GSMA

White Paper

Telecoms Under Pressure: When Emergency Access Breaks Down

Copyright © 2026 GSMA

November 2026



Unlock the benefits of GSMA membership

As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis – as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit:
http://www.gsma.com/membership/

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

© GSMA 2026. All rights reserved.

Disclaimer

This document is not an Industry Specification and is not developed or maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications. The GSMA is the publisher and owner of this document, but views and opinions expressed in this report may be solely those of the author(s) and do not necessarily reflect the views of the GSMA.

This document is provided "AS IS", for information only. The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for and disclaims any liability for the accuracy or completeness or timeliness of the information contained in this document. Any use of the information contained in this document is at the user's own risk and the user assumes liability for any third-party claims associated with such use. In no event shall the GSMA be liable for any direct, indirect, incidental, special, consequential or punitive damages, or any loss of profits, revenue, data or business opportunities arising out of or in connection with the use of or reliance on this document.

No licence is granted by implication, estoppel or otherwise under any intellectual property right of the GSMA or any third party. Nothing in this document shall be construed as granting any licence or right to use any trademark of the GSMA without prior written permission. Nothing in this document is intended to confer any benefit or right on any third party.

The GSMA is under no obligation to update, revise or supplement this document. The GSMA may withdraw or modify this document at any time without notice.

Anti-Trust Notice

The information contained herein has been prepared in accordance with the GSMA's Antitrust Policy:
https://legal.gsma.com/wp-content/uploads/2025/11/Antitrust-Policy-October-2025.pdf

Acknowledgements

Authors: Tony Baird (GF Tech Ltd.) and Wayne Cutler (GSMA)

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at www.gsma.com

GF TECH LTD
RESILIENT NETWORKS STRONGER COMMUNITIES

GF Tech Ltd is an independent company, with a focus on transformation, network resilience, emerging technologies and commercial growth. Recent work includes mobile emergency-calling reliability, digital business systems, AI-enabled infrastructure and IoT applications.
The company was founded and owned by Tony Baird.

Tony is an internationally experienced technology executive with more than 30 years of leadership across telecommunications, cybersecurity, digital transformation and critical infrastructure in New Zealand, Australia and the United Kingdom. Tony was Chief Technology Officer at Optus in 2025 and previously held senior technology and wholesale leadership roles at Vodafone New Zealand / One NZ for 14 years. His experience spans large-scale network modernisation, 5G deployment, IT and digital transformation, operational resilience and the management of technology portfolios exceeding $1 billion in capital expenditure. Tony has held board and governance roles with Kordia, the Rural Connectivity Group and public safety network organisations. and holds a degree in Electrical and Electronic Engineering from the University of Auckland.

Contents

Executive summary		1
1	Introduction: when connectivity is critical	2
2	The big picture: how reliable are mobile networks?	3
3	Key factors affecting access to emergency services	4
4	Global examples of emergency access failures	5
5	A snapshot of views from mobile network CTOs	8
6	How an emergency call reaches help	11
7	Where emergency calling can fail	17
8	Technology transitions and emerging risks	25
9	Processes	30
10	Organisational structure and culture	34
11	Regulatory and policy considerations	40
12	Conclusions and recommendations	47
Appendix 1: Network timers		51
Appendix 2: Control/user and management separation		52
Appendix 3: Areas for additional standards work		54
Appendix 4: Checklist		55
References		58
Glossary		59

List of figures and tables

Figure 1:	Emerging telecoms risks: top rankings	9
Figure 2:	Typical elements of a mobile network architecture and the relationships between them	11
Figure 3:	Typical mobile network emergency calling architecture	13
Figure 4:	Typical decision flow during an emergency call	15
Figure 5:	Layered transport/IP resilience	20
Figure 6:	Processes for a governance framework	30
Figure 7:	International mobile data traffic and ARPU, 1980–2025	40

Table 1:	The six linked stages of an emergency call	12
Table 2:	A snapshot of mobile device variances and volumes	17
Table 3:	Recommendations	48
Table 4:	Network timers used in mobile networks	51

Executive summary

Emergency calling has become a critical public safety service, with reliability depending on far more than just mobile coverage. As fixed-line services and circuit-switched networks are retired, the public and first responders increasingly rely on packet-switched 4G and 5G networks, creating greater exposure to software, device, infrastructure, process and governance failures.

This paper examines how emergency calls can fail – from handsets to emergency call centres – and proposes an end-to-end resilience programme for mobile network operators (MNOs), regulators, emergency service organisations, manufacturers and suppliers.

Emergency services are obviously of vital concern to society at large. They are also of vital concern for the MNOs licensed to provide an emergency calling service, which can incur heavy penalties in the event of failure and for whom this is not just a reliability issue but a survival issue. Emergency callers and first responders may also be on the same network, which further necessitates the need for the service to work.

This paper's central shift is from measuring network availability to assuring the emergency service outcome. Its consolidated recommendations are to:

- **Test** completed emergency calls from representative devices to emergency call centres every six to 12 months, including roaming, limited service, unauthenticated and no-SIM use cases.
- **Monitor** completed call outcomes, set-up time, routing, voice continuity, location and callback rather than the status of network components alone.
- **Maintain** standards-compliant devices, coordinated device-allowing and blocking processes and common emergency call behaviour.
- **Review** packet core, voice, timing, firewall, Internet Protocol (IP) addressing and fallback behaviour after material changes.
- **Provide** base station emergency call logs, session-based alarms, automated synthetic testing and useful handset feedback.
- **Map** critical physical and logical assets, reduce common mode dependencies and separate user, control and management paths.
- **Maintain** independent recovery routes, sufficient failover capacity, site power and emergency physical access.
- **Treat** public emergency calling and responder communications as separate but interdependent life-safety services.
- **Inform** operators, suppliers, regulators, emergency services, executives and customer teams together.
- **Promote** open, anonymised, "no-blame" information sharing so that the industry can learn from failures and solutions.

While these actions cannot guarantee that failures will never occur, they can create a system in which failures are less likely, smaller in scope, detected earlier, recovered from faster and less capable of blocking access to emergency assistance when help is needed.



1. Introduction: when connectivity is critical

For most people, a mobile phone is the first, and often only, way to reach emergency help. Until relatively recently, the public relied on fixed-line services, which had emergency backup power to the device and a system approved by the regulator. Over the past few years, however, these systems have been retired and now people are increasingly reliant on 4G packet data services.

This means that the simple act of dialling an emergency number conceals a vast amount of infrastructure: radio networks, transport links, IP routing and switching systems, databases, location functions, software platforms and hand-offs between telecommunications providers anywhere on the globe and then from emergency call centres to first responders, in many cases via the same network.

Under everyday conditions, this system feels invisible. In a crisis, it becomes one of the most important pieces of national infrastructure a country can have. A failed emergency call can mean police are not dispatched, an ambulance is delayed or a fire response is held up while a caller scrambles for another way to get help. Regulators increasingly treat these failures not as routine service interruptions but as serious public safety events.

Over the past year, several outages have been reported that affected emergency call handling. All these outages occurred on IP 4G/LTE networks providing VoLTE or packet-switched (PS) emergency calling.

No circuit-switched safety net

As the sunset of 2G/3G continues and older generations of mobile technology are retired, there is no longer a circuit-switched (CS) alternative available for the provision of emergency calling. This means there is no longer a CS safety net in a growing number of markets, and people must depend on 4G PS voice services via their smartphones to complete an emergency call. PS voice infrastructure is also in the process of being augmented with 5G/VoNR.

Recent outages have shown that the risks of emergency access failures are far-reaching. The most obvious issues are coverage "black spots" or natural disasters that cause power cuts and damage towers or fibre. However, emergency access can also be thwarted by misconfigured software, overloaded backup systems, human error during upgrades or failover, incomplete network segmentation, weak coordination between operators and emergency services or simply an incompatible handset.

The stakes have risen

It is critical that PS emergency calling is reliable, resilient and works every time to avoid tragic consequences. This means that the stakes are higher, both for the provision of PS emergency calls and for the emergency responders who use these networks for public safety response.

The challenge is also becoming more urgent as communications habits have changed and infrastructure is strained, such as by severe weather events. As fixed-line services recede and societies become mobile-first, more people depend on cellular networks to access essential services in an emergency. This makes reliability even more critical. A network that is up 99.9% of the time may still fail at the exact moment people need it most.

This paper looks at all aspects of emergency calling and the end-to-end issues that need to be addressed. It begins with an overview of recent outages and reported PS emergency call issues, followed by an overview of the network ecosystem and infrastructure underpinning PS voice. It then offers recommendations to address or mitigate problem areas and strengthen network resilience for PS emergency calling, from the caller through to the first responder. Finally, it considers some of the emerging alternative technologies and methods providing access to emergency services.

The paper also draws on an anonymous survey of mobile network Chief Technology Officers (CTOs), whose perspectives show how industry leaders view the resilience, complexity and reform needs of today's emergency communications environment.

How to get the most out of this paper

Sections 6 through 11 provide an overview of each issue for context, then a **"What can fail"** section that identifies the issues that can cause an emergency call to fail. This is followed by recommendations for **MNO executives and policymakers** to improve the end-to-end performance of their technologies, systems and processes.

For an overview of the key points in this paper, please see section 12, where the recommendations from sections 6 through 11 are captured in a summary table that includes references to earlier sections for related details. Section 12 also provides references to the Appendices at the end, which identify areas where additional work on standards may be required, as well as a checklist of issues identified in this paper.

2. The big picture: how reliable are mobile networks?

4G/5G mobile networks are highly reliable systems. Modern operators design their networks with redundancy, backup power, diverse routing and extensive monitoring, and most of the time those measures work. However, the reliability of emergency calling is not measured by average experience. It is judged by whether a person can reach help immediately, under stress and often in degraded or unusual network conditions.

This distinction matters because emergency calling depends on a chain of systems, not a single network component. A handset (from anywhere in the world) must connect to an available radio network and the network must recognise the emergency call, prioritise it and route it correctly. Then, location and call data may need to be conveyed. Emergency operators must receive the call and the platform handling the traffic must remain stable, even during sudden spikes or a partial outage. Then, the emergency dispatcher must contact the emergency responder, most likely on the same mobile network.

A weakness in any part of this chain can break the end-to-end service. Standards have typically looked at interfaces between network components, not the whole ecosystem. Also, the supply chain for fixed lines was significantly less complicated than smartphone-over-radio interfaces to an IP/AI distributed, cloud-enabled system.

Reports from regulators suggest that while such failures are infrequent relative to total call volumes, they are not rare enough to dismiss, and they occur globally, in many cases with similar root causes. For example, in the UK, a BT 999 outage in 2023 disrupted nearly 14,000 emergency call attempts over a 10.5-hour period and demonstrated that a configuration error cascaded into agent logouts, dropped calls, failed transfers and a breakdown of the disaster recovery process itself. In its review of the incident, the UK telecoms regulator, Ofcom, found not only a technical failure, but also insufficient warning systems, weak procedures for assessing impact and a recovery platform that did not have sufficient capacity to meet demand[1].

Australia has seen similar vulnerabilities exposed. Large-scale outages affecting the main emergency number, Triple Zero (000), have raised questions about IP network resilience, 3G and "camp-on" fallback arrangements, change and incident management processes (common in most outages), national coordination and how effectively emergency services are protected when carrier networks suffer serious faults.

The broader lesson is that emergency calling reliability sits at the intersection of engineering, operations and governance. High uptime figures can co-exist with dangerous edge cases if systems are complex, dependencies are opaque or backup arrangements are undertested.

Mobile networks are impressive, resilient machines, but emergency access requires more than resilience. It asks them to be dependable in the rare worst moments, when failure carries the highest human cost.



[1] Ofcom. (22 July 2024). "BT fined £17.5 million for 999 call-handling failures".

3. Key factors affecting access to emergency services

There are two key factors that make emergency access more difficult to guarantee. The first is the growing complexity and interdependence of telecommunications systems. The second is the shift to a mobile-first world in which far more people rely on cellular connectivity as their primary or only means of communication.

3.1 Growing complexity

The complexity of emergency access is easy to underestimate. Behind every call made or message sent is a tightly coupled system of mobile radio access networks (RANs), core networks, transmission links, cloud-hosted functions, databases, interconnect gateways, location systems, cybersecurity controls and emergency service hand-off platforms.

As networks modernise, more of these functions become software-defined and more dependent on shared platforms, remote management and automated orchestration. While this can improve efficiency and flexibility, it also creates new ways to fail. A software configuration mistake, a routing fault or a flawed upgrade can spread far faster than a traditional hardware fault.

The BT 999 case is a prime example. What began as a configuration error did not stay contained. It caused workstations to restart, calls to drop, transfers to fail and the first failover attempt to go wrong because procedures were poorly documented and staff on duty were unfamiliar with them. Resilience was weakened, not just because a component broke but because the surrounding systems and processes were too interdependent and insufficiently prepared for a bad day.

3.2 A mobile-first world

The second factor is the shift to mobile-first in conjunction with the shutdown of circuit switching. It is a mobile, all-IP world.

In many countries, households have abandoned landlines entirely and mobile phones are now the default tool for personal, business and emergency communication. First responders are also moving to mobile networks for both voice and data services. Governments themselves have reinforced this shift by promoting digital-first services and mobile-based identity and contact channels. The public expectation is now clear: if there is an emergency, mobile phones should work.

That expectation increases the consequences of outages. Even just a few years ago, a local mobile failure might have been mitigated by a nearby fixed line. Today, a person may have no practical fallback at all, especially during travel, in remote areas or in households that depend exclusively on mobile and internet-based services. This also means failures in emergency calling are no longer a niche telecoms issue. They have become a broader question of how societies organise access to essential services.

Taken together, these two factors pose a difficult policy challenge. As the public becomes more dependent on mobile, networks are becoming more sophisticated and software-driven. This combination makes failures potentially rarer, but more systemic and damaging when they do occur. The task for standards bodies, equipment manufacturers, handset manufacturers, operators, regulators and emergency agencies is therefore not just to maintain high uptime, but to design, test and govern for the moments when complexity and dependency collide.

4. Global examples of emergency access failures

This section examines use cases that resulted in the failure of PS emergency calls. In each case, the root cause of the failure is described as well as its impact.

4.1 Australia

In Australia, the Triple Zero (000) system has been the subject of public debate because it is both a national symbol of last-resort access to help and large carrier outages have been in the news recently.

Telstra

A Telstra outage in July 2026 led to multiple emergency calls failing. In total, more than 600 Triple Zero calls were affected. This problem was caused due to a process failure that resulted in an (old) Network Timing Protocol (NTP) server resetting its "week counter" after a data overflow of a 10-bit field resulted in the server mistakenly thinking it was 2006 (1,024 weeks is 19.7 years). The server had also had other classifications modified (design changes), which meant it had become a master timer. The server then pushed its time to other servers, which eventually led to equipment outages.

This IT infrastructure failure had serious consequences given the all-IP nature of modern communications networks, which depend completely on accurate clocks and timing. The incident triggered welfare checks and renewed scrutiny of how emergency traffic is handled when normal mobile services are severely disrupted. Again, this infrastructure failure can be traced to process failures. The official report of the outage can be found here[2].

Optus

An Optus outage in Australia in September 2025 illustrates how headline network reliability can mask critical weaknesses in emergency calling. In September 2025[3], a process failure during a routine firewall upgrade meant that while ordinary voice calls were automatically rerouted, hundreds of calls to Triple Zero could not get through, leaving users across several states unable to reach police, fire or ambulance services for nearly 14 hours.

An independent inquiry found at least 10 errors in various processes and reported that around 605 people attempted to dial Triple Zero, with roughly three-quarters of those calls failing. Deaths have been potentially linked to the incident, and regulators have responded with investigations and recommendations aimed at strengthening change management, incident detection and crisis response for emergency services outages.

Although the root cause of the outage was change and incident management on a network firewall upgrade, the incident exposed frailties in mobile networks and devices in terms of their "camp-on" network selection behaviour. This resulted in changes to 3GPP standards and highlighted the end-to-end processes needed for welfare checks following failed calls.

Many useful findings were documented in the Australian Government response to the review of the 2023 Optus outage[4].

[2] Technology Audit Partners (TAP). (2026). Findings Report on the July 8th Telstra Outage.
[3] Schott, K. (2025). Independent Report – The Triple Zero Outage at Optus: 18 September 2025.
[4] Australian Government. (2024). Australian Government Response to the Bean Review Final Report.

4.2 Lack of support for PS emergency calling

In 2026, reports emerged from Australia, and later Sweden, that Android devices supported normal VoLTE but inhibited or blocked the SOS APN and only supported CS emergency calls. This caused an issue when there was no CS network, as in Australia. In Sweden, there is still a Telia 2G network, which meant that devices of the country's other three biggest MNOs moved over to Telia for emergency calls (sometimes after a delay, sometimes after SIM removal).

In some cases, device behaviour could be modified over-the-air (OTA) depending on the age of the device. In both markets, there was extensive outreach to users to inform them of the problem and necessary remedial action. Devices that behaved in this manner and could not be modified OTA were blocked from service.

Investigations revealed that device software variants, access to open market devices (imported phones) and various network and handset configurations for CS 2/3G or 4G VoLTE had contributed to the failures.

The devices block or allow PS emergency calls based on the serving network. This behaviour is non-compliant with 3GPP specifications, but reflects the fact that deployment of normal/non-emergency VoLTE predated deployment of emergency calling via VoLTE and the two call types were treated differently.

In 2026, a major European MNO reported statistics captured over a 100-day period with a single roaming partner. This MNO had both 2G and 4G networks with PS and CS emergency call support. The statistics showed a 98%/2% split of non-emergency calls handled between 4G/2G (due to a small number of inbound roamers using feature phones) while the split for emergency calls was 54% 4G and 46% 2G.

