20–50 ms and typical downlink rates of 100–400 Mbit/s, giving them a clear technical advantage as a wide-area relay method.

(2) **Microwave relay.** Terrestrial microwave relay can provide tens to hundreds of Mbit/s of digital transmission bandwidth under line-of-sight conditions, making it an important alternative once the public communication backbone has been damaged. Its main limitation is that a single hop is generally a point-to-point link requiring line of sight, which is difficult to deploy in mountainous or densely forested terrain with complex obstructions, and its networking flexibility is limited. In emergency scenarios, microwave relay is more often used as a supplement to satellite communication, connecting emergency command nodes that are relatively close to one another, or providing a temporary substitute link when public fiber lines are cut.

(3) **HF (shortwave) communication.** High Frequency (HF) communication uses ionospheric reflection to achieve beyond-line-of-sight propagation. Equipment is small, lightweight, and can be rapidly deployed in any terrain, making it an important fallback for emergency communication, especially suited to extreme disaster conditions where all other wide-area links have failed. Its main drawback is narrow channel bandwidth (generally no more than tens of kbit/s), and transmission quality is heavily affected by ionospheric variation, so it can only support low-rate voice and short-message transmission and cannot carry bandwidth-heavy services such as video.

(4) **Public communication networks.** When the public communication infrastructure at the site of a sudden-onset incident has not been severely damaged, using the public mobile communication network for wide-area back-

haul offers high bandwidth and high reliability, making it the preferred option. However, public communication networks often face two challenges during major incidents: physical damage, particularly in natural-disaster scenarios; and traffic congestion, as large crowds gathering together with a surge in emergency traffic can overwhelm the network. Consequently, even where the public network is theoretically available, priority-assurance mechanisms are still needed for emergency communication traffic.

(5) **Fiber-optic communication**, with its high bandwidth, low latency, and strong resistance to electromagnetic interference, is the best-performing means of wired wide-area transmission. Unlike the temporary, mobile links established via satellite, microwave, or HF, a dedicated fiber network is normally built in advance of an incident and incorporated into routine operations and maintenance as part of the emergency communication infrastructure. Typical forms include government dedicated fiber backbones, fiber networks dedicated to emergency-management departments, and self-built fiber networks operated by sectors such as public security, fire and rescue, and electric power. Dedicated fiber networks offer ample transmission bandwidth, extremely low latency, and strong confidentiality; however, because the fiber lines themselves are fixed ground infrastructure, they are highly susceptible to being cut during highly destructive natural disasters such as earthquakes, floods, and landslides, and repair cycles can be lengthy.

2. Networking Strategy and Deployment Sequence

In the very first moments after a sudden-onset incident, portable equipment such as satellite phones or HF radios should be the first to deploy, establishing a basic communication link between the site and the rear as quickly as possible, so that the command center can obtain a first-hand picture of the situation. On this basis, as response personnel and equipment continue to arrive, higher-bandwidth equipment such as satellite VSAT terminals can be progressively introduced to improve imagery and video transmission capability. Once the public communication network has been restored to some degree, it can be incorporated as a backup or supplementary channel for the wide-area link.

Parallel deployment of multiple wide-area links with automatic switchover is key to improving the reliability of the wide-area relay tier. A typical approach is to use the satellite link as the primary path and the public network or microwave as backup, using link aggregation and multipath transmission control protocols to share load across multiple links and switch seamlessly

between them, minimizing the impact of any single link failure on emergency command.

3.3.2 On-Site Regional Relay Networking

When the geographic area affected by a sudden-onset incident is large, or the terrain is complex, a single access network often cannot cover the entire work area, and the vehicle-mounted trunking radios, portable base stations, and other equipment brought by each department form multiple independent, isolated sub-networks. The function of on-site regional relay networking is precisely to aggregate and interconnect these scattered access-network nodes, forming a unified command channel covering a large on-site area, which then connects to the rear command center via the wide-area relay tier. The bandwidth and flexibility of the regional relay tier are key to the efficiency of multi-department coordinated operations.

1. Main Technical Approaches

The main technical approaches available for on-site regional relay networking include satellite communication, terrestrial point-to-point microwave relay, broadband wireless ad hoc mesh networks, and Unmanned Aerial Vehicle (UAV) relay platforms. Their technical characteristics are compared in Table 19.

Technical approach	Bandwidth	Coverage radius	Networking flexibility	Deployment speed	Terrain adaptability
Satellite communication	Low	Not terrain-limited	Poor (point-to-point)	Fast	Excellent
Terrestrial microwave	Medium	Few to tens of km (line of sight)	Poor (point-to-point)	Medium	Terrain-limited

Technical approach	Bandwidth	Coverage radius	Networking flexibility	Deployment speed	Terrain adaptability
Broadband ad hoc network	High	Km per hop, extendable via multi-hop	Excellent	Fast	Medium
UAV relay platform	High (tens to hundreds of Mbit/s)	Tens to over a hundred km (depending on altitude)	Excellent	Fast	Excellent (unaffected by terrain obstruction)
Public communication network	High	Depends on infrastructure coverage	Excellent	Medium	Affected by facility damage

(1) **Broadband ad hoc networks.** A broadband ad hoc network is the most flexible technical approach for regional relay networking; its core feature is that it can dynamically form a network without fixed infrastructure – every node in the network acts simultaneously as a router and a communication terminal, forwarding data between nodes over multiple hops. Inside an occluded space, multiple relay nodes can be successively deployed along the interior of a building or an underground space, forming a stable link running from the core disaster area out to the forward command post, effectively overcoming the poor signal coverage that traditional wireless communication suffers from in high-rise buildings and underground spaces.

(2) **UAV airborne relay platforms.** With their high maneuverability and low dependence on terrain, drones have become an important emerging approach to on-site regional relay networking. By mounting a communication relay payload on a UAV platform and exploiting its higher vantage point relative to the ground, the coverage radius of a single station can be extended to tens

or even over a hundred kilometers – particularly useful in extreme terrain such as mountains and forests, large bodies of water, or areas where roads have collapsed and ground equipment cannot reach. The main constraints on UAV relay are flight endurance (a typical multirotor drone has an endurance of only 30–60 minutes), payload limits (which constrain relay power and antenna aperture), and flight feasibility under extreme weather. To address the limited endurance of multirotor drones, tethered drones – continuously powered through a cable – can remain aloft for hours or even tens of hours, and the cable can also carry high-speed backhaul data, effectively overcoming the bandwidth bottleneck of wireless backhaul.