The implication is that a significant number of the VoLTE-capable devices did not support PS emergency calls and that some roaming devices do not work in the visited network. This is a general problem affecting many markets and multiple devices, and the full implications are not yet understood as the problem is masked in markets that still have CS emergency call capability.

4.3 Europe

In 2025, it was reported that three European MNOs had rejected PS emergency call attempts due to the size of the initial (SIP INVITE) message. The reason for the call rejection was the presence of user-provided location information in the message (i.e. location information via the PIDF-LO[5] message body of the SIP INVITE), which resulted in a network access side firewall simply throwing the message away.

This was done simply because the message size exceeded a threshold, without any parsing of the message content. The problem was fixed by increasing the message threshold on the firewall. In reaction to this behaviour, devices only include PIDF-LO when initiating a PS emergency call to a network known to support the functionality.

However, the GSMA has specified since 2017 that devices include location information in PRD IR.92[1]. It is that salutary standards are not being followed on user equipment (UE) to cover network non-compliance.

4.4 United Kingdom

The United Kingdom offers another, equally important lesson: even mature, heavily regulated systems can fail catastrophically when technical errors are combined with weak recovery planning.

On 25 June 2023, BT suffered a 999 outage[6] that lasted 10.5 hours and affected nearly 14,000 emergency call attempts from 12,392 different callers. Ofcom's investigation found that the event began with a configuration error on a server, but the deeper problem was that BT was not adequately prepared for this class of disruption. Warning systems were insufficient, procedures for assessing severity were inadequate and the first attempt to switch to the disaster recovery platform failed because of human error, poor documentation and unfamiliarity with the process.

Even after traffic was moved, the backup platform struggled with demand. Ofcom concluded that the potential degree of harm was extremely significant and imposed a £17.5 million fine. The significance of this case is that no single dramatic physical failure occurred. Software, process and capacity weaknesses caused the system to shut down.

[5] Presence Information Data Format – Location Object is a standard format for conveying location information in IP-based communications.
[6] UK Government. (21 March 2024). Public Emergency Call Service disruption, Sunday 25 June 2023: post-incident review.

4.5 United States

AT&T 2024 nationwide wireless outage

A Federal Communications Commission (FCC) report[7] on AT&T's 12-hour "sunny day" outage on 22 February 2024 found that all voice and 5G data services were unavailable across all 50 states, Washington, D.C., Puerto Rico and the US Virgin Islands, affecting more than 125 million devices. The incident blocked more than 92 million phone calls and prevented more than 25,000 attempts to reach 911 call centres. It also disrupted FirstNet, the dedicated network for first responders.

AT&T August 2023 911 outage in four states

In a separate case, AT&T agreed to pay a $950,000 settlement[8] after an FCC investigation into an outage on 22 August 2023 in parts of Illinois, Kansas, Texas and Wisconsin. During 74 minutes of testing on portions of AT&T's 911 network, a contractor inadvertently disabled part of the system and automatic safeguards failed, resulting in more than 400 failed 911 calls and no timely notifications to affected 911 call centres.

T-Mobile June 2020 nationwide outage

T-Mobile experienced a 12-hour nationwide outage in June 2020 that the FCC said caused a "complete failure" for more than 23,000 911 calls, with additional calls connecting without critical information such as callback numbers or location data. The carrier later agreed to a $19.5 million settlement[9] over the incident.

4.6 Learning from failure

These cases highlight several recurring themes. First, when processes either do not exist or are not properly followed, they can trigger a chain of events that have masked an underlying problem. Second, resilience is often undermined by complexity and hidden dependency. A network may appear diverse on paper but still rely on a small number of critical software platforms, backbone paths or operational teams. Third, failover is often weaker than expected and monitoring systems fail to detect masked issues, delaying fault resolution.

Backup systems may exist, but they may not have enough capacity, may not be regularly exercised under realistic conditions ("design and test for the worst and hope for the best") or may require manual steps that become error-prone during a crisis. Emergency calling has unique stakes because people often assume any mobile signal on any network will get them through. In practice, the hand-off rules, roaming arrangements and platform dependencies are complicated and can break in unexpected ways.

Global evidence suggests that emergency communications failures are rarely the result of a simple broken tower. They are usually system failures involving technology, process, governance and human response. This is why protecting access to emergency services requires more than good coverage maps or strong average uptime. It requires treating telecoms networks as critical safety infrastructure, making processes foolproof, testing them for bad days rather than normal days and designing regulation around real-world, end-to-end failure patterns rather than ideal network diagrams.



[7] FCC. (2024). FCC Issues Report on Nationwide AT&T Mobility Outage.
[8] FCC. (2024). FCC Settles AT&T 2023 911 Outage Violations for $950,000.
[9] FCC. (2021). FCC Reaches $19.5M Settlement of T-Mobile 911 Outage Investigation.

5. A snapshot of views from mobile network CTOs

Several Chief Technology Officers (CTOs) at small, mid-sized and some of the world's largest MNOs were surveyed for their views on emergency calling resilience. Given the small sample size, the responses are indicative rather than statistically representative, but offer a useful snapshot of their perspectives. A more substantive survey carried out by an independent industry body such as the GSMA would be beneficial.

The central message is that executive accountability and technical awareness are generally in place, but assurance maturity varies significantly. Several respondents reported strong architectures and monitoring, while others identified known single points of failure, limited testing, delayed visibility and the need for more rigorous end-to-end validation. Processes, both technical and company-wide, were a consistent theme.

5.1 Where responsibility lies

The majority of respondents placed executive accountability for emergency call reliability with the CTO or another technology executive, with a small minority describing accountability as shared. This indicates that technology leadership is generally recognised as the principal owner, although emergency calling depends on multiple areas working seamlessly: operations, cybersecurity, customer functions, suppliers, emergency services and regulators.

Most respondents reported end-to-end testing of emergency calling failure scenarios at least every six months. A minority stated that they tested occasionally. The results are more concerning for enterprise preparedness: only half of respondents held company-wide emergency call "fire drills" at least every six months or annually.

This is an important gap. Technical testing can demonstrate that a call path works, but an emergency access failure also requires coordinated incident command, customer communication, regulator notification, welfare check processes, supplier engagement and collaboration with emergency services. The survey suggests these capabilities are tested less consistently than the technology itself.

5.2 Architecture and assurance

Most respondents described their emergency calling architecture as strong or highly resilient. However, half selected "strong" rather than "highly resilient", meaning they still acknowledged limited single points of failure. The other half described their architecture as moderate with known single points of failure or as limited with minimal redundancy and multiple single points of failure, while some reported no known single points of failure and full redundancy. This demonstrates the importance of Architecture Review Boards (ARBs) and standards.

Almost all respondents said they regularly review their emergency calling reference architecture; a small minority does not. This is a positive sign, but the architecture ratings suggest that a documented reference design does not necessarily indicate that recovery paths are independent, of adequate size or proven under realistic failure conditions.

Monitoring and change control processes were rated effective, near-real time or very effective by most respondents while the remainder rated them moderately effective or limited. This result was surprising given the number of outages that were triggered by process failures.

Comments from respondents identified several recurring weaknesses:

- Delays in operational data availability, including one report of roughly 30-minute delays.
- Monitoring that is insufficiently granular to isolate the impact of emergency calls.
- The absence of a unified, end-to-end service view, requiring manual "stitching" of information during incidents.
- Incomplete alarm correlation and root cause analysis.
- The lack of realistic traffic load simulation or a digital twin environment.
- The need for periodic or on-demand testing capability at radio sites.

The core message is that conventional infrastructure monitoring is not enough. MNOs need to monitor actual emergency call outcomes, including call initiation, set-up time, routing, voice continuity, location and callback capability, rather than inferring service health from alarms on individual network components.

5.3 Failure testing and transitions

The most frequently tested failure scenarios were signalling or routing errors, followed by core network and interconnect failures, software or configuration faults and power outages. More than half of respondents tested handset-related issues.

This shows a reasonably strong focus on core and routing risks, but it also reveals uneven coverage. Half of respondents did not identify handset-related testing even though device fragmentation was the most prominent emerging risk in the survey. The results support the adoption of a common minimum test catalogue covering devices, radio access, transport, power, timing, core and IMS functions, security controls, location, callback, interconnects, roaming, failover and loss of management systems.

Technology transition, rather than a traditional isolated network fault, was the dominant concern. The most frequently cited risks across the 27 ranked risk selections submitted are shown in Figure 1.

The repeated concern about device fragmentation is particularly important. Respondents highlighted inconsistent handset implementation of emergency standards, unclear fallback logic and the risk that a device remains attached to a cell that is broadcasting service but cannot complete an emergency call. One response called for device standards that support emergency call roaming fallback when a call fails – not only when no network coverage is detected.

The retirement of 2G and 3G networks was the next major concern. As CS fallback disappears, emergency access depends increasingly on correctly implemented PS emergency calling over 4G and 5G, reliable device behaviour, robust roaming arrangements and tested emergency call routing. LEO satellite integration was also frequently identified as a risk, reflecting its potential to improve coverage while introducing new questions about capacity, device behaviour, routing, location, callback and public expectations.

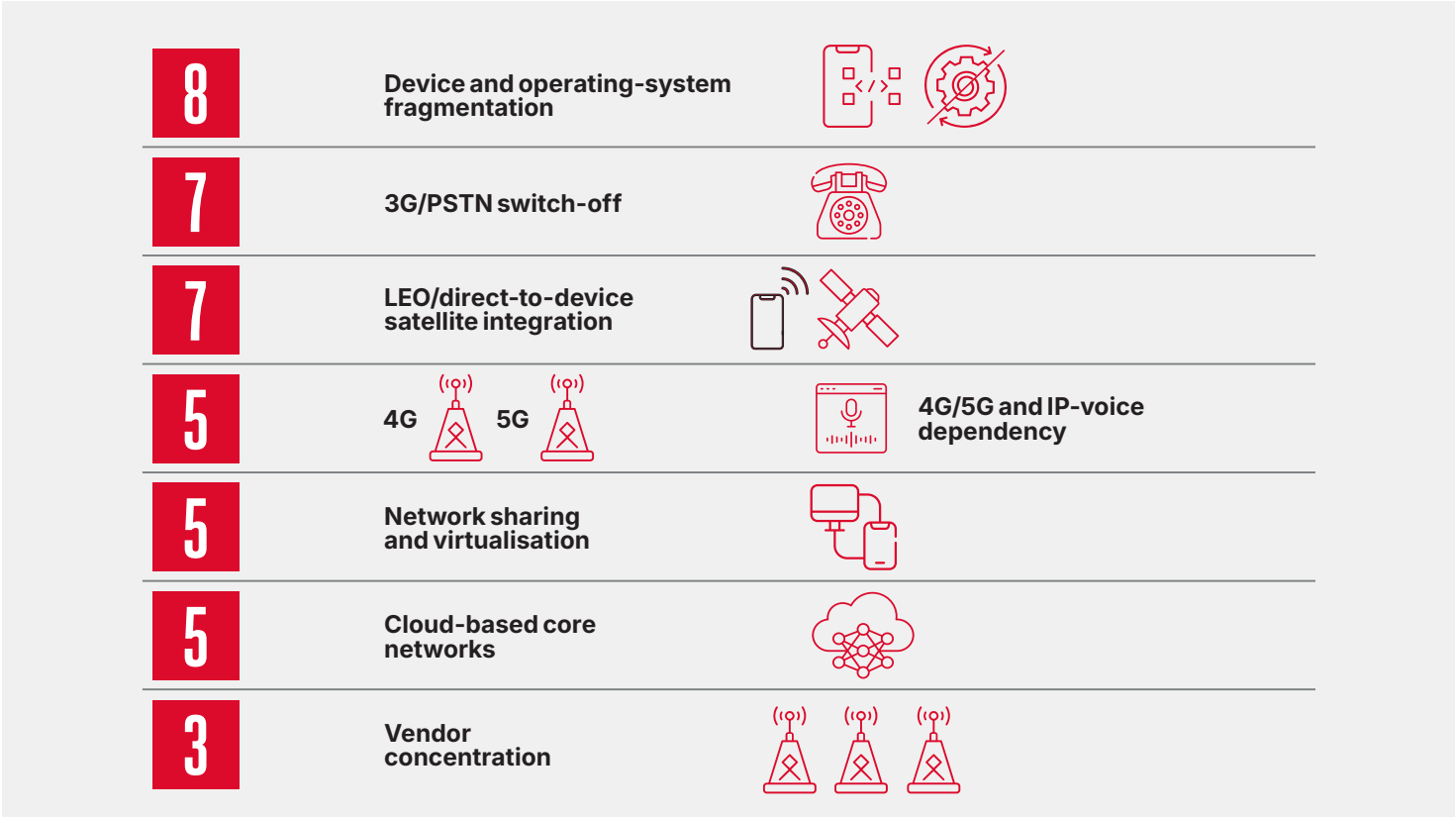


Figure 1: Emerging Telecoms Risks – Top Ranking



5.4 Main priorities

The survey responses highlight five consistent priorities:

- **Move from component monitoring to end-to-end assurance.** Respondents called for synthetic testing, more granular monitoring, automated alarms and a unified view of emergency call service performance. Advances in automation and AI will assist here.
- **Test recovery as well as failure.** Several responses stressed regular technology audits, validation of backup systems before network changes and more realistic failover exercises.
- **Address device interoperability.** There was a strong call for clearer, enforceable and internationally consistent device behaviour, particularly for fallback, roaming and emergency calling after 3G retirement.
- **Develop a shared resilience framework.** Respondents identified a gap in common reference designs that covered architectural resilience, progressive recovery, testing, operational processes, service levels and technical interoperability.
- **Strengthen cross-sector coordination.** Effective emergency calling requires closer alignment among regulators, standards bodies, operators, emergency services, device manufacturers and other technology suppliers.

One respondent summarised the underlying issue well. While existing standards may already provide many of the necessary capabilities, the industry must apply greater discipline to implementation, maintenance, testing and operational assurance. Another argued for a common framework that addresses not only technical architecture but also incident response, recovery, testing and the standards and regulatory environment.

6. How an emergency call reaches help

An emergency call is often treated as a simple event. A person dials an emergency number and is connected to police, fire or ambulance services. In reality, it is an end-to-end service that depends on many organisations, technologies and operational decisions working together in a matter of seconds.

For an emergency call to succeed, the caller's device must find a usable network, the mobile network must establish the prioritised emergency call, the call must be recognised and given emergency treatment, location and callback information must be made available where required, the call must be routed to the correct emergency call centre and the voice connection must remain usable until the caller can communicate with an operator. A fault anywhere in this chain can prevent help from being dispatched.

This section provides a simple reference model while identifying the technical dependencies that engineers must design, test and monitor. The central message is straightforward: emergency call resilience is an end-to-end outcome, not the property of any individual network component.

A network can appear healthy on conventional operational dashboards while emergency calls (due to their specific handling and low volumes) could be delayed, misrouted or unable to connect. Equally, duplicate equipment does not guarantee resilience if both the primary and backup paths depend on the same power supply, transport link, database, firewall policy, software release or operational process.

Figure 2 shows an end-to-end mobile architecture and identifies the main points at which an emergency call can fail. This provides the foundation for a more detailed failure analysis in the following section. Each block from left to right is examined as part of the entire ecosystem and call flow.

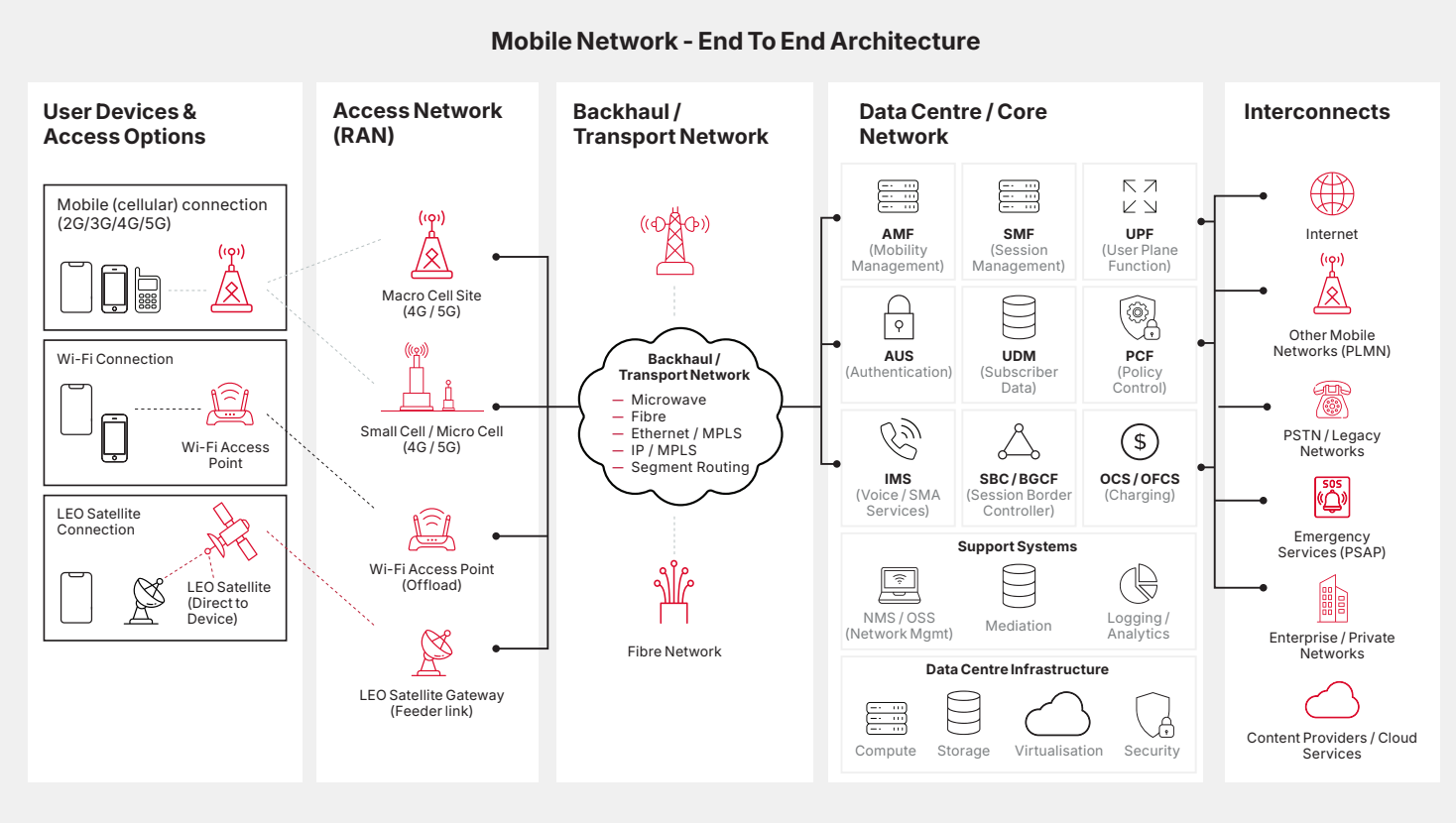


Figure 2: The typical elements of a mobile network architecture and the relationships between them

6.1 From fixed voice to a multilayered digital service

Traditional fixed-line telephony was relatively simple: a telephone was connected by a dedicated copper line to a local exchange and, in many cases, received power over the copper lines from the network. The service was limited as it was tied to a location, but the call path was relatively direct and the number of technical dependencies was limited.

Modern communications networks offer far greater mobility, capacity and functionality. Emergency calling now depends on a much more complex combination of radio networks, fibre and microwave links, IP transport, cloud or data centre platforms, databases, security systems, software-defined network functions, interconnects and emergency service systems. The transition away from 2G and 3G CS voice also makes packet-based voice over 4G and 5G increasingly important and, in the absence of CS emergency calling, essential.

New access technologies add value and complexity. Wi-Fi calling can provide service indoors where mobile coverage is weak, and private 5G networks are emerging for remote and stand-alone environments. Non-terrestrial networks (NTN), including low Earth orbit (LEO) satellite services, may provide a complementary path in remote areas or after disasters. Yet neither is equivalent to terrestrial mobile emergency calling; each has distinct dependencies, user device behaviours, location capabilities and regulatory arrangements. In many cases, these alternative systems also have different behaviours and standards than the mobile network emergency calling process.

For MNO leaders, the implication is clear: emergency call assurance can no longer be based solely on the availability of a radio site, mobile core node or emergency call gateway. It must test the completed service experienced by the person asking for help.

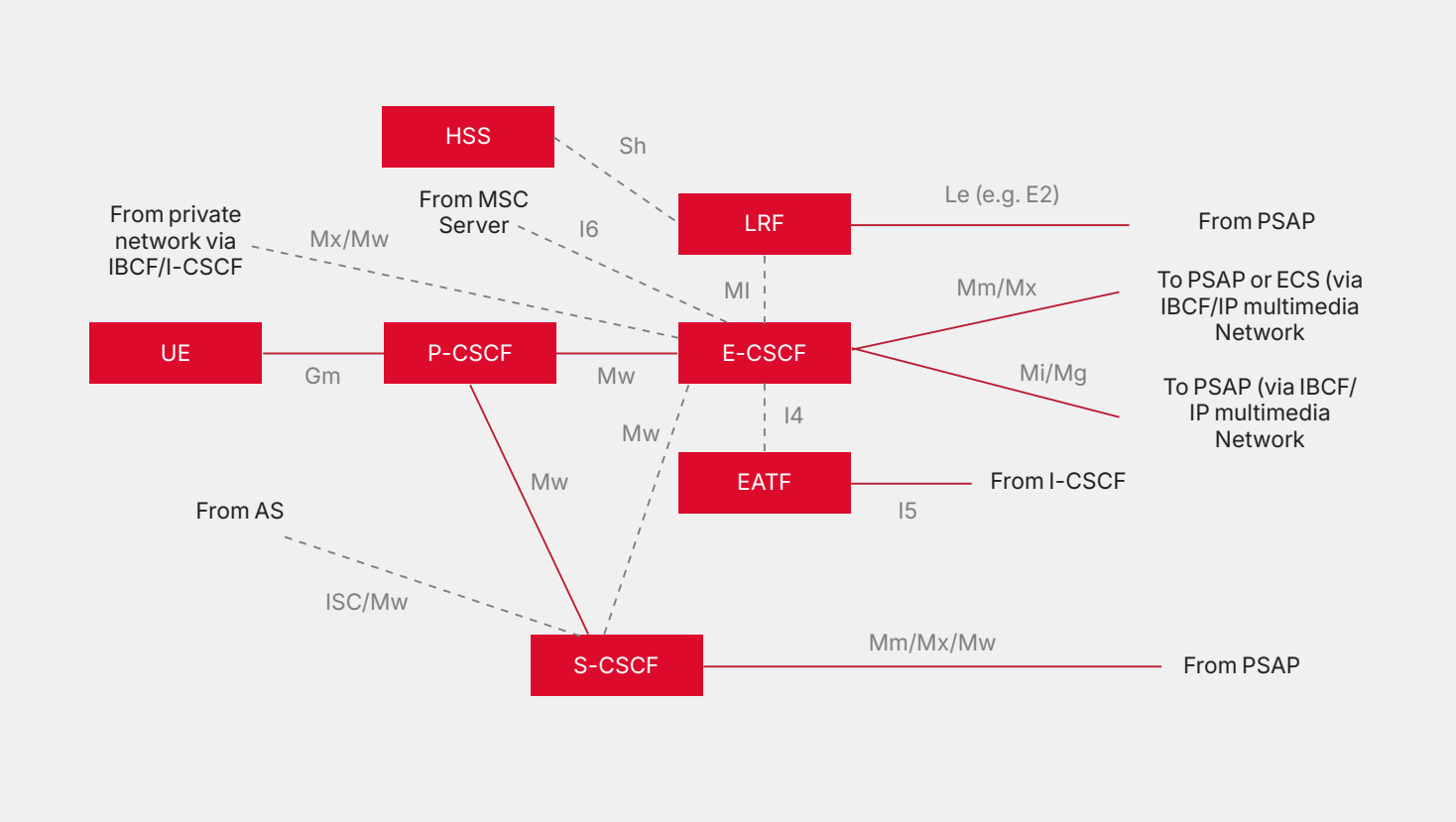
6.2 The emergency call service chain

A successful emergency call normally passes through six linked stages. The technologies differ across countries and operators, but the resilience questions are the same.

Stage	What must happen	Outcome of failure
1. Device and network selection (UE)	The handset must identify a usable network and initiate an emergency call, including in limited service or roaming conditions.	The device remains attached to a degraded network, takes too long to seek an alternative or cannot initiate an emergency session.
2. Radio access	The device must communicate with a functioning mobile site or other access network.	A coverage, power, radio, congestion or site configuration fault prevents the call from entering the network.
3. Transport	The call's signalling and voice traffic must travel from the site to the operator's core platforms.	A fibre cut/microwave failure, routing error, timing fault or capacity constraint disrupts call set-up or voice quality.
4. Core and voice services	The operator's packet core and voice platforms must authorise, establish and control the emergency call.	A database, DNS, firewall, security policy, software or configuration fault blocks the emergency session.
5. Location and routing	The call must be identified as an emergency call and routed to the appropriate emergency call centre with available caller details.	The call is misrouted, lacks location or callback information or cannot be transferred.
6. Emergency service hand-off	The emergency call centre must receive, answer and, where necessary, call the person back.	The call does not reach an available operator, drops during transfer or cannot support a callback.

Table 1: The six linked stages of an emergency call

Figure 3 shows an IP Multimedia Subsystem (IMS)-based network emergency calling architecture.



Source: 3GPP. TS 23.167[2]

Figure 3: Typical mobile network emergency calling architecture

The important point is that these stages are sequential and interdependent. A fault in one stage can defeat the entire service, even if the other stages remain operational. The appropriate measure is therefore not simply whether individual systems are "up", but whether a real or synthetic emergency call completes successfully from device to emergency call centre.

6.3 The main network functions

Figures 2 and 3 show the relationship between the principal network functions. The underlying 4G and 5G architecture is essentially a series of service layers that turn a dialled number into a conversation with an emergency operator.

Access network

The radio access network (RAN) is the part of the mobile network that connects phones to cell sites. It includes the radio equipment, antennas, spectrum, site power and local transmission links. For an emergency call, the access network must provide a usable connection quickly – even during congestion, partial network failure or a disaster.

A particular risk is the "black hole" condition: a mobile site may continue to advertise service to devices, but an upstream fault makes it unable to carry calls successfully. The caller may see signal bars, but the emergency call cannot progress. In shared network arrangements, operators must also test whether a failure on one operator's core or transport network permits appropriate access to another available network.

Transport network

The transport network carries traffic between cell sites, edge locations, data centres and service platforms. It commonly uses fibre, microwave and IP routing systems. Its resilience depends on physical path diversity, adequate capacity, routing behaviour during a fault, power, timing and the ability to manage the network while normal services are disrupted.

A transport network may be able to pass some data while still failing a time-sensitive voice service. For example, loss of synchronisation can degrade radio operation while a routing or security policy change can isolate a large area far beyond the original fault location.



Mobile core and voice platforms

The mobile core manages a device's connections to the network and provides the packet data session on which modern voice services depend. IMS is the service control environment used for VoLTE and VoNR, which establishes the voice session, applies policy and connects the call to other networks and services.

For emergency calling, specialised functions recognise the call as urgent, obtain available location and routing information and direct it to the appropriate emergency call centre. The key IMS element for emergency call handling is the E-CSCF (Emergency Call Session Control Function). Other IMS functions manage device-facing connectivity and broader session control.

The underlying risk is that a call can fail because a supporting database, Domain Name System (DNS) lookup, firewall policy, certificate, location service, session border controller or software configuration fails, even though radio access and ordinary data traffic may still appear functional.

Emergency service interconnection

The final network stage links the operator's emergency call platform to the public safety answering point (PSAP) – the organisation or centre that receives emergency calls. This hand-off must deliver more than voice where national arrangements require it: it may also need to provide the caller's location, phone number or a temporary callback identity. The regulatory requirements applicable to the PSAP can vary by region, therefore, every market or region requires tailored testing.

A call that reaches a network gateway but cannot be routed to an available PSAP, cannot provide a usable location or cannot support a callback is a public safety failure. End-to-end testing must therefore include the operator-to-PSAP interface, not just the operator's internal network.

6.4 What happens during an emergency call

In a conventional 4G or 5G mobile emergency call, the following events occur within seconds:

- The handset searches for and selects an available mobile network. This permits emergency access even if the person is not a normal subscriber, including terminating an existing connection if connected for Wi-Fi calling.
- The handset establishes radio access and a packet data connection suitable for the emergency service.
- The network identifies the request as an emergency call and establishes a voice session using its voice service platform.
- The emergency routing function obtains available location and routing information and directs the call to the appropriate PSAP.
- The voice path is established and the PSAP receives the call, with caller identity, callback and location information where supported.

Figure 4 illustrates these steps.

In practice, the path can vary by device, network generation, subscriber status, roaming arrangement and national emergency calling design. Some devices may attempt a legacy CS fallback where it remains available. Others may use an emergency packet data and IMS path. Wi-Fi calling and satellite-enabled services can introduce further variations.

The service should be designed to fail safely. If one path is unavailable, the handset and network should find the fastest viable alternative without leaving the caller in an extended, silent or misleading retry cycle. This is particularly important because a person under stress may abandon a call attempt, restart the handset or attempt a different emergency number before the network's fallback process has been completed.

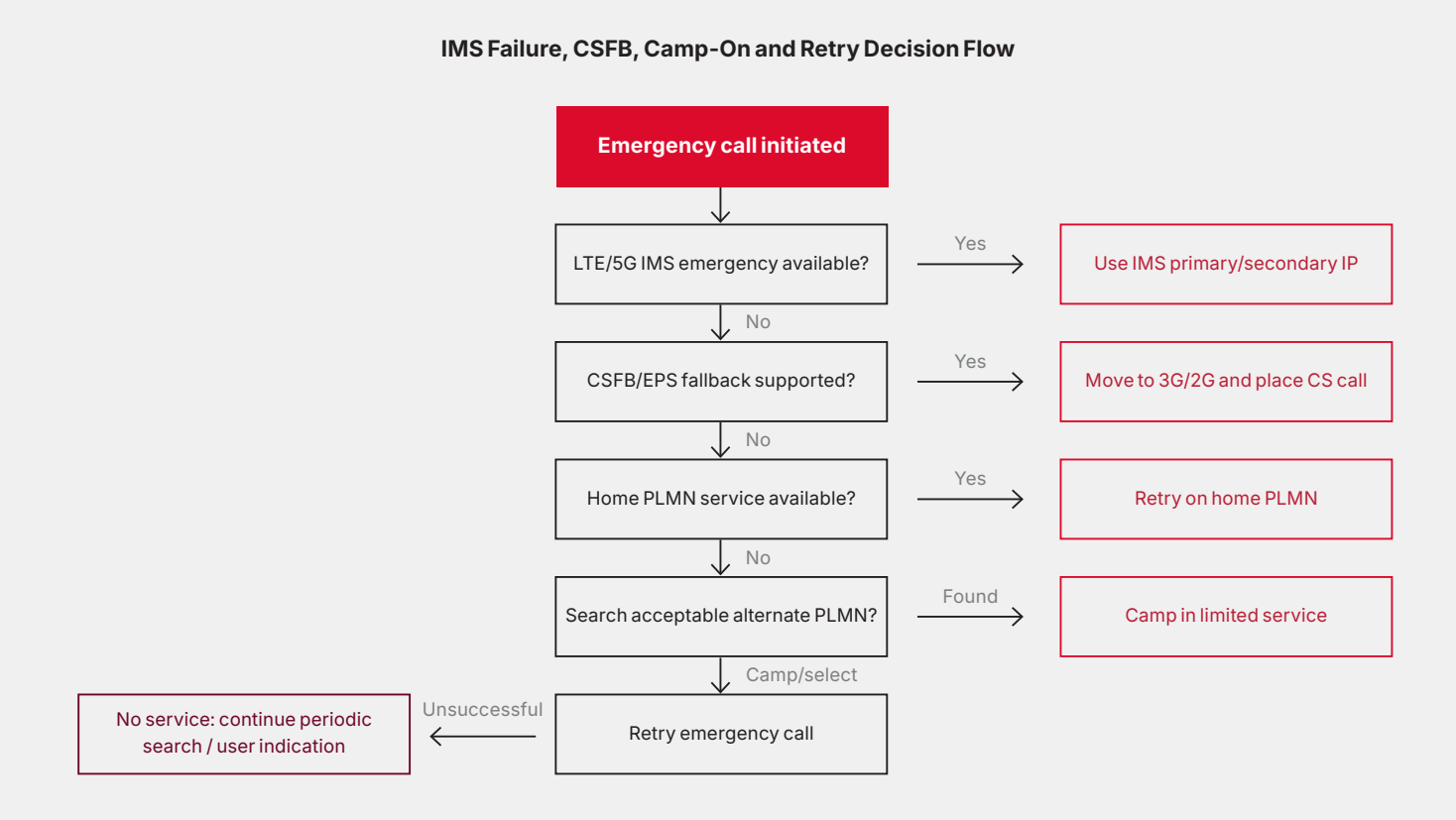


Figure 4: Typical decision flow during an emergency call

6.5 Timeouts, retries and user experience

Emergency calling is governed by many timers and retry rules in the handset and network. These determine, for example, how long a device waits for a response, when it retries a failed step and when it searches for another network or access technology. A full list of relevant network timers can be found in Appendix 1.

The underlying technical settings vary by network and device. What matters from a resilience perspective is their combined effect on the caller:

- Long timeouts can delay a move from a failed path to a working alternative.
- Multiple retries can create a long period in which the caller has no clear indication of whether help is being contacted.
- Different handset firmware and operator settings can produce different behaviours for the same network fault.
- A failure can be explicit, allowing fast fallback, or silent, causing the device to wait until a timeout expires.
- IPv4 and IPv6 address allocation, DNS resolution and security controls can each affect whether the emergency session is established successfully.

There is no single, universal emergency call timer that can simply be standardised. Rather, operators should understand and test the sequence of timers, error messages, fallback rules and retries across their deployed device population and network configurations.

What MNO executives should require:

- Establish performance targets for end-to-end emergency call set-up and completion, including during network degradation.
- Test representative devices, operating system versions, carrier profiles, roaming states and limited service conditions.
- Test explicit rejection, silent packet loss, partial connectivity and black hole scenarios, not only complete component failure.
- Monitor actual emergency call outcomes, including set-up time, routing, voice path continuity, location and callback capability.
- Review timer, retry and fallback behaviour after material changes to devices, radio configuration, core platforms, security controls or IP addressing.
- Provide clear, actionable handset feedback where feasible when an emergency call is being connected, delayed or redirected.

6.6 A practical leadership test

For Chief Executive Officers (CEOs), boards and senior executives, the most useful question is not whether the network contains redundant equipment. It is whether the organisation can demonstrate, through independent and repeatable tests, that a member of the public can reach emergency services when expected systems are unavailable or degraded.

That test should include realistic scenarios: a failed radio site, loss of transport, a core or IMS platform fault, a faulty firewall or configuration change, loss of a location service, a congested or unavailable emergency interconnect, roaming and limited service calls and loss of normal management or communications channels. Since a number of emergency access failures have been attributed to faulty processes, these should also be audited as part of normal governance.