2. Scenario Adaptability Analysis for Regional Relay Networking

In relatively open terrain such as plains and cities, broadband ad hoc networks and terrestrial point-to-point microwave relay can provide stable coverage at relatively low cost. In complex terrain such as mountains and canyons, where ground equipment is severely affected by terrain obstruction, UAV airborne relay or satellite communication become the primary choices. In scenarios involving large bodies of water, such as floods or maritime islands, water-surface mobile platforms carrying communication equipment can work together with UAVs and satellites to form a combined water–air regional relay network. It should be noted that, despite its many advantages, UAV relay can be severely restricted during earthquakes, landslides, heavy snowfall, and other extreme adverse weather; in such cases, satellite communication remains the ultimate fallback for both wide-area and regional relay.

3.3.3 On-Site Access Networking

On-site access networking sits at the outermost tier of the entire emergency communication network, providing wireless access for voice, data, and imagery directly to front-line response personnel (in this book, specifically referring to professional personnel engaged in on-site emergency response such as rescue teams and counter-terrorism/stability-maintenance personnel, hereinafter referred to as “individual field personnel”) and to the various on-site sensing and collection devices, and aggregating on-site information up to the mobile emergency command platform. Its coverage typically spans a work-area radius of 3–5 km. It is the network tier most tightly coupled to the response action itself, carries the widest range of service types, has the most demanding QoS requirements, and requires the greatest deployment flexibility.

1. Main Technical Approaches

The main technical approaches available for on-site access networking include trunked communication, broadband wireless access, wireless ad hoc networking, Wireless Sensor Networks (WSN), and – as a supplement for special scenarios – portable satellite and HF communication. Table 20 gives a comprehensive comparison of these technologies.

Technical approach	Bandwidth	Portability	Networking flexibility	Deployment speed	Service functions
Portable satellite terminal	Low	Excellent	Poor	Fast	Voice, low-rate data
Public network	Medium	Excellent	Medium	Fast	Voice, medium/high-rate data
Narrowband trunking (TETRA/PDT)	Low	Excellent	Excellent	Fast	Dispatch voice, low-rate data
Narrowband ad hoc network	Low/medium	Excellent	Excellent	Fast	Medium/high-rate data
Broadband trunking (B-TrunC/MCPTT)	High	Excellent	Excellent	Fast	Multimedia dispatch, medium/high-rate data
WLAN	High	Excellent	Poor	Fast	Medium/high-rate data
Wireless sensor network	Low	Excellent	Excellent	Fast	Low-rate data

Technical approach	Bandwidth	Portability	Networking flexibility	Deployment speed	Service functions
HF (shortwave)	Low	Excellent	Poor	Medium	Voice, low-rate data

(1) **Trunked communication.** Trunking is currently one of the most widely used access methods at emergency response sites; its core advantage lies in its mature command-and-dispatch functions — group calling, broadcast calling, priority calling, forced insertion, and forced disconnect — which can meet the complex organizational and command needs of coordinated multi-department operations. Traditional narrowband digital trunking standards mainly support voice services, with limited multimedia data capability. To meet the demands of bandwidth-heavy services such as video backhaul and real-time situational awareness, trunked communication is evolving toward broadband; the MCX suite defined by 3GPP is currently the mainstream direction for broadband trunked communication.

(2) **WLAN.** Based on the IEEE 802.11 family of standards, WLAN — with its deployment flexibility, low equipment cost, and high compatibility with the existing IP network ecosystem — has particular value in on-site access networking, especially suited to supplementary coverage in confined indoor spaces, local-area access for emergency command vehicles or forward command posts, and short-range data backhaul from UAV payloads. However, WLAN coverage is limited, typically 100–300 m, and because the 2.4 GHz and 5 GHz bands are open, unlicensed spectrum, co-channel interference becomes a significant problem under the dense equipment use typical of a multi-department emergency response.

(3) **Wireless sensor networks.** WSNs mainly perform end-point information collection within on-site access networking, using low-power wide-area protocols such as ZigBee, LoRaWAN, and NB-IoT to upload sensor data — temperature and humidity, toxic gas concentration, ground displacement, vital signs, and so on — from across the site to the on-site command platform. WSN nodes consume extremely little power, making them suitable for long-duration unattended deployment; their limitation is low transmission rate and limited single-hop range, so they typically need to be combined with ad hoc networking technology to form a layered end-point collection network.

3.3.4 Comprehensive Principles for Selecting Networking Modes

In actual emergency response, the three networking modes do not exist in isolation but are deployed together in a coordinated way. Selecting the appropriate networking technologies and determining the technical combination for each tier should follow the principles below.

(1) **Timeliness principle.** The focus of emergency communication needs differs across the different time phases of an unfolding incident, and technical approaches should be chosen to match the current phase. For example, in the early stage of an incident, priority should go to quickly establishing the wide-area link, using portable satellite and HF equipment to connect the site to the rear at the earliest possible moment; during the expansion of the response, the focus shifts to extending regional relay coverage, introducing broadband mesh and UAV relay to achieve multi-system interconnection; and in the mid-to-late stage of the response, the progressive restoration of the public network can be used to supplement system bandwidth, and the dedicated emergency network can be interconnected with the public network.

(2) **Applicability principle.** Different geographic environments and different incident types place different demands on the applicability of emergency communication technology; the most suitable technical approach should be chosen based on actual on-site conditions, avoiding a blind pursuit of technical sophistication at the expense of environmental fit. For example, UAV airborne relay and portable satellite are preferred in mountainous earthquake scenarios; broadband trunking and the public network are the main approaches in urban public-safety incidents; and multi-hop ad hoc networking is an effective way to overcome signal blockage in confined-space scenarios such as tunnel or mine rescue.

(3) **Moderation principle.** Emergency communication networking should not aim to maximize the variety of technologies used, but should instead aim for the minimum technical set that meets current emergency communication needs, avoiding the added system-integration difficulty and operational complexity that comes with excessive technical heterogeneity. Under this principle, the choice of networking technology at each tier should give priority to interoperability, ensuring that equipment from different vendors and different standards can access a unified converged communication platform, with transparent interoperability at the service level achieved through standardized interfaces.

3.4 Heterogeneous Network Interoperability

At the site of a sudden-onset incident, there is typically a simultaneous presence of communication networks from different departments, built on different standards at different times – for example, the ePDT trunking network of the emergency-management sector, the PDT trunking network of the public-security sector, the TETRA trunking network of the fire-and-rescue sector, dedicated networks belonging to vertical industries, on-site satellite communication stations, and even rescue personnel's own public 4G/5G phones. These systems physically coexist at the same site but are logically isolated from one another, unable to communicate directly, forming a set of isolated communication islands.

The core goal of heterogeneous network interoperability is to achieve seamless flow of voice, video, and data across different networks – without requiring any system to change its own standard or rebuild its infrastructure – through gateway equipment, standardized protocols, and a unified management platform, so that a commander can invoke all of the heterogeneous terminals through a single dispatch interface. The difficulty of achieving this goal shows up across three dimensions: first, terminal heterogeneity, meaning that terminals of different standards differ fundamentally in codec format, call signaling, and physical interface; second, system heterogeneity, meaning that each sub-network is independent in terms of network topology, frequency resources, QoS mechanisms, and security/authentication systems; and third, management heterogeneity, meaning that each sub-network falls under the jurisdiction of a different department, each with its own standards for operating policy, cost structure, and priority definitions.

3.4.1 Basic Framework for Interoperability

In emergency communication scenarios, the need for interoperability is uniquely urgent and complex. Unlike the network convergence found in conventional communication systems, emergency interoperability must complete system access and dispatch configuration within a short time after an incident occurs, and the operators involved may be under considerable pressure and cognitive load, making ease of use and speed of access just as important as the interoperability itself. Emergency-scenario interoperability also faces the following specific challenges: first, the long-term coexistence of legacy systems – some departments still use analog

trunking or early-generation digital trunking that cannot natively support IP-based interoperability protocols; second, the instability of on-site network infrastructure, which means the interoperability platform itself must have high reliability and fault tolerance; and third, differences in security policy across departments – different departments have different requirements for communication encryption and identity authentication, and cross-system interoperability can introduce new security risks.

The technical path to achieving interoperability can be understood at three levels, as shown in Figure 7. The first level is the standardized interoperability framework – the reference system, defined by international standards bodies, specifying how various systems should achieve interoperability. The second level is engineering implementation – the converged communication gateway and its various integration methods, which is currently the most widely deployed interoperability technology in the emergency communication field. The third level is the public–private convergence mechanism – enhancing public-network capability or enabling adaptive terminal-side switching, working from both the network side and the terminal side to solve the convergence problem between public and private networks.

Figure 6. Technical Paths for Heterogeneous Network Interoperability

From a protocol-architecture point of view, interoperability among heterogeneous networks involves three functional planes that are independent of one another yet closely related; understanding this framework is a prerequisite for grasping the essence of the various interoperability technologies.

(1) **User-plane interoperability** refers to the conversion and delivery of media streams (voice, video, data) between systems of different standards. Its core technology is media transcoding – converting an audio/video stream from one codec format to another in real time, for example converting the narrowband ACELP voice coding used by TETRA into the AMR-WB wideband voice coding used by IP voice systems. The difficulty in user-plane interoperability lies in controlling transcoding delay and audio-quality loss, and in handling multiple concurrent media streams in multi-party conference scenarios.

(2) **Control-plane interoperability** refers to the conversion and mapping between different signaling protocols. Trunking functions such as group-call

setup, floor-control requests, priority preemption, and forced insertion/disconnect all depend on signaling protocols, and trunking systems of different standards differ fundamentally in their signaling design. Control-plane interoperability must accurately map the dispatch signaling of one system into a signaling sequence recognizable by another, without losing critical semantic information such as priority or floor-control state. Control-plane interoperability is significantly more difficult to achieve than user-plane interoperability and represents the core challenge of interoperability technology.

(3) **Management-plane interoperability** refers to the unified coordination of cross-system user-identity mapping, group management, and resource configuration. In a joint, multi-department emergency scenario, each department's trunking system has its own independent user directory and group configuration; management-plane interoperability must establish a unified identity namespace so that cross-system individual and group calls can accurately address their target users, and must support the dynamic creation and management of cross-system groups. Management-plane interoperability is typically achieved through a unified dispatch-management platform or an interoperability group server.

Interoperability across the three planes differs in technical maturity. Media transcoding at the user plane is a fairly mature technology and can be achieved by any converged communication gateway; deep interoperability of dispatch functions at the control-plane signaling level remains an engineering challenge even within international standards frameworks; and management-plane interoperability, in most engineering projects, has only achieved basic user mapping, with cross-system dynamic group management still at an early stage of standardization. Figure 3-5 shows, in block-diagram form, how the three functional planes map onto the interoperability gateway.

Figure 7. Figure 3-5: Mapping Between Interoperability Functional Planes and the Converged Communication Gateway

3.4.2 Standardized Interoperability Framework: MCX and IWF

Before the MCX standards suite was established, interoperability among trunked communication systems from different vendors relied mainly

on bilateral agreements or proprietary interfaces, tightly binding the interoperability solution to a particular equipment vendor and making it difficult to swap platforms between vendors – this created a serious risk of vendor lock-in for the long-term maintenance and cross-agency deployment of emergency communication infrastructure. This background motivated 3GPP, starting with Release 13, to build MCX, a standardized interoperability suite covering the full range of broadband mission-critical communication services. Its design goal is to replace the traditional narrowband dedicated trunking network with a standardized IP bearer layer, providing dispatch functions on an LTE/5G broadband network that are equivalent to, or exceed, those of traditional trunked communication, while using open, standardized interfaces to enable interchangeability of multi-vendor equipment, fundamentally solving the vendor-lock-in problem. MCX covers three categories of service capability: MCPTT provides voice group calling, individual calling, priority preemption, and floor-control management that meet public-safety command-and-dispatch requirements; MCVideo provides real-time video transmission and video-surveillance access capability; and MCData provides short data messaging, file transfer, and location-sharing capability.

Following the establishment of the general MCX framework described above, 3GPP addressed a specific and equally important problem: how newly-defined MCX systems can interoperate with the large installed base of existing narrowband Land Mobile Radio (LMR) systems (such as TETRA, PDT, and P25) – this is the role of the InterWorking Function.

IWF (InterWorking Function) Mechanism

To solve the problem of interoperability between MCX systems and existing narrowband Land Mobile Radio (LMR) systems (such as TETRA, PDT, and P25), 3GPP introduced the IWF mechanism in Release 14, specified in detail in 3GPP TS 23.283. Architecturally, the IWF is deployed as an independent functional entity on the MCX side of the system; the LMR system requires no modification at all, and can achieve two-way voice interoperability with the MCX system purely through the IWF.

Per the TS 23.283 specification, the IWF connects to the MCX system through three standardized reference points, covering three functional planes: reference point IWF-1 connects to the MCPTT server, achieving signaling and media interoperability for voice group calls and individual calls; reference point

IWF-2 connects to the MCData server, achieving cross-system delivery of short data services; and reference point IWF-3 connects to the group-management server, achieving configuration synchronization and member management for interoperability groups. At the user plane, the IWF performs real-time transcoding between the narrowband voice coding used by the LMR system and the AMR-WB wideband coding used by MCPTT; at the control plane, the IWF maps the LMR system's floor-control signaling into MCPTT signaling while preserving priority semantics. Table 21 summarizes the IWF's core functions across the three functional planes.