The next section examines these points of failure in detail, considering the technical, operational and governance weaknesses that can turn a local fault into an emergency access failure, and the controls required to prevent, detect and recover from them.



7. Where emergency calling can fail

The most significant failures in a mobile network are often not caused by a single broken cell site. They arise when a fault, software change, shared dependency or recovery process affects several parts of the service chain at once. A network can show normal availability for many users while emergency calls fail at a specific point in their journey.

This section identifies the main points of failure. It is intended to help executive leaders ask the right assurance questions and help technical teams focus their design, testing and monitoring on the outcome that matters: whether a person can reliably reach emergency services under normal, degraded and failure conditions.

The appropriate measure of resilience is not whether individual network components are operational. It is whether an emergency call can be established, routed, located, answered and, when necessary, called back.

The following sections follow the path of an emergency call, from a user's handset through to radio access and transport networks, core and voice platforms and, finally, to the emergency call centre. They also address the operational systems and shared dependencies that can turn a local problem into a widespread public safety incident.

7.1 User devices: the first point of failure

The emergency call journey begins with the user's device. Mobile handsets are not uniform end-points. A comparatively small number of global manufacturers produce thousands of device models, software versions, carrier configurations and chipset combinations. Each can behave differently when attempting an emergency call, particularly during network degradation, roaming or technology transition.

The result is a critical but sometimes overlooked risk. A phone may display a signal yet fail to establish an emergency call quickly. It may remain attached to a network that cannot complete the call, delay before searching for an alternative or follow a fallback sequence that no longer works after a legacy network shutdown.

Category	Approximate number	Notes
Major global handset manufacturers	10–15	Apple, Samsung, Google, Motorola, OPPO, vivo, Xiaomi, HONOR, Huawei, Sony, Nokia (HMD), etc.
Active handset models	>20,000	Includes legacy and current devices worldwide
Android variants	>10,000	Firmware differs by operator, country and software release
iOS variants	5–10	Apple maintains relatively consistent software versions
Mobile operating systems	3 major	Android, iOS and HarmonyOS (plus legacy operating systems)
Major chipset suppliers	<10	Qualcomm, MediaTek, Apple, Samsung Exynos, Google Tensor, HiSilicon and Unisoc

Table 2: A snapshot of mobile device variances and volumes

What can fail

Non-compliance with standards. Some mobile devices do not fully comply with standards for PS emergency calls. This includes:

- Not taking note of the local emergency number list provided by the network during attachment. This can cause local emergency numbers to be treated as non-emergency numbers with delayed emergency set-up or even call failure.
- Not providing location information via the PIDF-LO message body for emergency calls. This is reported to be done either on the basis of the known capability of the serving network or whether the HPMN supports location information. Regarding the PIDF-LO, an emergency call attempt can occasionally be delayed while a device obtains location information. This is not sensible as the connection to the emergency operator is of prime importance and should not be delayed. Further, the location information can be subsequently signalled during the emergency session. This point needs to be clarified in standards.

Network selection and fallback. A device may remain connected to a degraded network rather than promptly seeking another available network for emergency access. These selection steps can take significant time and occasionally results in the caller terminating and recommencing the process. SIP retransmission timers via UDP/TCP can also incur significant delay and 3GPP standards related to PS emergency session retry are not always implemented correctly. There is a need to focus on the compliance of deployed devices and to determine whether further clarifications or improvements are required in emergency call standards.

Device software and carrier settings. Operating system releases, modem firmware, carrier profiles and network settings can alter emergency registration, retry and fallback behaviour.

Legacy technology or fallback. Some devices depend on CS fallback to 2G or 3G for emergency voice. As these networks are retired, the device must support PS emergency calling over 4G or 5G.

Interoperability. A device that supports ordinary 4G voice must also support all emergency calling functions, particularly on a visiting network or with an unusual carrier configuration. This is not always the case.

Roaming and limited service. An inbound roamer, a person without a valid subscription or a device in limited service mode can have a different emergency call path than a non-roaming user. In some cases, the messages can be configured differently, resulting in failures.

User experience. During an emergency, a long silent delay or unclear display may lead the caller to abandon the attempt, restart the device or try another number before the network has completed its fallback process.

What MNO executives should require

Operators should manage device diversity as a resilience issue, not merely a product certification issue. This means:

- Compliance to standards and associated testing to prove compliance. This includes maintaining a risk-based test portfolio that reflects the devices, operating systems and carrier profiles used in the market and, where possible, standardise across the industry with a list of approved devices and emergency numbers (911, 000, 999, 111, etc.)
- Testing emergency calling after material device, software, radio, core network or configuration changes.
- Including roaming, limited service, no-SIM and legacy fallback scenarios in test plans.
- Testing the time taken to establish an emergency call, not simply whether a call is eventually completed.
- Working with device manufacturers and standards bodies to ensure consistent emergency call behaviour without regional or country-specific variants. Also provide testing of these devices in real networks and in lab environments. It is important to introduce failure responses, not just successful cases.
- Providing clear, actionable device feedback (where feasible) when an emergency call is being connected, delayed or redirected so that the caller will not hang up. This can include the caller's ability to perform self-tests (e.g. the 1280 code in Iceland is a test emergency number).
- Work with manufacturers and regulators to agree on a minimum device operating standard. This may result in country-specific lists of approved devices rather than a specific operator deciding to block the device.
- Create a global registry of device identities to enable operators and regulators to implement lists of blocked devices.
- Review alternatives to voice-based emergency calling, such as texting/messaging or apps.

7.2 Radio access: when a device has a signal but cannot reach help

The radio access network (RAN) connects a handset to the mobile network through cell sites, antennas, radio equipment, spectrum, site power and local transmission links. This is the most visible part of a mobile network, but visible coverage is not the same as a working emergency call path.

A base station may continue to advertise service even when a fault in its backhaul, core connectivity or configuration prevents calls from being completed. In this black hole condition, the device is encouraged to connect, but the network cannot carry the emergency session onwards. The caller may see signal bars and assume help is reachable when it is not.

What can fail

- **Loss of site power or physical damage.** Storms, fires, flooding, equipment faults, generator failures and access restrictions can take a site out of service.
- **Radio or software fault.** A configuration, software defect or hardware fault can stop a cell from accepting or sustaining emergency sessions.
- **Upstream disconnection.** A site can remain on air while losing the transport or core network connection required to complete calls.
- **Black hole or "sleeping cell" behaviour.** A cell advertises service but cannot provide a usable end-to-end path.
- **Congestion.** An emergency may generate a sudden local surge in call attempts, data use and device registrations. Priority mechanisms are needed to help with congestion but cannot restore a failed site, transport link or core platform.
- **Shared network dependencies.** Multi-operator radio-sharing arrangements can introduce new dependencies. A failure on one operator's transport or core network may affect the ability of its customers to access emergency calling at a shared site. This is also true when other access technologies are included (LEO Satellite D2H; VoWifi, etc.)
- **Timing and synchronisation.** Mobile radio networks require accurate time and frequency synchronisation. A site can retain IP connectivity while radio performance degrades because timing is lost or impaired.

What MNO executives should require

- Monitor whether sites can complete an emergency call, not just whether they are broadcasting radio service. This is a common issue as many alarms are ICMP (ping) "Are you alive?" rather than end-to-end session alarms that would quickly highlight call failures.
- Test loss of power, transport, core connectivity and timing from representative cell sites.
- Validate that site and network behaviour support rapid emergency fallback to another available network where this is technically and legally possible.
- Use automated or synthetic end-to-end testing from representative sites and regions, including tests during planned changes and restoration events.
- Retain local SOS logs that allow operators to investigate failed emergency call attempts quickly and accurately for follow-up.
- Treat shared RAN arrangements as shared resilience obligations, with jointly tested failure and recovery scenarios.
- Provide software to disable the cell site from emitting radio signal in any situation where calls cannot progress (known as "wilting" the site's radio). It must be noted that this is by PLMN ID (Public Land Mobile Network Identity) as some sites may have shared radios (MoCN/MORAN shared networks).
- Require equipment suppliers to have:
  - SOS access point name (APN) log files of time-stamped emergency calls
  - End-to-end session alarms, not ICMP alarms
  - Automatic emergency call test software in a base station to allow operators to automate synthetic testing

7.3 Transport, power and timing: the dependencies behind the radio network



The transport network carries signalling, voice and data between cell sites, edge locations, data centres, core platforms and emergency service interconnects. It includes fibre and microwave links, packet-routing equipment, transmission systems, power supplies, synchronisation services and network management tools.

This layer is often invisible to users, but a failure here can affect many sites and services simultaneously. The key risk is that an apparently diverse network may contain shared routes, shared equipment, shared power, common timing sources or common configuration processes.

These hidden dependencies can turn one fault or one poorly controlled change into a large outage. See Figure 5.

Note: Fast local protection contains transient failures; routed restoration and service-layer redundancy handle wider faults. Segregation of layers into blast zones can limit impact.

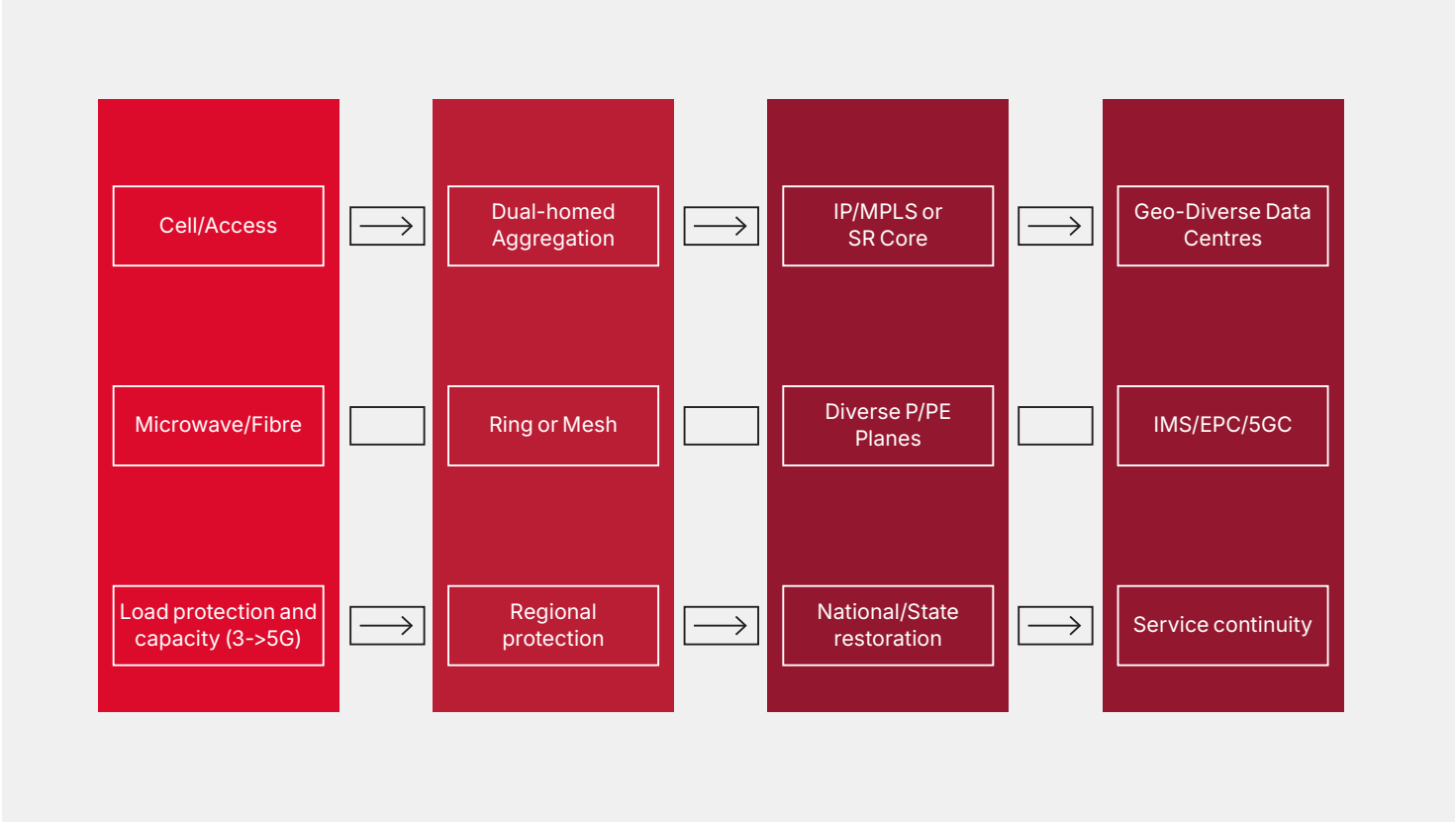


Figure 5: Layered transport/IP resilience

What can fail

- **Physical path failure.** Fibre cuts, damaged ducts, microwave link failures/congestion or loss of an aggregation site can isolate multiple cell sites.
- **Insufficient diversity.** Primary and backup paths may share a duct, route, building, power source, network device or operational team.
- **Routing and policy faults.** A routing change, software defect, incorrect traffic engineering policy or security rule can disrupt service across a wide area. In some cases, "common cause" faults may be due to a bug with a particular vendor.
- **Capacity exhaustion.** During a failure, traffic may be redirected onto backup paths that do not have enough capacity for voice, signalling and emergency demand.
- **Power loss.** Failure of grid supply, batteries, generators, fuel logistics or data centre power can remove multiple parts of the service chain.
- **Timing failure.** Loss of satellite timing, synchronisation faults or degraded timing over a packet path can impair radio service even though some traffic continues to flow.
- **Loss of management access.** If engineers lose secure access to routers, sites, logs or recovery tools, restoration can be significantly delayed.

What MNO executives should require

- Map the physical and logical dependencies supporting emergency calling, including power, timing, transport, management and third-party services.
- Test restoration under realistic traffic conditions, rather than assuming a backup route or platform will perform as designed.
- Maintain sufficient capacity for failure scenarios, including emergency call traffic and device re-registration surges. In a 5G world, microwave must be audited against capacity requirements with fibre.
- Use genuinely independent management and recovery paths – often called "out-of-band" (OOB) management – so that operators can diagnose and restore a failed network.
- Include power and other site-specific resilience in emergency call planning, especially for high-risk sites and disaster-prone areas.
- Physical site access should be included as part of critical infrastructure; this may require government support.
- Establish timing resilience through diverse sources (e.g. GPS and 1588), appropriate holdover capability and fault testing.
- Ensure adequate segregation of network functions, especially reducing geographic dependency or "blast zones" to a regional, not national, level.
- Maintain software base levels; this could benefit from automation/AI for a more standard operating environment.



7.4 Core, voice and emergency routing platforms

Once a call leaves the radio and transport network, it relies on software platforms in the mobile core and voice environment. These platforms establish the device's data connection, recognise the emergency request, control the voice session, obtain available location and routing information and send the call to the appropriate emergency call centre.

In 4G and 5G networks, voice uses the IP Multimedia Subsystem (IMS), a standards-based service control environment. The technical components may have specialised names, but the executive risk is easier to state: ordinary data service, and even ordinary voice calling, may appear available when an emergency call fails because a supporting platform, database, DNS lookup, security control or routing rule does not behave as required.

What can fail

- **Non-compliance with standards.** Some networks have not been fully compliant with standards for PS emergency calls. Examples include:
  - Lack of support for PIDF-LO location information, including in some cases rejection of emergency call attempts due to the SIP INVITE message being too large when including the PIDF-LO message body. This was caused by an access-side firewall that was blindly rejecting SIP signalling messages based on message length only. This was fixed by altering the threshold limits of the firewall (to 5,000–5,500 octets).
  - Some networks do not support the "3GPP-IMS+XML" message body to explicitly notify an inbound roamer that anonymous call should be attempted. Fortunately, devices still typically attempt the anonymous call and mask the network deficiency. The cited XML body was introduced in 3GPP TS 24.229[3] in R14 (2017).
- **Emergency session establishment.** The device cannot establish the packet data session, emergency registration or voice session required for the call.
- **Routing or location failure.** The network cannot determine where to send the call, cannot obtain suitable location information or sends the call to the wrong destination.
- **Identity and callback failure.** The emergency call proceeds without an available calling number or temporary identifier, preventing the call centre from calling the person back if the call drops. Work is currently being done on standards to improve callback success.
- **Roaming interoperability failure.** An inbound roamer requires a local emergency call path even though its ordinary voice service is controlled by its home operator. Device and network support for this path must be tested.
- **Security control failure.** A firewall, session border controller, certificate, rate limit or denial-of-service protection mechanism can unintentionally reject valid emergency signalling or media.
- **Name, database and orchestration dependency failure.** DNS, subscriber and location databases, cloud services, automation tools and certificate services can be single points of failure even when core nodes are duplicated.
- **Media failure after call set-up.** A call may appear connected but suffer one-way or absent voice because the media path, network address translation or firewall state has failed.
- **Insufficient disaster recovery capacity.** A standby system may activate but be unable to process the call volume, registrations or routing load produced during a major incident.

The common mode failure problem

A resilient service requires more than duplicate nodes. Two supposedly separate systems may still share a firewall policy, transport route, DNS service, database, orchestration platform, certificate, software defect, configuration repository or change window. In this case, one failure can disable both the primary and backup paths.

Node redundancy does not equal service resilience when critical dependencies are shared.