Functional plane	IWF reference point	Connects to	Core function
User plane, control plane	IWF-1	MCPTT server	Voice group-call/individual-call signaling mapping; real-time transcoding between LMR narrowband coding and AMR-WB
User plane	IWF-2	MCData server	Cross-system delivery of Short Data Service (SDS)
Management plane	IWF-3	Group-management server	Interoperability-group configuration synchroniza-tion; cross-system member management

3.4.3 Converged Communication Gateway

1. System Architecture

At the engineering level, the converged communication gateway is the core piece of equipment for achieving heterogeneous network interoperability. It is deployed at the aggregation point of multiple heterogeneous sub-networks and simultaneously handles the parsing, conversion, and forwarding of multiple communication protocols, as shown in Figure 3-6. From a protocol-stack perspective, the gateway performs media transcoding at the user plane, converting the voice codec formats of different systems into one another, and performs signaling adaptation at the control plane, mapping the call signaling of different systems onto one another so that dispatch functions such as group calling and individual calling can pass transparently across systems.

Figure 8. Figure 3-6: Deployment Position of the Converged Communication Gateway in Heterogeneous Networks

A typical logical architecture for a converged communication system consists of five layers: the terminal layer, the access layer, the convergence-service layer, the enablement layer, and the application layer. The convergence-service layer is the core of the entire system: it aggregates the media and signaling streams arriving from the various gateways in the access layer, achieving voice-service convergence, video-surveillance convergence, video-conferencing convergence, location-information convergence, data-service convergence, and trunking-dispatch convergence, and exposes a unified business interface to the upper-layer emergency command applications through the enablement layer. The access layer deploys dedicated gateway equipment matched to the standard of the system being connected — PDT/TETRA gateways, broadband trunking/LTE/5G gateways, satellite communication gateways, video-surveillance gateways, and PSTN/Public Land Mobile Network (PLMN) gateways — with each gateway type corresponding to one or more access protocols. As the maturity of the MCX standards suite has improved, commercial converged communication gateway products conforming to the 3GPP IWF specification are progressively replacing earlier engineering implementations based on proprietary protocols.

2. Main Integration Methods

Depending on the technical characteristics of the system being connected, the integration methods used by a converged communication gateway generally fall into four categories: protocol integration, air-interface integration, SDK proprietary-interface integration, and back-to-back hardware cascading. The applicable scenarios and characteristics of each are as follows.

(1) **Protocol integration.** Protocol integration is the most standardized way to achieve system-level interoperability: the two systems establish signaling and media channels directly through a standard communication protocol, without the need for dedicated hardware middleware. It applies where both sides support some recognized standard protocol.

(2) **Air-interface integration.** For trunking systems with a closed protocol stack that does not expose a system-level interface, air-interface integration can be used: a radio module matching the target system's standard is built into the converged communication gateway, which then accesses the target system over the air interface, acting simply as an ordinary trunking terminal, with the gateway handling the protocol conversion to the convergence platform on the other side. The advantage of air-interface integration is that it does not affect the target system and does not depend on the vendor exposing a system interface; the disadvantage is that access capacity is limited by radio channel resources, and equipment cost and power consumption are relatively high.

(3) **Software Development Kit (SDK) proprietary-interface integration.** Some equipment vendors provide a proprietary SDK, and the converged communication platform calls the APIs exposed by that SDK to control the vendor's equipment and retrieve data. The advantage of SDK integration is functional completeness – it allows deep access to a vendor's proprietary device functions; the disadvantage is a low degree of standardization, requiring re-adaptation whenever the SDK version changes, which raises long-term maintenance cost.

(4) **Back-to-back hardware cascading.** For older or specialized equipment that offers neither an open protocol interface nor SDK support – such as some legacy hardware video-conferencing terminals – a back-to-back approach can be used, directly cross-connecting the input/output ports of two devices through interfaces such as HDMI or analog audio cabling, achieving physical-layer interoperability of the audio/video signal. Back-to-back integration is simple to deploy, but it can only achieve basic media interoperability and

cannot achieve deep functional linkage at the signaling level.

3.4.4 Convergence of Public and Private Networks

In the engineering practice of emergency communication systems, the public mobile communication network and the dedicated emergency network have long been built and operated as independent systems. The private network can be tailored to emergency requirements in terms of frequency resources, QoS policy, and security control, unaffected by fluctuations in public-network traffic; the public network, by contrast, relies on large-scale commercial deployment to achieve a density of wide-area coverage that no private network can match. However, the coverage of a dedicated emergency network is limited by the scale of investment in its construction, and it struggles to match the density of full-area coverage achieved by the public network – a gap that is especially pronounced in remote mountainous regions and offshore areas. In addition, when a sudden-onset incident occurs, the public in the affected area often flood onto the communication network, causing severe congestion; if on-site emergency commanders are relying solely on public-network terminals, they face the same network unavailability as ordinary users, with no priority assurance whatsoever. In recent years, public–private convergence has been moving from scattered pilot projects toward systematic, large-scale deployment, and this goal can be pursued along two paths: the network side and the terminal side.

1. Network-Side Convergence Deployment

From the network side, convergence deployment between the public network and the dedicated emergency network mainly takes three forms: an independent private network, 5G network slicing, and joint public–private construction and sharing. An independent private network offers the highest security, but is limited in coverage and costly, making it suitable for high-security core command nodes. 5G network slicing is the main direction of current technical evolution – under a 5G SA architecture, the operator creates a dedicated slice for the emergency-management department with its own resource pool and QoS policy, achieving logical isolation on a shared physical infrastructure through SDN and NFV. Joint public–private construction and sharing is suited to lightweight deployment during a transition period, using mechanisms such as pre-configured emergency-service priority markers and dedicated core

networks within a 4G LTE or 5G Non-Standalone (NSA) network to ensure that emergency traffic gets priority access to radio resources when the network is congested.

In practice, the three modes are typically used in combination: core command functions and highly confidential services are deployed on a self-built private network, while wide-area on-site coverage borrows capacity from the operator's network through a 5G slice, with the two converged through standardized interfaces to form a hybrid networking architecture. This primary/backup combination balances the three needs of security, coverage breadth, and cost control.

2. Terminal-Side Convergence

From the terminal side, the dual-mode terminal offers another technical path for solving the problem of coordinated access across public and private networks. A dual-mode terminal integrates both a public mobile communication module and a dedicated emergency communication module, with a built-in intelligent switching engine that automatically selects the optimal access method based on network status, service priority, and signal quality, presenting the user with a single, unified communication interface.

The switching strategy of a dual-mode terminal can be executed as a three-tier priority fallback: PTT dispatch traffic is preferentially carried over the dedicated trunking network, taking full advantage of the private network's QoS assurance; if the private network is unavailable, the terminal automatically switches to the public 4G/5G network, providing equivalent dispatch functionality through an MCPTT client or a PoC application; and in the extreme case where neither network is available, the terminal supports direct mode, maintaining local contact through direct terminal-to-terminal communication in the absence of any infrastructure coverage.

3.4.5 Security Assurance for Interoperability

While heterogeneous network interoperability improves the ability of multiple systems to work together, it inevitably enlarges the attack surface: if the interoperability channels among the various systems lack encryption and access control, they can become a path for information leakage or network intrusion. Security assurance must run through the entire interoperability

chain, addressed jointly across three levels — identity authentication, media encryption, and platform isolation.

(1) **Identity authentication and access control.** Cross-system interoperability requires a unified identity and authentication mechanism, strictly authenticating every system and terminal that connects to the converged communication platform to prevent unauthorized access. In scenarios shared by multiple departments, role-based access control can restrict how users from one department can access another department's communication resources, achieving cross-department communication authorization on an as-needed basis and preventing sensitive information from spreading beyond its authorized scope.

(2) **Media-stream encryption and transcoding security.** Voice and video streams forwarded through the converged communication gateway must be protected with end-to-end or segment-based encryption at the transport layer. However, when the IWF needs to perform voice-coding conversion, it must first decrypt the media stream before transcoding it, which makes the gateway node a security-sensitive processing point. A trusted computing environment must be used to protect the decryption keys and the transcoding process, preventing plaintext media content from being exposed at the gateway node.

(3) **5G slice security isolation.** In a public–private convergence deployment, the emergency communication slice shares physical infrastructure with public slices, and mechanisms for resource isolation, traffic isolation, and management isolation are all needed to prevent interference between slices. Both 3GPP and ETSI have developed slice-security specifications covering slice access control, verification of inter-slice data isolation, and slice security monitoring — these form the security foundation for 5G emergency communication applications.

It is worth noting that the security policy of an emergency communication system requires a reasonable trade-off between security strength and response speed. End-to-end encryption is good for the confidentiality of media content, but it adds to the security-processing complexity of IWF transcoding; strict access control is good for preventing unauthorized access, but it can cause delay in the early stage of an emergency response, when many systems need to be connected quickly. A common practice is to preconfigure an interoperability authorization whitelist that can be activated with a single action when an incident is triggered, avoiding the delay that ad hoc

authorization negotiation would otherwise cause.

3.5 Communication Support Emergency Plans and Drills

The completeness of the emergency communication system architecture must ultimately be assured through a mechanism that integrates peacetime and wartime operations: in peacetime, the organizational procedures, technical means, and resource-deployment plans needed for emergency response are codified into an executable plan document; when an incident occurs, the experience built up through long-term, systematic drilling ensures that the plan can still be accurately executed under the high-pressure, chaotic conditions of a real response. A communication support emergency plan shares common ground with emergency plans in general, but also has its own technical specificity. In terms of common ground, the *National Overall Emergency Response Plan for Sudden-Onset Incidents* (issued in 2025) provides the top-level institutional framework for the nationwide response to sudden-onset incidents, and communication support, as an important component of the overall emergency-assurance system, must be drafted within that overall framework. In terms of specificity, the content of a communication support plan — frequency coordination, network topology, equipment dispatch, multi-system interoperability, and so on — is closely tied to the technical logic of communication engineering, and the scientific soundness of the plan depends heavily on how deeply the people drafting it understand the communication technology system. This section takes a communication-engineering perspective, introducing in turn the hierarchical structure of the communication support plan system, the drafting and management of plans, the classification and organizational process of drills, drill evaluation and continuous plan improvement, and the latest applications of digital technology in plans and drills.

3.5.1 Communication Support Emergency Plan System

An emergency plan is an action plan that governments at all levels, relevant departments, and enterprises and institutions draw up in advance so that they can respond to various sudden-onset incidents lawfully, promptly, scientifically, and in an orderly way. Its core function is to convert the organizational procedures, division of responsibilities, resource deployment, and response measures of emergency response from on-the-spot improvisation

into standardized, executable actions, so that orderly organizational behavior and response speed can still be assured under the extreme uncertainty and time pressure of an actual incident.

A communication support emergency plan is a specialized plan addressing communication needs during a sudden-onset incident, and is one of the specialized-plan categories within the overall emergency-plan system. Its task is to establish and improve the working mechanism for emergency communication support, meet communication-support needs under sudden-onset conditions, and ensure that communications remain secure and unobstructed. Compared with a general-purpose emergency plan, a communication support plan has significant technical specificity: its content must cover the network's damage-resistance strategy, the switchover procedure for backup links, the operating procedures for emergency equipment, and the coordination mechanism for cross-department, cross-system communication resources – the accuracy of this content directly determines how workable the plan will be in a real response.

The *National Overall Emergency Response Plan for Sudden-Onset Incidents* specifies that the system of emergency plans for sudden-onset incidents includes the various plans drawn up by party committees and governments at all levels, by the relevant departments of party committees and governments at and above the county level, by grassroots organizations, and by enterprises, institutions, and social organizations; the emergency plans of party committees and governments at and above the county level consist of an overall plan, specialized plans, and departmental plans. Within this overall framework, the communication support emergency plan system takes the form of a national, provincial/ministerial, prefecture/city, and enterprise-level hierarchy. The *National Communication Support Emergency Plan* (revised 2011) is the top-level document of the entire system, applicable to communication outages or communication-support work for sudden-onset incidents that require coordination by the State Council or a department authorized by the State Council, and it also guides communication-support emergency work nationwide. A lower-level plan must be drafted on the basis of the plan above it and must not conflict with it; when a higher-level plan is activated, lower-level plans automatically enter a linked-response state; when an incident exceeds the response capability of the current level, the corresponding communication-support command body must promptly request support from the level above and must report upward as required, without delay or omission. Horizontal coordination is reflected in the requirement that a communication support

plan at a given level must be coordinated with other specialized emergency plans at the same level – public security, fire and rescue, medical, electric power, and so on – clearly defining the rules for cross-department sharing of communication resources and priority allocation, so as to avoid resource conflict and command confusion during a joint multi-department response.

By the nature of the support task, communication support plans can be divided into two broad categories: communication-restoration plans and communication-support plans. The former addresses repair and restoration after the communication network itself has been damaged; the latter addresses the communication-support work needed for responding to a major sudden-onset incident or supporting a major event. The two categories differ significantly in their activation conditions, the entities responsible for response, and the types of resources required, and must be drafted separately, while remaining consistent with each other in overall plan structure and management mechanism.