What MNO executives should require

- Compliance with standards. Networks need to be tested to ensure full compliance with PS emergency call standards. Compliance cannot simply be assumed on the basis that non-emergency VoLTE calls are successful.
- Test completed emergency sessions from the device to the emergency call centre, including voice, location, routing and callback, not just node availability or network "heartbeat" checks.
- Treat changes to sovereign functions, such as timing, firewall policies, certificates, DNS, session border controllers, IMS core, routing and emergency call configurations, as high-risk changes requiring explicit pre- and post-change assurance.
- Identify and reduce common mode dependencies across primary and recovery platforms, for example, emergency calling requires IPv4 and IPv6 pools for the SOS APN.
- Test failover under realistic demand, including call surges, device re-registration and partial infrastructure loss.
- Validate emergency call support for domestic and inbound roaming, including anonymous or limited service scenarios, where applicable.
- Monitor for partial success. A call set-up alone is not sufficient if the voice path, location transfer or callback capability fails.

7.5 Emergency service hand-off: connection is not the same as a successful outcome

The final stage is the hand-off from the telecommunications network to the organisation that receives emergency calls. In many jurisdictions this is a PSAP, which may be operated by police, fire, ambulance, a national emergency service or a specialist call-handling organisation.

The network's responsibility does not end when a call reaches an interconnect gateway. A public safety outcome requires that the call reaches the right call centre, that the operator can communicate with the caller and that information needed to dispatch help – especially location and a callback number – is available and usable.

What can fail

- The call is routed to the wrong call centre or cannot be transferred to the responsible agency.
- The interconnect is unavailable, congested or incorrectly configured.
- Location is missing, delayed, inaccurate or rejected by the receiving platform.
- Callback information is unavailable, particularly for roaming, anonymous or limited service calls.
- A voice session drops or becomes one-way after reaching the call centre.
- The emergency call centre is unable to receive calls at the expected capacity or cannot communicate a fault rapidly to MNOs.

What MNO executives should require

- Joint operator-emergency service testing of call routing, transfer, location, callback and voice quality.
- Clearly defined ownership and escalation procedures across operators, emergency service organisations and interconnect providers.
- Shared incident processes that rapidly identify whether a problem lies in access, transport, core platforms or the emergency service hand-off.
- Realistic capacity and failure testing, including the loss of a primary call centre or interconnect path.
- Clear public communication when alternative channels, such as text, Wi-Fi or satellite, are available but do not offer equivalent voice, location or callback capability.

See Appendix 2 for additional information on control/user and management plane separation, transport/IP protocols and network timers.

7.6 Operations, monitoring and change: how recoverable faults become major incidents

Emergency call failures are frequently prolonged not because the original technical fault is impossible to repair, but because operators cannot detect its impact on public safety quickly, assess the full scope of the problem or execute a safe recovery plan under pressure.

Traditional network monitoring often focuses on the health of individual components: whether a server responds, a router is reachable or a cell site is transmitting. These checks are necessary but insufficient. They may not reveal that emergency sessions are failing, location data is missing or calls are not reaching the emergency service platform.

What can fail

- **Insufficient service-level monitoring.** Component alarms remain normal while emergency calls fail end to end.
- **Delayed or incomplete telemetry.** Call failures are visible only after a significant delay, or data from key sites and platforms is unavailable during the incident.
- **Unsafe change.** A configuration, security policy, software or routing change has broader consequences than anticipated.
- **Weak rollback.** A recovery process is undocumented, manual, unfamiliar to staff or dependent on systems affected by the same incident.
- **Loss of operational control.** Management networks, authentication systems, collaboration tools or vendor support channels are unavailable when they are most needed.
- **Fragmented incident response.** Multiple teams act independently, creating conflicting changes and delaying escalation to executives, regulators, emergency services and the public.

What MNO executives should require

- Measure emergency call success, completion time, routing, location and callback outcomes in near-real time, end to end.
- Use independent synthetic transactions to test the complete path continuously, not just after an incident is suspected.
- Require pre- and post-change emergency call validation for changes capable of affecting access, transport, core, security, location, routing or interconnect functions.
- Separate monitoring and assurance functions from the teams implementing high-risk changes, where practical.
- Maintain independent management, communication and recovery channels, including out-of-band management, blast zones and common mode failure scenarios.
- Run regular exercises that include technical restoration, executive decision-making, regulatory engagement, public communication and welfare check processes.

7.7 Constraining blast zones and common mode failures

A blast zone is the maximum scope of service that can be affected by one fault, change or dependency failure. For emergency calling, the objective is to prevent a single incident from removing all viable paths for an entire region, customer group or emergency service function.

Blast zones can be geographical – for example, several cell sites depending on one fibre route – or logical, such as multiple core platforms sharing a database, firewall rule, cloud environment, timing source or automation system. They can also be organisational: a single vendor, team or poorly controlled change process may create a common point of failure across otherwise separate systems.

The most dangerous common mode failures are often hidden. A design may show duplication at the equipment level but not at the dependency level. A primary and backup platform that receive the same erroneous policy update, depend on the same DNS service or are restored by the same inaccessible management system do not provide independent protection.

What MNO executives should require

- Senior leaders should be able to obtain clear answers to the following questions:
- What is the largest plausible emergency calling outage that one technical fault, cyber-event, supplier failure or operational change could cause?
- Which critical dependencies are shared by primary and recovery paths?
- Can the organisation detect a failed emergency call independently of component alarms?
- Has the organisation demonstrated recovery through a realistic, end-to-end exercise rather than a desktop review?
- If the main network is degraded, what tested alternatives remain for the public, for inbound roamers and for emergency responders?

7.8 What MNO executives should require from end to end

The following actions provide a baseline for an emergency calling resilience programme:

- **Assure the outcome.** Measure and test successful emergency calling from representative devices through to the emergency call centre.
- **Test failure, not only normal operation.** Include partial failure, silent loss, black hole, overload, failover, roaming and loss-of-management scenarios.
- **Identify shared dependencies.** Map and reduce common mode risks in power, transport, timing, security, DNS, databases, cloud platforms, tools and processes.
- **Treat high-risk changes differently.** Apply enhanced review, staged implementation, independent validation and tested rollback to changes that could affect emergency calling.
- **Build device and transition assurance.** Test devices and emergency call paths as networks retire 2G and 3G, expand 4G/5G voice, introduce Wi-Fi calling and deploy satellite-enabled services.
- **Test the entire organisation.** Test technical recovery alongside emergency service coordination, regulator notification, customer communication and welfare check processes.

The next chapter considers how technology transitions and emerging access methods, including public safety mobile broadband, Wi-Fi calling, messaging and satellite connectivity, create additional opportunities and risks for emergency access.



8. Technology transitions and emerging risks

Some network reliability issues have arisen in recent years due to the interaction of emerging technology and mobile networks:

- **Emergency services** – Public safety mobile broadband networks where public safety/first responders are using the same mobile infrastructure.
- **New access technologies** that must be taken into account for the provision of emergency calling: VoWiFi and NTN-LEO Satellite D2H.
- **Alternatives to voice calls** as society moves to a digital world: voice versus data, emergency texting/ messaging and emergency apps.

8.1 Emergency services: public safety radio for emergency calling

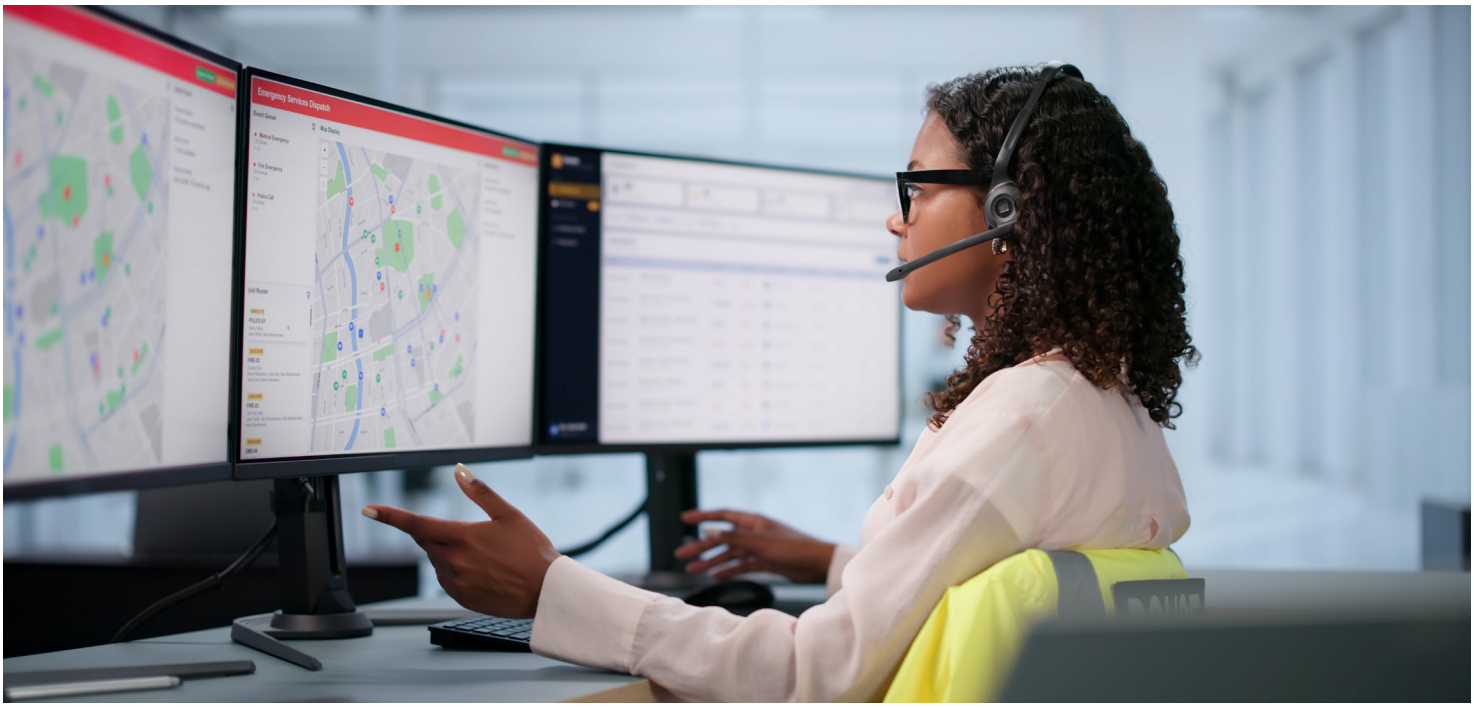
Public safety radio and other dedicated radios such as GSM-R are moving from dedicated narrowband "press to talk" LMR/TETRA/P25-style systems to PSMB and LTE/5G mission-critical services, and commercial networks are co-existing with commercial partnerships.

This transition can give police, fire, ambulance and emergency management agencies high-speed data, video, location, situational awareness and traditional mission-critical push-to-talk over mobile broadband.

However, if public safety communications share the same access, transport, core, IMS, data centre, power, security or operational systems used for public emergency calling, a single outage can simultaneously impair both sides of the emergency response chain: the public cannot call for help and responders cannot coordinate effectively.

Risks are greater than shared radio spectrum where standards have sorted quality, priority and pre-emption (QPP), and a common mode dependency should be eliminated. Emergency calling and public safety radio/ broadband can depend on the same cell sites, fibre routes, IP/MPLS network, firewalls, DNS, timing, authentication, subscriber databases, IMS/session control, packet core, monitoring systems, change processes, vendor software and incident command teams. Priority and pre-emption help during congestion, but they do not fix a failed control plane, corrupted configuration, common software defect, power failure or shared firewall outage.

The preferred architecture should therefore consider a hybrid, multilayered resilience model. Public safety users may use commercial mobile broadband for capacity



and national coverage, but emergency communications should have protected logical domains, physically diverse critical dependencies, roaming to alternative carriers, satellite and deployable cell fallback, independent operational procedures and routine multi-agency failure testing.

A regulator should refuse a shared network public safety model without evidence that emergency calling remains available and that public safety users can still communicate when the host mobile network experiences realistic failure modes.

What MNO executives should require

- Treat public emergency calling and public safety communications as two separate but interdependent life-safety services, each requiring its own reliability controls and testing from spectrum to core.
- Do not rely on priority and pre-emption as the primary resilience control. They are congestion controls, not outage controls.
- Mandate alternative carrier roaming for public safety users, including automated or policy-controlled fallback when the primary host network is unavailable or degraded. This has been successfully deployed in New Zealand as a joint venture between the country's two major MNOs. See the following case study.
- Mandate emergency calling fallback to alternative mobile networks where technically available, with tested camp-on/limited-service behaviour and clear routing rules.
- Separate critical control planes, subscriber/authentication dependencies, IMS/emergency routing functions, security zones and management systems, wherever practical.
- Where possible, deploy physically diverse transport and power for shared critical sites, plus deployable cells, satellite backhaul and direct-to-device/satellite messaging as disaster layers.
- Run joint carrier, regulator and emergency services exercises that deliberately fail the shared network and verify both citizen emergency access and responder communications.
- Create transparent outage accountability, including which party is responsible for emergency call continuity, public safety user continuity, alternative carrier roaming and restoration priority.
- As a critical service, enable operations staff to access sites during national emergencies for maintenance, such as generator deployment and refuelling.

Case study: Public safety network cellular roaming in New Zealand

New Zealand has created a dedicated, managed multinetwork service for frontline emergency responders under the national public safety network, Te Kupenga Marutau. It enables authorised devices and SIMs used by police, Fire and Emergency New Zealand, Hato Hone St John and Wellington Free Ambulance to operate across both the Spark and One NZ mobile networks.

The service, PSN Cellular Roaming, went live in July 2023 and is delivered by Hourua, a Spark-One NZ joint venture, for the government's Next Generation Critical Communications programme. It expands usable coverage, particularly in rural areas, and when the host network is unavailable it automatically reconnects the device to the other participating carrier.

The model also includes a separate cellular priority capability, live since November 2024, which gives priority to emergency service voice and data over ordinary traffic during congestion or network degradation. By December 2024, more than 22,000 users had used roaming more than 855,000 times.

A practical example of resilience was in the West Coast region. During a planned Spark outage at Fox Glacier, a Hato Hone St John responder's PSN device moved to One NZ and retained connectivity, and the same device remained connected during a subsequent local civil defence emergency when other volunteers lacked service.

Why priority and pre-emption are necessary but insufficient

Public safety broadband generally relies on quality of service, allocation/retention priority, access class barring controls, pre-emption, network slicing, dedicated APNs/DNNs and MCX priority mechanisms. These controls are essential for congestion. They do not by themselves assure resilience.

Control	Good for	Not sufficient for
QoS/ARP	Protecting critical packets during congestion	Loss of RAN, backhaul, core, IMS, DNS, power or authentication
Pre-emption	Freeing resources from lower-priority users	Common software defect, firewall block, wrong routing or failed database
Network slicing	Policy separation and traffic engineering	Shared physical infrastructure, cloud platform or operations failure
Dedicated APN/DNN	Logical separation and policy control	Shared packet core, transport, spectrum or RAN failure
MCX priority	Mission-critical group communications under load	Failure of MCX server, identity, application cloud or bearer establishment
Reserved spectrum/ capacity	Capacity assurance in busy cells	Power outage, fibre cut, core outage or cyber compromise

Multicarrier roaming for public safety users

The most important mitigation for a shared commercial host network is the ability of public safety users to roam to alternative carriers when the primary network is unavailable, degraded or congested. This should not be treated as ordinary consumer roaming. It should be a mission-critical roaming arrangement with priority, authentication, security, application reachability and operational visibility.

- Public safety SIM/eSIM profiles should support prioritised roaming to at least one alternative mobile network, and preferably two, where coverage exists.
- Roaming should include priority and pre-emption treatment where legally and commercially agreed, not just best-effort.
- Agency applications, MCX platforms, VPNs and identity systems must remain reachable when the device is on the alternative carrier.
- Roaming should be tested for loss of primary RAN, loss of primary core, congestion, home network authentication failure, DNS failure and disaster overload.
- Operational dashboards should show which public safety users have roamed and whether their mission-critical services are functional.
- Fallback rules should define whether devices automatically reselect, wait for command or use agency-controlled profiles to avoid oscillation between networks.

8.2 Alternative access technologies

As discussed throughout this paper, mobile emergency calling was historically engineered around terrestrial cellular access. The handset camps on a PLMN, establishes radio access, uses CS fallback, VoLTE or VoNR via IMS, and is routed to the emergency call service with caller identity and location information.

That model is changing. Handsets can now attempt voice and messaging through Wi-Fi calling, proprietary handset satellite messaging and emerging LEO direct-to-handset (DTH) cellular satellite systems. These technologies can materially improve emergency reachability, especially indoors, in rural areas, after natural disasters or when terrestrial radio coverage is absent. However, these same technologies can also create new failure modes.

VoWiFi depends on a third-party broadband path, home power, Wi-Fi quality, IPsec/ePDG reachability, IMS registration state, location handling and national rules about whether emergency calls are allowed over Wi-Fi. Also, the configuration of the service and the behaviour of the emergency calling standards in many cases cause the Wi-Fi connection to drop and a reconnection to be undertaken on the mobile network (which may not be present).

LEO DTH satellite depends on satellite visibility, device capability, spectrum authorisation, partner mobile network arrangements, limited capacity, messaging vs voice maturity, regulatory 000/112/911/111 routing rules and the ability to pass accurate location. Also, the DTH equipment manufacturers have different architectures (for example, SpaceX inherently has a roaming interface and AST remote antennas), resulting in different call scenarios to be tested.

The key policy conclusion is that alternative access should be treated as a complementary safety layer, not a guaranteed substitute for terrestrial emergency calling. Operators and regulators should define when each technology may be used for emergency communications, how priority and fallback behave, how the user is informed and how the service is tested across real outage scenarios.