3.5.2 Plan Development and Management

1. Core Elements of a Plan

Structurally, a communication support emergency plan typically contains the following core elements, which relate to one another to form an actionable framework.

(1) **General provisions.** These state the purpose of the plan, its drafting basis, its scope of application, and its working principles. The working principles generally follow the basic principles of unified leadership with responsibility assigned by level, territorial responsibility as the primary mode with rapid response, close coordination, and reliance on science and technology.

(2) **Organizational command structure and responsibilities.** This establishes a command body matched to the level of the incident, clarifying the conditions under which the command body is stood up, the division of responsibilities among member units, and the rules for establishing an on-site communication-support command body. Particular attention is needed where multiple departments are involved horizontally (such as public security, fire and rescue, and medical services): the boundaries of communication-support responsibility and the coordination interfaces must be made explicit, to avoid gaps or overlaps in responsibility.

(3) **Prevention and early-warning mechanism.** This specifies the monitoring and early-warning mechanism for communication-network security risks, including the trigger conditions, classification standards, confirmation procedures, and notification process for warning information. Basic telecommunications operators must establish and improve network early-warning and monitoring systems capable of continuously monitoring the operating state of the telecommunications network, and must establish disaster-warning information-sharing mechanisms with relevant departments such as meteorology, seismology, and water resources, so that communication risks can be identified early.

(4) **Emergency response.** This specifies, level by level, the activation procedure, on-duty requirements, decision and deployment process, on-site command rules, and closing procedure for each response level. The design of the response procedure must balance standardization and flexibility – standardization ensures that key steps are not omitted, while flexibility allows dynamic adjustment based on actual conditions in a complex and fast-changing on-site environment.

(5) **Post-incident handling.** This covers four aspects: summary and evaluation, requisition compensation, recovery and reconstruction, and rewards/penalties and accountability. Summary and evaluation is the key mechanism for feeding real-world experience back into plan improvement; it requires statistical compilation of the losses to public telecommunications-network facilities caused by the incident, and an analysis and evaluation of how well the response was carried out, providing the basis for revising the plan.

(6) **Assurance measures.** This specifies the requirements for building emergency communication support teams, the reserve standards for emergency equipment and supplies, the coordination mechanism for transportation and power support, and channels for funding assurance. In particular, emergency communication equipment procurement should emphasize small, portable, highly adaptable equipment, forming an equipment lineup with diverse capabilities that can independently form a network.

From an analytical perspective, the core elements of an emergency communication plan can be grouped into three functional structures. **Subject and object** together form the basic participation framework of the plan, used to define the organizational system, division of responsibilities, and the object of communication support. **Goals and scenarios** form the plan's needs-analysis framework, used to define emergency communication support needs and

the conditions under which they apply. **Measures and methods** form the plan's operational-implementation framework, used to guide the deployment of communication resources, the application of technical means, and dynamic adjustment during the response process. This analytical structure can be used to check the plan's content for completeness from a system-wide perspective, avoiding the omission of key elements and improving the plan's systematic quality, executability, and practical value.

2. Drafting Process and Quality Considerations

The drafting of a communication support emergency plan should follow a standardized, systematic organizational process to ensure that the plan is scientifically sound, complete, and executable. Drafting typically begins with forming a dedicated working group whose members should include the emergency-management department, the communication regulatory department, basic telecommunications operators, and relevant experts. On this basis, a risk assessment and vulnerability analysis of the local communication network is carried out, identifying critical communication facilities, major risk sources, and the types of sudden-onset incidents that might occur, and designing the corresponding communication-support needs and response plans for typical disaster scenarios. A draft plan is then produced, followed by internal review and external expert evaluation, systematically checking the organizational mechanisms, resource deployment, technical measures, and response procedures in the plan. After further revision based on the review comments, the plan is submitted for approval and filing according to the prescribed procedure, and finally published and put into effect.

Plan quality can generally be assessed along five dimensions: scientific soundness, completeness, executability, relevance, and compliance. **Scientific soundness** emphasizes that the plan's basis, the process by which it was formed, and its response measures should conform to the actual patterns by which communication-related sudden-onset incidents unfold, and should be grounded in risk analysis and systematic assessment rather than relying solely on experience-based judgment. **Completeness** requires that the plan cover the entire process – early-warning monitoring, emergency response, communication restoration, and post-incident support – and that it clearly define organizational responsibilities, key positions, and operating procedures, ensuring that each stage connects smoothly to the next. **Executability** emphasizes that the plan must have realistic conditions for execution, including

institutional-mechanism assurance, communication-equipment and resource reserves, and a logically sound cross-department coordination process, so that the plan can actually be put into practice quickly in a real emergency environment. **Relevance** requires that the plan be customized to the local communication-network structure, disaster characteristics, and key risk sources, with dedicated response measures for critical nodes, weak links, and high-risk scenarios, avoiding the simple copy-paste use of a generic template. **Compliance** requires that the content of the plan conform to relevant laws, regulations, and industry norms — such as the *Emergency Response Law of the People's Republic of China*, the *Telecommunications Regulations of the People's Republic of China*, and the *Radio Regulations of the People's Republic of China* — ensuring that the plan's drafting and implementation are lawful and standards-compliant.

In existing emergency communication plan practice, some common issues are still worth noting. First, the classification and grading mechanism still needs further refinement. There is not necessarily a simple correspondence between the level of a sudden-onset incident and the level of communication support it requires; determining the communication-support response level purely from the incident level can easily lead to over-investment of resources or insufficient support capability, undermining the efficiency of emergency resource allocation. Second, some plans give insufficient attention to the scheduling of emergency communication resources, lacking clear resource-allocation principles, cross-department coordination mechanisms, and dynamic support systems, making it difficult to achieve rapid, unified coordination and efficient scheduling of communication resources in complex disaster scenarios. Third, some plans describe preparatory work in overly general terms, lacking targeted detail on the communication-support measures, equipment-deployment plans, and on-site networking approaches needed for different types of sudden-onset incidents, which makes it difficult for the plan to effectively guide actual emergency response and undermines its practical value and executability.

3. Review, Filing, and Dynamic Revision of Plans

A communication support emergency plan is not a one-time document but a dynamic one that must continue to iterate as internal and external conditions change. For example, the *National Communication Support Emergency Plan* specifies that the Ministry of Industry and Information Technology should

convene relevant departments and experts as needed to evaluate the plan, make appropriate revisions as circumstances change, and report the revised plan to the State Council for approval. The main circumstances that trigger a plan revision include: a major change in the scale or technical architecture of the communication network; an adjustment to the organizational command structure or departmental responsibilities; a revision of the plan above it; a drill-evaluation report revealing a major deficiency in the plan; or a revision request from a relevant government department. Among these, revision driven by drill evaluation is the most routine iteration mechanism and an important closed loop for feeding real-world experience effectively back into the plan text.

On the filing side, once a communication support plan at any level is published, it must be filed with the level above within the prescribed time limit, forming a vertically traceable archive of plans. Filing is not merely an administrative procedure – it is also an important means by which a higher-level body can check the consistency of lower-level plans, catching content that conflicts with the higher-level plan or that leaves gaps in execution.

3.5.3 Classification and Organization of Communication Support Drills

1. Purpose and Objectives of Drills

An emergency drill is a rehearsal activity in which personnel at every level of the emergency command system act out their respective responsibilities and tasks, following the emergency plan, under a preset hypothetical incident scenario. For communication support, the significance of a drill lies not only in familiarizing participants with the content of the plan, but – more importantly – in testing the gap between the plan's design and real-world operation, and in uncovering technical and management weaknesses under conditions of multi-system, multi-department coordination.

Communication support drills generally serve several kinds of objectives: testing the feasibility and workability of the plan, exposing logical flaws or missing content; assessing the performance of emergency communication equipment under real conditions, including interoperability, speed of rapid deployment, and operating stability in extreme environments; developing the technical skills and organizational coordination ability of the emergency

communication support team; testing the effectiveness of communication coordination mechanisms across departments; and accumulating case data through drills to provide a quantitative basis for dynamically optimizing the plan.

2. Drill Classification Framework

Emergency drills can be classified along three dimensions – content, organizational form, and purpose – and the combinations across these three dimensions produce a variety of drill types, as shown in Table 22.

Classification dimension	Type	Main characteristics	Typical scenario
By drill content	Single-item drill	Targets one or a few emergency functions, such as rapid-deployment operation of a particular type of emergency equipment, or communication networking for a specific scenario (e.g., underground spaces)	New-equipment validation, single-technique operational assessment

Classification dimension	Type	Main characteristics	Typical scenario
	Comprehensive drill	Covers the full set of emergency functions – early warning, emergency response, command coordination, on-site handling and rescue, support and recovery – involving multi-department coordination	Annual comprehensive emergency communication support drill, cross-regional joint drill
By organizational form	Tabletop exercise	Conducted indoors through discussion, a sand table, or computer-based simulation, without actual equipment operation; low cost and organizationally flexible	Command decision rehearsal, plan-logic testing

Classification dimension	Type	Main characteristics	Typical scenario
	Live exercise	Conducted at an actual or simulated site, involving real equipment deployment, commissioning, and operation; genuinely tests equipment performance and personnel skill	Emergency communication equipment deployment drill, live multi-system interoperability test
	Hybrid exercise	Combines tabletop and live exercise, typically using the tabletop portion to confirm the decision process and the live portion to validate technical execution	Coordinated command-decision and on-site-operation drill

Classification dimension	Type	Main characteristics	Typical scenario
By drill purpose	Assessment drill	The scenario is not disclosed in advance; the organizer injects event information under random control, genuinely testing participants' adaptability and the plan's real-world fitness	Annual surprise emergency assessment
	Demonstration drill	Executed according to a predetermined script, mainly intended to show observers a standardized emergency process, serving a publicity and training-demonstration role	Observation training, cross-department experience exchange

Classification dimension	Type	Main characteristics	Typical scenario
	Research drill	Intended to validate the feasibility of a new technical approach or the soundness of a new plan design, with an element of R&D validation	Network-entry testing of new emergency communication equipment, validation of a new interoperability approach

3. Drill Organization Process

Regardless of the drill format used, a complete emergency drill process can generally be divided into three phases: preparation, execution, and summary/evaluation.

(1) **Preparation phase.** The quality of organization during the preparation phase directly affects the effectiveness of the drill. This phase typically includes forming a drill-planning and organizing team, setting up command, planning, operations, logistics, and general-support working groups as appropriate to the scale and complexity of the drill; clarifying the drill objectives, scope of tasks, and key subjects; designing the drill scenario based on factors such as disaster type, affected area, and the extent of communication-facility damage; drafting the drill plan, script, rules, and evaluation criteria; completing the inspection and deployment of equipment, venue, and communication resources; and conducting pre-drill training and briefing so that participants fully understand the drill process, the rules, and their own responsibilities.

(2) **Execution phase.** Once the drill begins, each participating unit carries out emergency communication support actions according to the predetermined plan, including network restoration, equipment deployment, on-site networking, service restoration, and command dispatch. During execution, dedicated personnel should be assigned to control the drill scenario and inject information, dynamically releasing simulated disaster and task information to

participating teams according to the script, while simultaneously recording the entire process and monitoring safety. For live, realistic exercises, particular attention must be paid to the operating safety of communication equipment, power systems, and vehicles, to avoid equipment faults or personnel injury caused by mishandling. After the drill ends, participating units stop drilling activity in a coordinated manner and conduct an on-site summary and preliminary review.

(3) **Summary and evaluation phase.** After the drill ends, a systematic summary and evaluation should be organized promptly, sorting through and analyzing the problems exposed during the drill and identifying whether each problem lies in the plan design, organizational coordination, resource assurance, or on-site execution; assessing whether the drill objectives were met and the level of communication-support capability demonstrated; producing a formal drill-evaluation report; and putting forward targeted recommendations for revising the plan and improving capability. The summary and evaluation phase is the key stage for "using drills to drive construction and using drills to drive improvement" – its effectiveness directly determines the continuous optimization of the emergency communication support system and the improvement of real-world response capability.

3.5.4 Drill Evaluation and Continuous Plan Improvement

1. Drill Evaluation Indicator System

Drill evaluation should be built on a scientific, quantitative indicator system rather than relying solely on subjective, experience-based judgment. The evaluation indicators for a communication support drill can generally be constructed along four dimensions: timeliness, coverage quality, coordination, and plan execution. **Timeliness indicators** mainly include the time to activate the emergency response, the time to deploy communication equipment, and the time to establish a communication link, reflecting the responsiveness of the emergency communication support effort. **Coverage-quality indicators** mainly include communication coverage range, signal quality, bit error rate, voice clarity, and data transmission rate, used to assess the technical performance and support effectiveness of the communication system. **Coordination indicators** focus on the efficiency of cross-department information transfer, the ability of heterogeneous systems to interoperate, and the continuity and integrity of the multi-level command chain, used to measure organizational co-

ordination and joint support capability. **Plan-execution indicators** include the completeness of execution of key procedures, any instances of non-compliant operation, and the consistency between on-site handling and the plan's design, used to evaluate the plan's workability and real-world adaptability.