Key findings

- VoWiFi is mature and valuable for indoor coverage, but emergency support varies by operator, device, jurisdiction and location capability. 3GPP standards mandate cellular emergency calling where any cellular access is available. However, if there is no cellular network, some devices may still terminate the VoWiFi connection and cause delays to emergency calls while network scans are completed.
- LEO DTH satellite is emerging rapidly. In 2026, Starlink/T-Mobile-style services are commercially oriented around SMS, app-limited data and Text-to-911 in selected markets, while AST SpaceMobile is positioning a broadband cellular satellite model capable of voice, video and data on ordinary smartphones.
- Satellite-to-handset services can significantly improve emergency access in coverage black spots, but they introduce lower-capacity, higher-latency, sky view-dependent access that may be unsuitable as the sole emergency call path.
- AST and SpaceX differ architecturally. In simple terms, AST uses very large phased array satellites that are designed to behave like broadband antennas in space using the partner MNO's RAN base station at an Earth station. SpaceX, on the other hand, uses a roaming handover link to the SpaceX satellite, which has the RAN base station in space. Both use the partner MNO's spectrum.
- Emergency calling policy must handle voice, text, location, callback, user interface, cross-network eligibility, unauthenticated/limited service cases, lawful intercept/security, public alerting and outage reporting.
- Regulators should mandate transparent consumer messaging. A handset showing "satellite" or "Wi-Fi calling" must not imply that all emergency voice, text and location capabilities are equivalent to terrestrial cellular service.

What MNO executives should require

- Create a technology-neutral emergency access hierarchy: cellular first where available and reliable; VoWiFi where supported and location is adequate; and satellite text/voice/data where terrestrial access is unavailable or impaired.
- Mandate emergency call test plans that include VoWiFi, cellular-to-VoWiFi transitions, no-cellular/yes-Wi-Fi, no-Wi-Fi/yes-satellite, degraded satellite, roaming and limited service cases.
- OTT apps such as WhatsApp and Snapchat need special attention and standards should be developed for emergency calling.
- Require clear regulatory treatment of LEO DTH as either part of the emergency call service, a supplementary emergency messaging service or both.
- Define minimum location and callback rules for non-terrestrial and Wi-Fi emergency access.
- Require operators to disclose capability differences to users and emergency service organisations before launch.

8.3 Alternatives to VoLTE and voice messaging

Although not widely supported, VoLTE calls can be enriched by the addition of media such as video and text (RTT). It is also possible to use SMS for emergency messaging, either independent of or complementary to the voice session. Location information (PIDF-LO) can also be sent via SMS if sent via IMS.

In addition, 3GPP has initiated a new work item aimed at R21, "Additional capabilities for emergency services". The results will be published in 3GPP TR 22.846 covering:

- Exchange of additional data related to an emergency call, including the seamless transmission of images, video and medical data in emergency services.
- Enhancements to accessibility support during emergency communications, including the negotiation of language, assistance and communication channel.
- Aspects related to emergency calls involving multiple parties to assist the caller.

Although volume is an issue, it can easily be scaled with AI, text-to-voice and other additions. Standard SMS and iMessage should be accompanied. This approach will also be more reliable for intermittent LEO coverage where a store and forward would mean the voice hold-time requirements are not needed.

OTT voice apps

OTT apps like Snapchat and WhatsApp do not have a deterministic behaviour for emergency calling and some standardisation should be mandated.

Emergency apps

With e-SIM becoming the default, it is not a great leap to have a forced app download with e-SIM registration. This could be a standard app but with geographical variants. One push, geolocation emergency service notification and video could be easily added, and health monitoring apps (for blood pressure, pulse, etc.) could also be integrated. Alarm video surveillance could also be linked to PSMB services for responders to better prepare for a given situation.



9. Processes

Processes, or process failures, are the source of the vast majority of emergency call and network outages. A network must be designed right, upgraded for new releases, capacity and other reasons, operationally managed and continually tested.

Figure 6 identifies four processes, which provide a governance framework for introducing change safely, responding to service disruption, maintaining sound technical architecture and protecting critical telecommunications services during major events.

Almost all outages and their impacts can be traced in some way to the failure of these processes, whether critical patches were not rolled out, timers were changed and never updated, architectural changes were undocumented and left dormant or no timely remedies were "pre-canned" for a natural catastrophe.

Their effectiveness depends on clear accountability, disciplined execution, timely escalation and strong feedback between operational and design teams. This is one area in which AI, automation and independent audit could help prevent outages and provide expedient responses when they occur.

What MNO executives should require

The four processes shown in Figure 6 should be in place and undergo continual review and improvement, with independent compliance audits reported on.

Process	Primary objective	Typical outputs	Key risk if weak
Change management	Introduce network, IT, cyber and service changes with controlled risk.	Approved change record, implementation plan, testing, rollback, post-change validation	Change-triggered outages, hidden dependency failures, poor rollback
Incident management	Restore service quickly and safely while managing operational impact.	Incident command, triage, restoration actions, communications, timeline and closure. Trigger business continuity and crisis management plan (BCCP) based on severity.	Slow recovery, confused ownership, unsafe concurrent actions
Architecture Review Board (ARB)	Ensure designs meet strategic, security, resilience and operability standards.	Architecture decision, exceptions, conditions, design assurance actions	Single points of failure, excessive blast zones, technical debt
Business continuity and crisis management plan (BCCP)	Maintain critical services and organisational response during severe disruption.	BCCP/disaster response (DR) activation, crisis command, stakeholder communications, recovery priorities	Uncoordinated response, prolonged service loss, regulatory and reputational harm

Figure 6: Processes for a governance framework

9.1 Change management

Purpose: To ensure planned changes to IT, cyber, network, platforms, software, configuration and infrastructure are assessed, authorised, implemented and validated with an acceptable level of service risk, and conform to the architectural standards defined by the ARB.

Core practices

- Classify changes by risk, customer impact, reversibility and urgency. Distinguish between standard, normal and emergency changes.
- Complete impact and dependency assessment across RAN, transport, core, IMS, IT, cloud, security, power, third parties and interconnects.
- Require implementation steps, pre-checks, test evidence, back-out criteria, rollback method and named accountable owners. This is especially important for emergency calling, and both manual and automatic pre- and post-change checks should be performed.
- Use change windows and freeze periods appropriate to service criticality, with additional controls for emergency calling and other regulated services.
- Perform post-change validation at the service level, not just for device or interface reachability, and review failed or high-impact changes.
- Ensure there are audited and compliant Change Review Board processes that do not allow governance to be breached (e.g. emergency changes bypassing executive sign-off, if applicable.

What MNO executives should require

- Classification of any change to sovereign functions affecting emergency calling as critical, and the use of relevant change review processes.
- Prevention of common pitfalls, including approving changes to component-level health only, inadequate dependency mapping, untested rollback, large multidomain changes, excessive emergency change bypasses and continuing implementation after warning indicators appear.
- Access to resources throughout the change window.
- Pre- and post-changes should include manual and automatic emergency calling checks and be approved as passed by the independent operations, administration and management (OA&M) team.

9.2 Incident management

Purpose: To detect and restore customer and critical service as rapidly as practical while preventing uncontrolled activity and maintaining clear operational command. This process is one of the mechanisms that will trigger the BCCP (see below).

Core practices

- Use severity levels based on user/service impact, geographic scope, regulatory obligations, duration and safety implications, and trigger BCCP if required. Appoint a single incident commander and establish defined technical, communications, vendor and regulatory workstreams.
- Prioritise service restoration before root cause analysis. Control parallel changes so that recovery actions do not compound the outage.
- Maintain a time-stamped incident log, hypotheses, decisions, actions, ownership and evidence throughout the event.
- Check emergency call volumes and failures (see above for log files on base station) and conduct relevant welfare checks and other processes.
- After restoration, conduct a blameless but accountable post-incident review with root cause, contributing factors, corrective actions and tracked closure.

What MNO executives should require

- Reviews for fragmented command, multiple teams making conflicting changes, over-reliance on infrastructure alarms, late escalation, weak customer/regulator communications and closing incidents before corrective actions are owned.
- Alarms and events that affect sovereign/critical infrastructure are flagged in OSS, inventory and asset systems.
- Timely BCCP escalation. This critical decision point cannot be overstated, and requires a one-company approach.

9.3 Architecture Review Board (ARB)

Purpose: To provide independent technical governance so that new designs and major changes align with target architecture, resilience, security, operational support and life-cycle strategy.

Core practices

- Review logical and physical architecture, failure domains, capacity, redundancy, geographic diversity, security controls and external dependencies – a simultaneous end-to-end and domain-specific view.
- Challenge blast-zone size and correlated failure modes, including shared power, timing, DNS, firewalls, load balancers, databases, cloud zones and management systems.
- Assess observability, service-level alarms, testability, rollback, maintainability and operational readiness before production deployment.
- Record architectural decisions, approved exceptions, compensating controls, expiry dates and accountable owners. Ensure there are closed-loop processes, for example, several known outages can be traced to changes that had not been updated (e.g. synchronisation architecture, network and device timers).
- Monitor and audit domains for patch levels and other "entropic" changes to network functioning.
- Feed lessons from incidents and continuity exercises back into standards, reference architectures and design patterns.

What MNO executives should require

- Elevate the ARB. Reviewing too late in the delivery life cycle, accepting redundancy claims without end-to-end failure analysis and approving temporary exceptions without remediation must be addressed by the ARB.
- Changes must be continually checked for currency, for example, temporary quick-fix changes that have not been documented.

9.4 Business continuity and crisis management plan (BCCP)

It cannot be overstated that, even with the best intentions, technology occasionally fails. As geopolitical tensions, data sovereignty concerns, global warming and natural disasters increase, public expectations of mobile networks also rise (as reflected in regulatory and other requirements). The ability to respond at an organisational level – end to end, continuously and with the correct information flows to stakeholders and customers – has never been more important.

This plan should not just cover cyber-scenarios or natural catastrophes such as floods, fires and earthquakes, but also what at first might appear mundane. A few failed calls? A customer query to a call centre? These can be considered canaries in the coal mine and should be used as random fire drills for the process.

Purpose: To sustain critical telecommunications services and coordinate executive, operational and external response when an event exceeds normal incident management capability.

Core practices

- Define critical services, maximum tolerable outage, recovery time objectives, recovery point objectives and minimum operating capability.
- Maintain tested business continuity and disaster recovery plans for sites, network platforms, IT systems, suppliers, staffing, cyber-events, natural hazards and loss of utilities.
- Establish crisis leadership, decision rights, communications protocols and clear thresholds for transition from major incident to crisis management.
- Prioritise life-safety and regulated services, including emergency calling, lawful obligations and critical government/enterprise services.
- Test plans regularly using realistic scenarios, including simultaneous failures and loss of normal communications, then close identified gaps.

What MNO executives should require

- Clear crisis authority, maintain contact lists and integrate technical recovery with executive and external communications.
- Perform fire drills on some seemingly minor outages not just major cyber-threats or natural catastrophe (NatCat) events, for example.
- Test all changes and recovery assumptions, including third-party dependencies across all departments.



How the processes work together

The processes should operate as one closed governance loop rather than as separate functions:

1. Architecture Review Board sets the design, resilience and operability requirements.
2. Change management controls how approved designs and operational changes enter production.
3. Incident management restores service when failures occur and captures operational evidence.
4. Business continuity and crisis management take command when disruption is prolonged, widespread or business-critical.
5. Lessons learned feed back into architecture standards, change controls, monitoring, testing and continuity plans.

Key organisational principle: A high-reliability telecoms culture treats availability and customer service continuity as shared engineering responsibilities. Governance should encourage early escalation, challenge assumptions, make risk visible and reward prevention and learning rather than the completion of paperwork.

10. Organisational structure and culture

Emergency calling is a life-safety service, but resilience is shaped by more than network design and technical standards. It also depends on how an organisation allocates accountability, makes investment decisions, manages suppliers, shares information, responds to warning signs and learns from failure.

For an MNO, reliable emergency access must be treated as an end-to-end organisational responsibility. No individual team controls full service. Network engineering, IT, cybersecurity, operations, customer care, procurement, legal and regulatory affairs, communications, vendors and emergency service partners each influence whether a call can be completed when the network is under pressure.

The challenge for telecoms leaders

This presents a leadership challenge. Modern telecoms networks are more distributed than the vertically integrated fixed-line networks that preceded them. They rely on software platforms, cloud infrastructure, specialist vendors, shared sites, outsourced operations, device manufacturers and interconnections with other operators and emergency services. These arrangements can bring expertise, flexibility and efficiency, but can also obscure accountability, fragment operational knowledge and create dependencies missing from conventional organisational charts.

The result is that an emergency calling failure may begin as a local engineering, software, vendor or process issue, but quickly become an enterprise-wide public safety event. Organisations that manage this risk well build a culture in which emergency call continuity is understood as a shared duty, risks are surfaced early and teams are empowered to act before a small anomaly becomes a major incident.

A resilient emergency calling service requires end-to-end accountability. Technical teams must understand the public safety outcome of their decisions, while executive leaders must ensure that commercial, organisational and operational incentives do not weaken that outcome.

10.1 From component ownership to service ownership

Telecommunications organisations have traditionally organised themselves around technology domains and functional responsibilities, from radio access to cybersecurity. However, emergency calling crosses all these boundaries.

A team may operate its own component correctly, but an emergency service can still fail elsewhere in the chain. For example, a radio site may be transmitting, a core platform may be available and a security control may be functioning as configured, yet a caller may still be unable to reach emergency services because of a routing, location, interconnect, device behaviour or failover problem.

The organisational objective should therefore be service ownership, not merely component ownership. This means assigning clear executive accountability for the end-to-end emergency call outcome, supported by named operational owners for the principal technical and external dependencies.

What can fail

- **Fragmented accountability.** Different teams own the device, radio, transport, core, security, emergency routing and customer-impact components, but no one owns the completed emergency call outcome.
- **Siloed decision-making.** A change is assessed within one domain without understanding its consequences for emergency calling across other domains.
- **Conflicting incentives.** Cost, time-to-market, network modernisation or operational efficiency targets override the investment, testing or design decisions needed for life-safety resilience.
- **Unclear escalation.** A technical issue is not recognised as a potential emergency access incident \ early enough or teams disagree about who has authority to initiate a wider response.
- **Incomplete end-to-end visibility.** Data and alarms sit in separate operational systems, leaving incident teams to manually assemble a picture of service impact.
- **Loss of organisational memory.** Temporary workarounds, historic configuration decisions and known technical exceptions are not documented, reviewed or retired as the network evolves.

What MNO executives should require

- A named executive accountable for emergency calling resilience, with authority to convene the necessary network, IT, security, operations, customer and external partner functions.
- A documented end-to-end service ownership model that identifies accountable owners for device behaviour, access, transport, core/IMS, location, routing, interconnect, monitoring, incident response and customer communication.
- Emergency call impact assessment as a mandatory part of architecture review, major investment decisions, technology retirement, supplier changes and high-risk change approval.
- A single, executive-level view of emergency call service performance, material risks, known exceptions, resilience test results and remediation actions.
- Clear thresholds for escalation from a technical fault to a public safety incident, including decision rights for customer notifications, regulator engagement and emergency service coordination.
- A closed-loop process that ensures findings from incidents, exercises, near misses and technology transitions are reflected in designs, standards, test cases and operating procedures.



10.2 Organisational design and third-party dependency

Most MNOs outsource aspects of technology service provision. The critical question is not whether a function is delivered in-house or by a third party. It is whether the operator retains sufficient technical understanding, operational authority, access to information and recovery capability to protect emergency calls when the supplier, platform or normal management process is unavailable.

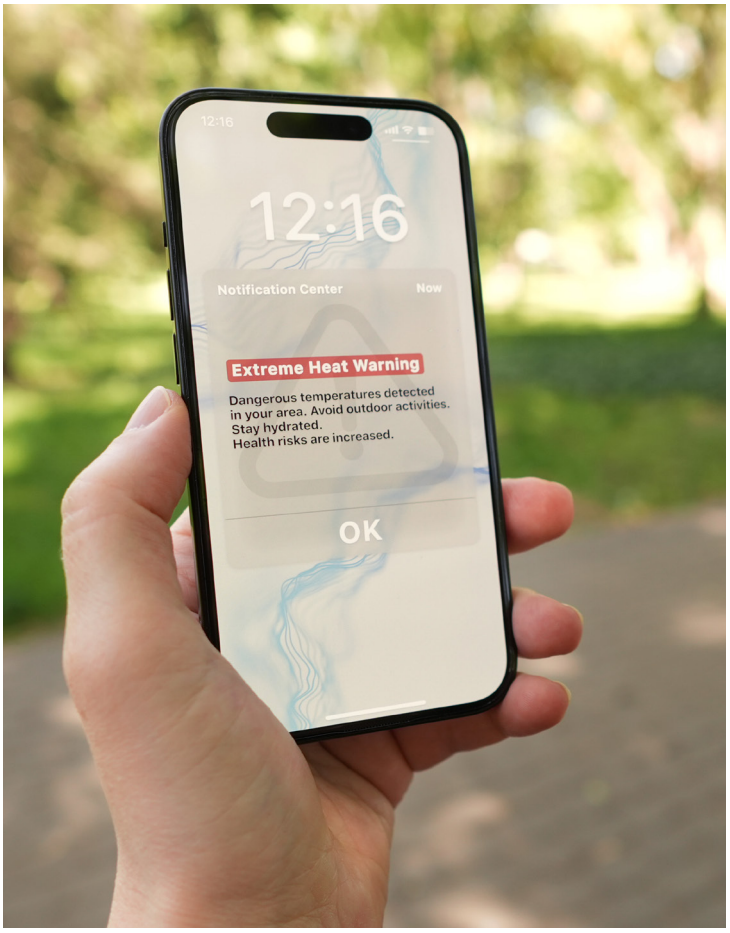
A resilience model that assumes a vendor will always be reachable, a cloud service will always be available or a subcontractor will always be able to access a site is not a complete emergency plan.