In terms of evaluation methods, a combination of approaches is typically used to conduct a comprehensive assessment, including full-process observation and recording of key drill moments by dedicated observers, automatic collection of communication-link and network-operation data through an equipment monitoring system, self-assessment and after-action review by participating personnel, and specialized review by invited independent experts. When a drill involves units outside government departments or participation by civil-society forces, an external evaluation mechanism should also be introduced to improve the objectivity and fairness of the evaluation conclusions.

2. Compiling the Evaluation Report and Attributing Problems

The drill evaluation report is a document that systematically summarizes the entire process and effect of the emergency drill; it typically includes the basic facts of the drill, an assessment of whether objectives were met, a list of problems, root-cause analysis, and recommendations for improvement. The basic facts of the drill cover the time, location, participating units, scale, and main subjects of the drill; the assessment of objectives evaluates whether the drill achieved its intended training goals and capability-testing requirements; the problem list records and organizes the problems exposed during the drill and the point at which each occurred; and the recommendations propose follow-up optimization measures targeted at the problems found.

Throughout the evaluation process, root-cause analysis is one of the most critical steps, and its accuracy directly determines how effective the subsequent corrective measures will be. Problems exposed during a drill can generally be grouped into three levels: plan design, capability building, and resource assurance. Problems at the **plan-design level** typically show up as unreasonable procedures, an unclear division of responsibilities, or flaws in the technical approach, and need to be addressed by revising and improving the plan. Problems at the **capability-building level** typically show up as unfamiliarity with technical operations, insufficient organizational coordination, or inadequate on-site handling ability, and need to be addressed by strengthening training, routine drilling, and realistic combat-style training.

Problems at the **resource-assurance level** mainly include insufficient communication equipment, incomplete spare-parts reserves, and inadequate power-supply support, and need to be addressed through resource replenishment and optimization of the support system. Only by accurately distinguishing and analyzing the root cause of each problem can corrective measures avoid staying at a superficial level and genuinely achieve continuous improvement in emergency communication support capability.

3. Dynamic Plan Optimization Based on Evaluation Results

Once the drill evaluation report is complete, the closed-loop process of plan revision must be initiated: the list of root-cause findings is checked line by line against the plan text to determine which specific clauses need revision; the plan-drafting group is organized to discuss the revision approach; and once the revision is complete, the plan is resubmitted for approval and filing according to the prescribed procedure. If the same type of problem recurs across multiple drills, consideration should be given to whether there is a deeper, systemic cause, and the direction of capability-building investment should be adjusted accordingly.

The continuous-improvement mechanism of drilling, evaluating, revising, and drilling again is an important way for the emergency communication support system to keep optimizing itself and adapting to technological evolution and changing, complex disaster environments. The relevant requirements on summary and evaluation in the *National Communication Support Emergency Plan* are precisely the institutional expression of this closed-loop management mechanism. The core value of drill evaluation lies in obtaining objective feedback through real operational processes, providing the basis for plan optimization and capability improvement. For this reason, the design of a drill scenario should have a certain degree of complexity and challenge, capable of effectively exposing weak links and potential problems in the communication support system, rather than simply repeating the validation of an already-standardized process.

3.5.5 Application of Digital Technologies in Plans and Drills

1. Digital Plans and Intelligent Decision-Assistance Systems

A plan in traditional paper form, or as a static electronic document, has inherent limitations: information updates lag behind reality, retrieval is in-

convenient, it is difficult to keep plan versions consistent across multiple departments, and in a real response it is difficult to quickly pull up the relevant response measures as on-site conditions change dynamically. A digital plan system structures and digitizes the content of the plan, enabling dynamic updates, multi-device synchronization, and rapid retrieval, significantly improving the accessibility and timeliness of the plan.

Building on a digital plan, an intelligent decision-assistance system goes a step further by introducing artificial intelligence technology to enable plan generation, dynamic adjustment, and decision-assistance functions. Based on the information reported about a sudden-onset incident (type, location, scale), the distribution of nearby communication resources, historically similar cases, and an expert knowledge base, the system can automatically generate a preliminary emergency communication support plan for the commander's reference; as on-site feedback continues to come in, the system continuously and dynamically adjusts its recommended plan, helping the commander make more accurate resource-scheduling decisions amid a rapidly changing situation. The combination of big-data platforms and large models is driving rapid advances in intelligent decision-assistance capability.

2. Simulation-Based Drilling

The introduction of simulation technology is fundamentally changing how drills are organized and how effective the resulting training is. Traditional tabletop exercises rely on manual scenario injection and verbal response, making it hard for participants to develop a sense of immersion close to a real emergency scenario; a virtual-simulation system built on 3D scene construction, by contrast, can recreate highly realistic disaster scenes — earthquake rubble, a burning building, a flooded area — greatly enhancing the immersion and training effectiveness of a drill. For example, the *Notice on Administrative Measures for Emergency Drills in Response to Urban Rail Transit Operational Incidents*, issued by the Ministry of Transport in August 2024, explicitly requires that drill centers have a dedicated emergency-drill simulation system built using techniques such as 3D scene construction and virtual reality.

3. Application Trends of Artificial Intelligence (AI) Large Models in Drill Evaluation and Plan Generation

Large AI models are opening up new directions for application in the field of emergency plans and drills. In drill evaluation, a large model can analyze

the transcripts, call logs, and operational data generated throughout a drill, automatically identify deviations at key moments, and generate a structured root-cause report, reducing the subjectivity and risk of omission inherent in manual evaluation. In plan generation, a large model can help produce a first draft of a plan based on a description of the disaster scenario, a library of historical cases, and the topology parameters of the communication system, significantly reducing the workload of plan drafting. In drill-scenario design, a large model can automatically generate a logically consistent drill script and information-injection sequence based on a specified disaster type, scale, and training objective.

At present, large models still play a supporting role in these applications, and their output must be reviewed and corrected by qualified professionals – particularly where the content touches on specific communication-system parameters or the accuracy of laws and regulations, it should not be adopted directly without review. As domain-specific pretraining data accumulates and model capability continues to improve, the depth of AI's involvement in emergency plans and drills is expected to keep increasing, gradually evolving toward the autonomous generation of executable plan proposals.

References

[1] 3GPP. TS 22.179 *Mission Critical Push to Talk (MCPTT) over LTE*; *Stage 1*[S]. Sophia Antipolis: 3GPP, 2022.

[2] 3GPP. TS 22.281 *Mission Critical (MC) Video*; *Stage 1*[S]. Sophia Antipolis: 3GPP, 2024.

[3] 3GPP. TS 22.282 *Mission Critical (MC) Data*; *Stage 1*[S]. Sophia Antipolis: 3GPP, 2024.