What can fail

- **Unclear supplier accountability.** Contracts specify availability of individual components but not the end-to-end emergency call service outcome.
- **Concentrated dependency.** Multiple supposedly independent functions rely on the same vendor, cloud region, software stack, management platform, field services provider or security control.
- **Insufficient operator capability.** The operator lacks the skills, system access, configuration knowledge or operational authority to diagnose and restore a critical service without the supplier.
- **Restricted access during an emergency.** Field technicians, vendors or fuel suppliers cannot reach sites or equipment during a natural disaster, security event or wider civil emergency. Noting this may require regulatory intervention.
- **Weak information sharing.** Suppliers do not provide sufficiently timely telemetry, incident data, software defect information or change impact analysis.
- **Misaligned recovery priorities.** A supplier's restoration plan does not prioritise emergency calling, critical sites or emergency service interconnects in the same way as the operator and public authorities.

What MNO executives should require

- A complete dependency map for emergency calling that covers suppliers, cloud platforms, managed services, shared infrastructure, field services, utilities, interconnects and emergency service partners.
- Contracts and operational-level agreements that specify emergency call obligations, incident notification, access to operational data, escalation routes, recovery priorities, test participation and audit rights.
- Evidence that primary and recovery arrangements do not rely on the same hidden supplier, platform, software, control plane, management path or operational team.



- Retained in-house competence and "break-glass" access sufficient to assess impact, make safe decisions and support restoration when normal supplier processes fail.
- Joint exercises with critical suppliers, including loss of supplier systems, loss of management access, cloud region failure, site access restrictions and simultaneous demand surges.
- Supply chain resilience plans for power, fuel, spares, specialist personnel, site access, transport and emergency logistics.

10.3 Culture, reporting and early escalation

The most serious emergency calling failures are rarely completely without warning. They may be preceded by failed synthetic tests, unexplained changes in call volumes, unusual device behaviour, incomplete alarms, customer reports, repeated near misses or staff concerns that do not fit the normal operational picture.

A high-reliability culture treats these signals as valuable evidence. It encourages staff and suppliers to escalate concerns early, even where the root cause is not yet known. It does not penalise teams for expressing uncertainty or stopping a change when an impact on emergency calling cannot be confidently ruled out.

This does not mean creating unnecessary alarm. It means recognising that, for a life-safety service, an unexplained anomaly should be investigated quickly and systematically.

What can fail

- **Normalisation of warning signs.** Repeated small anomalies, delayed telemetry or failed test cases are accepted as routine rather than treated as potential indicators of a larger weakness.
- **Reluctance to escalate.** Staff fear blame, commercial delay or reputational damage if they identify a risk or recommend pausing a planned change.
- **Over-reliance on dashboards.** Teams assume that normal component alarms prove the emergency service is functioning, despite incomplete end-to-end evidence.
- **Weak cross-functional communication.** Network, IT, security, customer, regulatory and communications teams do not share a common understanding of incident severity or customer impact.
- **Poor learning discipline.** Root cause reviews identify actions but do not assign owners, deadlines, assurance evidence or follow-up verification.
- **Inadequate external coordination.** Emergency services, regulators and other operators receive incomplete, late or inconsistent information during an event.

What MNO executives should require

- A just and accountable reporting culture in which staff, suppliers and partners can raise emergency call concerns without fear of blame or commercial penalty.
- Defined escalation triggers for failed synthetic tests, abnormal emergency call volumes, loss of location or callback capability, prolonged call set-up times and discrepancies between network health indicators and customer outcomes.
- A common incident operating model across network, IT, security, customer operations, legal, regulatory and corporate communications teams.
- Regular executive review of near misses, test failures, unresolved risks and overdue resilience actions, not only major outages.
- Blameless post-incident reviews that still produce clear accountability: named corrective actions, due dates, independent closure validation and board-level visibility of material risks.
- Pre-agreed communication and escalation arrangements with emergency services, regulators, major suppliers and relevant peer operators.

10.4 Investment, modernisation and resilience decisions

The transition to all-IP, cloud-enabled, software-defined and multi-access networks creates significant efficiency and capability benefits. It also changes the network's resilience profile. Decisions about 2G/3G retirement, network sharing, cloud migration, vendor consolidation, automation, security architecture and device acceptance can all affect the public's ability to reach emergency services.

Emergency calling should therefore be a formal design and investment criterion, not a late-stage compliance check. The cost of resilience may be visible in an investment proposal. The consequence of failing to invest may only become visible during a rare but severe incident.

What can fail

- **Resilience is treated as a cost centre.** Investment decisions optimise for average utilisation, short-term savings or delivery speed without adequately considering low-probability, high-consequence emergency failures.
- **Technology transitions outpace assurance.** Legacy services are retired, platforms are virtualised or functions are moved to cloud environments before device, roaming, routing and emergency call fallback are fully validated.
- **Temporary workarounds become permanent.** Exceptions introduced during deployment remain in place without review as networks, devices and regulatory requirements change.
- **Capacity is assessed only for normal conditions.** Backup systems cannot accommodate emergency call volume, device re-registration or signalling surges during a major fault.
- **Security and resilience are treated separately.** A security control reduces one risk but unintentionally blocks emergency signalling, location information, routing or voice media.
- **No independent challenge.** Architecture and investment decisions are approved without an effective review of failure domains, common mode dependencies, blast zones and recovery assumptions.

What MNO executives should require

- Emergency call resilience criteria in business cases, procurement decisions, architecture standards, network modernisation programmes and technology retirement plans.
- An independent architecture and operational readiness review for changes that could affect emergency access, including migration to cloud or virtualised platforms, network sharing and major security changes.
- Explicit testing and acceptance gates before retiring legacy emergency call paths or introducing new access technologies.
- Capacity and recovery objectives that reflect failure conditions, not only normal demand, including call surges, registration storms and loss of a major platform or interconnect.
- A time-limited exception process with compensating controls, accountable owners, review dates and executive visibility of unresolved risk.
- Investment in observability, synthetic testing, independent management access, operational training and exercises alongside investment in network capacity and new technology.

10.5 Continuous learning and whole-of-organisation exercises

A resilient organisation does not assume that a design, test plan or crisis procedure will be effective indefinitely. Networks, software, devices, suppliers, public expectations and emergency service arrangements change continuously. A control that worked during a prior incident may fail after a new device release, a change in routing, a cloud migration or a 3G shutdown.

Regular, realistic testing is therefore both a technical and cultural discipline. The CTO survey described earlier reinforces this. While most respondents reported end-to-end emergency call failure testing at least every six months, a minority reported conducting company-wide fire drills at least every six months or annually. This suggests that technical testing is more mature than organisation-wide preparedness.

What can fail

- **Testing is narrow or predictable.** Exercises confirm normal operating procedures but do not test partial failure, silent faults, shared dependencies, loss of management access or real-world decision-making.
- **Recovery is assumed rather than demonstrated.** Backup systems, alternative routes and manual procedures exist on paper but have not been operated at meaningful scale or by the staff who would use them during an incident.
- **Exercises exclude critical participants.** Suppliers, emergency service partners, customer care teams, communications specialists and executives do not participate, leaving key hand-offs untested.
- **Lessons are not embedded.** Exercise findings are documented but not reflected in training, architecture, contracts, monitoring, change processes or investment priorities.
- **Capabilities weaken over time.** Staff changes, vendor transitions and technology upgrades leave procedures out of date and key personnel unfamiliar with recovery actions.

What MNO executives should require

- A rolling, risk-based exercise programme covering technical, operational and enterprise response to emergency call incidents.
- Scenarios that include a major software or configuration error, loss of a core platform, degraded radio access, black hole cells, failure of location or routing, loss of management systems, public safety network dependency, supplier outage and a natural disaster power outage event.
- At minimum, and as part of a wider BCCP, one organisation-wide emergency calling exercise should be conducted every 12 months. This should include executive decision-making, technical recovery, customer communications, regulator notification, emergency service coordination and welfare check processes.
- Independent validation that recovery paths, manual procedures, contact lists, access credentials and escalation routes are current and usable.
- A formal lessons-learned process with named owners, dates, funding decisions and verification that corrective actions have reduced the identified risk.
- Board or executive committee oversight of material risks to emergency call resilience, test outcomes and unremedied findings.

10.6 A practical leadership checklist



Senior leaders should be able to obtain clear, evidence-based answers to the following questions:

- Who is accountable for the completed emergency call outcome across device, network, interconnect and emergency service boundaries?
- Can the organisation demonstrate through independent testing that emergency calls succeed under degraded and failure conditions?
- Which teams, suppliers, platforms and physical assets are critical dependencies, and where are the shared points of failure?
- Can the organisation detect an emergency call failure before users, emergency services or the media report it?
- Are high-risk changes independently reviewed and validated against real emergency call outcomes before and after implementation?
- Can technical teams restore the service if normal management, supplier, cloud or communications systems are unavailable?
- Have executives, engineers, customer teams, suppliers and emergency service partners exercised their roles together?
- Are known exceptions, workarounds and resilience gaps time bound, funded and tracked to closure?

A positive answer to these questions does not guarantee that an emergency calling failure will never occur. It does demonstrate that an organisation is managing the service as critical public safety infrastructure: anticipating failure, detecting it quickly, limiting its impact and recovering with discipline.

11. Regulatory and policy considerations

Emergency calling has become an essential public safety service delivered through increasingly complex, software-driven and interdependent communications networks. Yet regulatory, policy and assurance arrangements in many markets were developed for an earlier environment: one in which CS voice, fixed-line services and clearer operator boundaries provided a simpler path to emergency assistance.

That environment is changing. The retirement of 2G and 3G networks, the migration to PS voice over 4G and 5G, the growing reliance on cloud and shared infrastructure, device fragmentation and the emergence of Wi-Fi and satellite-enabled access all create new opportunities and risks. Emergency calling must therefore be governed as an end-to-end critical service, not merely as an obligation to route a call when the network is functioning normally.

Commercial reality

In most countries, competition regulators are tasked with ensuring the telecommunications market works effectively to deliver affordable, robust and affordable services, which are considered essential to the economic and social well-being of a nation.

Regulatory incentives and requirements can inform investment decisions that consider emergency calling infrastructure, processes, monitoring and reporting. However, care needs to be taken not to over-regulate the telecoms industry at a time when exploding demand for services has put growing pressure on operator revenues.

Figure 7 illustrates the challenge facing the industry: network demand is growing exponentially, but competition, regulation and commodification of telecoms services due to technological innovation has seen average revenue per user (ARPU) decrease.

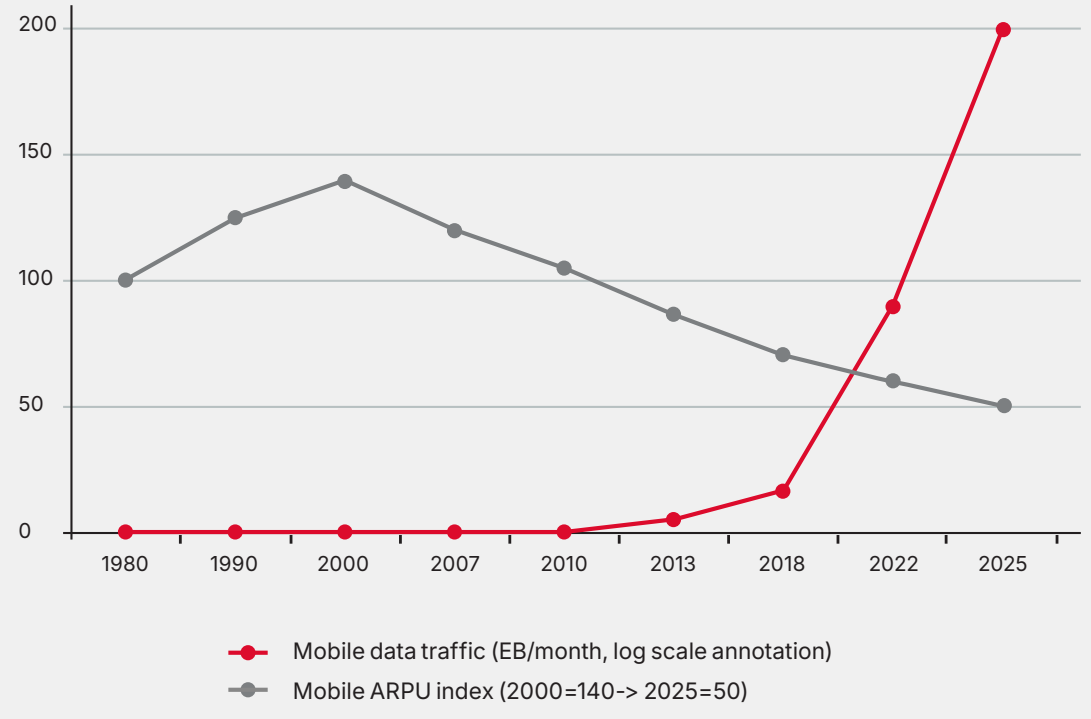


Figure 7: International mobile data traffic and ARPU, 1980–2025

What regulators need to consider

The policy challenge is not to prescribe a single network architecture or impose identical rules in every country. Markets differ by geography, emergency service arrangements, operator structure, spectrum policy, technology maturity and legal authority. The objective should instead be outcome-based: every jurisdiction should be able to demonstrate that people can reach emergency services reliably, that failures are detected and managed quickly and that responsibility is clear across the entire service chain.

Effective policy should reward resilient outcomes, require transparent assurance and create clear accountability for emergency call continuity across networks, devices, suppliers and emergency services.

11.1 Treating emergency calling as critical infrastructure

Telecommunications policy has often needed to balance affordability, competition, innovation, coverage, investment and consumer protection. These remain important objectives. However, as mobile services become the primary way many people contact emergency services, emergency calling must be treated as critical infrastructure with a distinct public safety standard.

A focus on average network availability or broad population coverage is not enough. Those measures do not establish whether a person can make an emergency call during a software fault, power outage, routing failure, partial network degradation, device interoperability problem or loss of a normal fallback path.

What can fail

- **Emergency calling is treated as a secondary service obligation.** Policy focuses on commercial service availability or coverage while failing to establish separate end-to-end requirements for emergency access. This should also accommodate physical site access during outages, as discussed earlier.
- **Legacy assumptions persist.** Requirements assume that CS voice, fixed lines or a legacy mobile network remain available as a fallback after those services have been withdrawn.
- **Investment incentives are misaligned.** Operators are expected to maintain the resilience of life-safety services, but regulatory, commercial or procurement settings do not recognise the cost of diverse paths, independent management access, testing capacity, power resilience and recovery capability.
- **Requirements are technology-specific.** Rules become obsolete as voice, messaging, Wi-Fi, satellite and other access methods develop.
- **Compliance is based on design claims.** Operators demonstrate that systems are present or standards are referenced, rather than proving that emergency calls work under representative failure conditions.

What policymakers and MNOs should require

- Define emergency calling as an end-to-end, life-safety service with explicit obligations for availability, continuity, routing, location, callback, accessibility and incident response. This can include PSAP access (via test number).
- Establish outcomes-based resilience requirements that apply regardless of access technology, while allowing implementation to reflect local market and emergency service arrangements.
- Require operators to demonstrate emergency call performance during normal operation and define degraded or failure scenarios, not just component availability or theoretical redundancy.
- Consider emergency call resilience explicitly in policy decisions affecting 2G/3G retirement, network sharing, cloud migration, infrastructure consolidation, spectrum policy and public safety communications.
- OTT apps such as WhatsApp and Snapchat need to be standardised as they are currently non-deterministic for emergency calling yet widely used as primary voice services.
- Ensure that investment and regulatory frameworks recognise the higher assurance needed for life-safety services, especially in remote, disaster-prone or low-infrastructure areas.
- Access to remote mobile sites by suitably authorised staff to repair or replace equipment to restore service.



11.2 Clear accountability across the service chain

Emergency calling crosses organisational boundaries. A successful call may depend on a device manufacturer, MNO, shared network provider, transport and cloud suppliers, emergency call platform, interconnect provider and a PSAP. During a major incident, public authorities, regulators and emergency services also need accurate and timely information.

Without a clear responsibility model, each party may meet its own contractual or technical obligations while the end-to-end service fails. Accountability must therefore be determined by the outcome: a caller's ability to reach and communicate with emergency services.

What can fail

- **No end-to-end service owner.** Responsibility is fragmented across operators, suppliers and emergency services, with no party accountable for the full outcome of an emergency call.
- **Unclear incident thresholds**. Participants disagree about when a fault becomes an emergency access incident, who must notify whom and who has authority to activate crisis arrangements.
- **Incomplete information sharing.** Operators, PSAPs and regulators cannot rapidly determine the geographic scope, affected technologies, failed call volumes, location/callback impact or available alternatives.
- **Misaligned restoration priorities.** Suppliers and network teams restore general services first while emergency routing, location, interconnect or management functions remain degraded.
- **Opaque third-party obligations.** Critical vendors and cloud, shared infrastructure or managed service providers are not required to support emergency call assurance, incident response or independent audit.

What policymakers and operators should require

- A jurisdiction-wide responsibility matrix covering mobile operators, fixed operators where relevant, device manufacturers, infrastructure and cloud providers, emergency services, interconnect providers and the regulator.
- A named accountable executive within each operator for end-to-end emergency call resilience and a defined senior counterpart within the emergency service organisation.
- Common incident definitions, escalation thresholds, notification time frames, information-sharing protocols and crisis communications procedures.
- Pre-agreed data exchange during incidents, including emergency call attempts, failures, connection times, affected locations, available fallback paths and relevant location/callback impacts.
- Contractual and regulatory obligations on critical suppliers to participate in emergency call testing, provide timely incident information and support recovery priorities.
- Joint, cross-sector exercises that test not only technical recovery but also regulator notification, public advice, welfare arrangements and coordination with emergency service organisations.

11.3 Consistent standards and interoperability

Emergency calling is global at the device and technology level, but local at the emergency number, routing, legal and public safety level. This creates unavoidable variation, and problems arise when national differences, incomplete standards implementation or unclear responsibility between device manufacturers and operators create inconsistent behaviour at the moment a person needs help.

What can fail

- **Inconsistent device behaviour.** Handsets implement emergency registration, fallback, network selection, roaming or location functions differently across operating systems, firmware versions and carrier profiles.
- **Uneven implementation of standards.** Operators, device manufacturers and suppliers interpret or implement common specifications differently, especially for emergency services, roaming and legacy network transition.
- **Country-specific fragmentation.** Devices sold across borders, open-market devices and visiting roamers encounter emergency call configurations for which they have not been validated.
- **Unclear fallback logic.** A device remains attached to a network that is visible but unable to complete emergency calls, instead of seeking an available alternative where one exists.
- **Insufficient interoperability testing.** Conformance tests focus on normal voice service or individual interfaces rather than the full outcome of an emergency call.

What policymakers and operators should require

- A common baseline of emergency call interoperability requirements for devices, networks and emergency service interconnects, with particular attention to PS emergency calling, roaming and technology transition.
- Clear, testable requirements for emergency call network selection and fallback when a home network is unavailable, degraded or unable to complete an emergency session.
- Industry-agreed test cases for no-SIM and limited service calls, domestic and inbound roaming, loss of CS fallback, black hole cells, location transfer, callback, security control failure and partial network outage.
- Greater alignment among mobile standards bodies, device manufacturers, network suppliers, operators and national emergency authorities on the interpretation and implementation of emergency call requirements.
- A process for rapidly identifying, testing and remediating emergency call interoperability defects across markets, including timely manufacturer and operator engagement.
- A common terminology and reporting framework so that emergency call failures can be compared, analysed and addressed across jurisdictions.

11.4 Device assurance and market access

A mobile device is the first link in the emergency call chain, yet it is often outside the direct operational control of the network operator. Device diversity, software updates, imported handsets and changing carrier settings can all have an impact on emergency call behaviour.

A national or regional approach to device assurance can reduce this risk. It should not unnecessarily restrict consumer choice or create duplicative testing regimes. Rather, it should establish that devices used on a network can make emergency calls reliably in the conditions for which the network was designed.

What can fail

- **Devices are approved based on ordinary service capability.** A handset is certified for data or normal voice but has not been tested for emergency calling, roaming, fallback, location or callback behaviour.
- **Software changes introduce regression risk.** Operating system, modem firmware or carrier profile updates alter emergency call behaviour after a device has been approved.
- **Open market devices bypass assurance.** Imported, grey-market or non-certified devices operate on a network without validation against local emergency call requirements.
- **Operator responses are inconsistent.** One network allows a known non-compliant device while another restricts it, creating unpredictable public safety outcomes.
- **Consumer communication is inadequate.** Users are not told when a device may have limited emergency call functionality following a network transition or software defect.

What policymakers and operators should require

- A risk-based device assurance framework covering emergency call initiation, PS emergency support, limited service, roaming, fallback, location and callback behaviour.
- A maintained and transparent register of validated devices or device configurations, where appropriate to the market, including the basis for validation and the treatment of material software changes.
- Shared processes for operators, manufacturers and regulators to identify, investigate and remediate emergency call defects.

— Requirements for device manufacturers and operating system providers to provide timely technical information, fixes and test support when an emergency call issue is identified.
— Clear, proportionate consumer communications and remediation options for known device limitations, including software updates, replacement pathways or restrictions only where necessary to protect public safety.
— Cross-operator coordination so that device treatment is consistent within a jurisdiction, wherever possible.

11.5 Cross-network resilience and fallback

A person attempting an emergency call may be unable to use their normal network because of a radio, transport, core, power or software failure. In many circumstances, another mobile network may be available. The ability to use that network for emergency access can provide an important additional layer of resilience, but it depends on technical capability, handset behaviour, roaming rules, emergency call routing and national policy.

The same principle applies to public safety mobile broadband. Priority and pre-emption are valuable congestion controls, but they do not protect against the complete failure of a shared radio, transport, core or management platform. Emergency responders and the public may require distinct but coordinated alternative paths.

What can fail

— **A device cannot move to an available alternative network.** The device remains attached to a failed or degraded home network, or fallback rules are slow, inconsistent or not supported.
— **Emergency access is not enabled in limited service conditions.** A network is technically available but does not permit or correctly route emergency sessions from non-subscribers or roamers.
— **Fallback is assumed, not tested.** Operators and regulators rely on coverage maps or standards compliance rather than end-to-end demonstrations of emergency access during real failure modes.
— **Public safety users share the same failure domain.** Emergency responders and the public depend on the same host network, control plane, power, transport or management systems.
— **Alternative technologies are misunderstood.** Wi-Fi or satellite indicators lead users to assume equivalent emergency voice, location or callback capability where this is not available.

What policymakers and operators should require

— A national assessment of the feasibility and value of emergency calling via alternative mobile networks, including technical, legal, security, spectrum, routing and emergency service implications.
— Common requirements for emergency fallback to another available mobile network when the home network is unavailable or cannot complete an emergency call. The call should also be completed in real time.
— Mandatory testing of limited service, cross-network, roaming and “visible but unable to complete” network conditions.
— Separate resilience analysis for public emergency calling and public safety responder communications, including shared infrastructure and common mode failure risks.
— Tested multinetwork or alternative access arrangements for public safety users where these form part of the national communications strategy.
— Clear public information about what Wi-Fi calling, satellite-enabled messaging and other alternative technologies can and cannot provide during an emergency.



11.6 Monitoring, testing, reporting and transparency

Emergency call failures are often difficult to detect because normal network alarms can remain green while calls fail to establish, route, deliver location or support a callback. Policy should therefore encourage a shift from component-based monitoring to service-based assurance.

The survey findings in this paper reinforce this. While 78% of respondents reported conducting end-to-end emergency call failure testing at least every six months, testing scope and whole-of-organisation preparedness varied. Only 44% reported company-wide emergency call fire drills at least every six months or annually.

What can fail

- **Monitoring measures infrastructure, not outcomes.** Operators know that nodes are reachable but do not know whether emergency calls are completed successfully.
- **Testing is intermittent or narrow.** It does not include representative devices, different access technologies, roaming, failure conditions, location, callback or emergency service hand-off.
- **Reporting is late or incomplete.** Regulators and emergency services cannot assess the potential public safety impact quickly enough to issue advice, coordinate welfare action or scrutinise recovery.
- L**essons remain private.** Similar defects recur across operators or jurisdictions because incident findings, test results and remediation patterns are not shared appropriately.
- **Public information is unclear.** People do not know what to do if a network outage affects emergency access or what alternative methods may be available.

What policymakers and operators should require

- Near real-time monitoring of end-to-end emergency calls, emergency call outcomes, including successful connection, set-up time, routing, voice continuity, location transfer and callback capability where applicable.
- Independent or regulator-observed synthetic testing of critical emergency call paths at a risk-based frequency.
- A common minimum test catalogue, with scope adjusted to national emergency calls, emergency call architecture and technology maturity.
- Prompt incident notification to emergency services and regulators based on defined thresholds and including affected areas, services, estimated impact of failed calls, recovery actions and available alternatives.
- Post-incident reporting that identifies root cause, contributing factors, service impact, corrective actions and evidence of closure, with appropriate public transparency.
- Periodic publication of aggregated resilience indicators or assurance outcomes that improve accountability without creating unnecessary security exposure.
- Public information protocols that are accessible, accurate and coordinated across operators and emergency service authorities.

11.7 A practical reform agenda

Reform need not begin with a comprehensive legislative overhaul. Many improvements can be made through coordinated industry, regulator and emergency service action, then be incorporated into formal obligations as standards, evidence and market capability mature.

Immediate actions

- Convene a standing national emergency calling resilience forum involving regulators, mobile operators, emergency service organisations, key infrastructure providers, device manufacturers and relevant consumer representatives.
- Develop a shared end-to-end emergency call service map and responsibility matrix for each jurisdiction.
- Agree to a minimum set of failure scenarios and begin joint testing of the highest-risk paths, including core or routing failure, loss of legacy fallback, device incompatibility, black hole cells, interconnect failure and loss of management access.
- Establish common incident notification thresholds, contacts, reporting templates and public communication protocols.
- Identify known device, roaming, location, callback and alternative network interoperability gaps, with owners and time-bound remediation plans.

Medium-term actions

- Publish an outcomes-based emergency calling resilience framework covering architecture, operational processes, testing, monitoring, incident response, recovery and continuous improvement.
- Introduce risk-based independent assurance or regulator-observed testing for critical emergency call functions.
- Create a device assurance and defect management programme, coordinated across operators and manufacturers.
- Update regulatory requirements before major 2G/3G retirements, cloud migrations, network-sharing programmes or new Wi-Fi and satellite emergency access launches.
- Develop proportionate resilience indicators that report both preparedness and demonstrated performance under test conditions.



Longer-term actions

- Align international standards and implementation guidance for PS emergency calling, device behaviour, fallback, roaming, location, callback and emerging access technologies.
- Develop technology-neutral emergency access policy that can accommodate voice, text, real-time text, data, video, Wi-Fi and satellite capability while preserving the reliability and accessibility of core emergency calling.
- Strengthen cross-border interoperability and information sharing, recognising that devices, visitors and supply chains operate globally.
- Embed emergency calling resilience within broader critical infrastructure, disaster resilience and public safety communications strategies.

The purpose of reform is not to eliminate every possible outage, as no complex technical system can offer that guarantee. Rather, it is to reduce the likelihood that a fault prevents a person from reaching help, to limit the scale and duration of any failure, to ensure that the failure is detected quickly and to make responsibilities clear when rapid action is required.

12. Conclusions and recommendations

For billions of people, their mobile phone is the first – and often only – practical way of contacting police, fire, ambulance and other emergency services. It is also becoming an essential tool for the responders who must coordinate and act on those calls.

That dependence changes the nature of the industry's responsibility. Telecommunications have evolved from a service valued mainly for convenience, reach and economic productivity into critical infrastructure on which people depend when they are frightened, injured, isolated or otherwise at their most vulnerable. In those moments, the public does not distinguish between a handset, radio site, fibre route, core platform, cloud service, firewall, emergency call gateway or call centre. They expect one outcome: that help can be reached.

This paper has shown why that outcome cannot be taken for granted. Modern emergency calling depends on an end-to-end chain of devices, access networks, transport, packet core and voice platforms, location and routing functions, security controls, interconnects, emergency call centres, power systems, suppliers and operational processes. A weakness in any part of that chain can prevent a call from connecting, delay it, disrupt voice, remove location information or make a callback impossible.

The recent incidents examined in this paper demonstrate that the greatest risks are not confined to natural disasters, coverage gaps or physical damage to mobile sites. They include software and configuration changes, security policy errors, timing failures, inadequate disaster recovery capacity, device incompatibility, weak fallback behaviour, hidden common dependencies and insufficiently tested incident processes. These are failures of systems, not simply failures of equipment.

The survey of mobile network technology leaders reinforces this conclusion. While many respondents reported strong architectures, regular end-to-end testing and effective monitoring, the results also revealed known single points of failure, inconsistent testing scope, gaps in end-to-end visibility and limited whole-of-organisation exercises. A more rigorous and substantive survey would help to refine the areas requiring attention and should be carried out by an independent industry body such as the GSMA.

The shift required

The main shift required is from network availability to emergency service assurance. While traditional measures of uptime, coverage and component redundancy remain necessary, they are not sufficient. A network can appear healthy while emergency calls fail. A device can display a signal while attached to a site that cannot carry a call onwards. A backup platform can exist but fail because it shares a database, firewall policy, transport route, certificate, management system or change process with the primary platform.

Emergency calling must therefore be designed, monitored, tested and governed as an end-to-end life-safety service. The relevant test is not whether individual elements are operational, but whether a person can establish contact, be routed to the right emergency service, communicate with an operator, provide or transmit location information where available and receive a callback if the call is interrupted.

This requires a corresponding shift in organisational practice. Reliability cannot sit solely with the radio, core, IT, security or operations team. It is a shared responsibility across executives, network engineers, device and platform suppliers, emergency service organisations, regulators and standards bodies. Commercial efficiency, technology modernisation and competition remain important, but none should weaken the public's ability to obtain help in an emergency.

A resilience programme

No complex technology system can guarantee that failures will never occur. The objective is to make failures less likely, smaller in scope, easier to detect and faster to recover from. It is also to ensure that a single technical, operational or organisational problem cannot remove every viable path to emergency assistance.

The recommendations in this paper, outlined in Table 3, are intended as a practical reference for MNOs, emergency service organisations, regulators, standards bodies, device manufacturers, technology suppliers and public safety policymakers.

Major area	Recommendations	Reference
Business continuity and crisis management	— Maintain clear crisis authority, current contact/escalation paths and integrated technical, executive and external communications. — Run realistic fire drills for both major and seemingly minor warning events, including third-party dependencies and cross-department recovery assumptions.	Ch. 9, BCCP
Testing	— Conduct regular end-to-end testing. — Set measurable targets for emergency call set-up and completion under normal and degraded conditions. These tests should include both live networks and lab testing and be run a minimum of every 6 to 12 months company- and industry-wide. — Testing should include both non-roaming and roaming scenarios, including limited-service state (unauthenticated SIM and absent SIM). — Failover testing should include intra/inter network. — Provision of a dummy emergency number to terminate on dummy PSAP for customer self-testing.	Ch. 6, §6.5
Devices	— All devices should be compliant with a common global standard (i.e. no carrier-specific behaviour). — Creation of country-specific device allow/block lists for all MNOs. — OEMs should work with industry bodies and declare any non-compliance on their devices. — Ensure consistent minimum emergency call behaviour and coordinated device allow/lock treatment.	§7.1
Alarms	— Monitor emergency calls and completed call outcomes – set-up time, routing, voice continuity, location and callback – rather than component status alone. — Standardise incident definitions, thresholds, notification times and data exchange.	Ch. 9, §11.6
Processes	— Review and continuously improve the four processes: Change management, Incident management, ARB and BCCP. — Require post-incident root cause/corrective action reporting, appropriate public transparency, aggregated resilience indicators and coordinated public information protocols. — Provide board/executive oversight of material resilience risks, test outcomes and unresolved findings. — Create a jurisdiction-wide responsibility matrix, including named senior accountability for operators and emergency service organisations.	Ch. 9, 10, §10.5, §11.2, §11.6
Core, IMS network	— Ensure the network implementation is fully standards-compliant. This includes, for example, timers, retry and fallback behaviour after and during failure conditions. — Review again after material device, RAN, core, security or IP-addressing changes. — Review of IPv4 and IPv6 pools.	§7.4

Table 3: Recommendations

Major area	Recommendations	Reference
Equipment/OEM enhancements	— Provide feedback to user during emergency call set-up. — Base station log files of SOS APN for rapid analysis/diagnostics. — Session based alarming, not ping. — Review standard configurations via eSIM. — Base station to contain emergency call test software for loopback testing (device image to PSAP). — Ensure that "wilting" of RAN considers all failure modes, including MOCN and MORAN. — Create shared operator/manufacturer/regulator defect processes and timely manufacturer support.	§7.2, §11.4
Standardisation	— Review current standards across multiple technologies (CS, 4G, 5G, WiFi, satellite). — Review of domain selection rules in the CS sunset era. — Improve and validate failover durations within and between technologies.	§11.3
Alternative emergency calling	— Investigate alternative technologies to voice (messaging, OTT, satellite).	§8.2, §8.3
PSMB	— Validate PSMB as an independent service via the same underlying broadband infrastructure.	§8.1
Culture and ownership	— Open sharing of problems and solutions for the common good between stakeholders. — Define a single point of ownership for end-to-end emergency services. — Run joint cross-sector exercises covering technical recovery, regulatory notification, public advice, welfare and emergency service coordination. — Conduct public education on emergency call behaviour. — Maintain a complete dependency map and contractual obligations covering emergency call duties, incident information, recovery priorities, testing and audit rights. — Prove recovery arrangements are independent of hidden shared suppliers/platforms/teams; retain in-house competence and "break-glass" access. — Exercise critical suppliers and maintain supplier obligations for supply-chain resilience, including specialist staff, emergency logistics and site access. — Embed emergency call resilience criteria in business cases, procurement, architecture standards, modernisation and technology retirement programmes.	§9.4, Ch. 10, §10.2, §10.4, §11.2
Register of critical assets (managed by ARB)	— End-to-end emergency calling is dependent on critical assets that are not necessarily obvious (e.g. timers, blast zones). — Map physical and logical dependencies for power, transport, timing, management and third-party services. — Reduce hidden common mode dependencies. — Separate management, user and control planes. — Any changes to critical assets require pre- and post-emergency call validation. Critical assets require additional review. — Track temporary exceptions and historic changes to remediation/closure so undocumented "quick fixes" do not become permanent hidden risk.	§7.3, §7.6, §7.7, Ch. 9, §9.1
Physical site access	— Regulators to recognise critical infrastructure and allow site maintenance access during emergencies, such as natural catastrophes. — This would also allow for deployables such as "cell sites on wheels".	§10.2

Table 3: Recommendations

Other areas in which additional standards efforts may be required have been identified, along with a checklist of items identified in this paper. These are listed in Appendix 3 and 4, respectively.

The path forward

The telecoms industry should not wait for a perfect global regulatory framework or a single technical solution. Operators, regulators, emergency service organisations and suppliers can begin now by mapping the end-to-end service, identifying shared dependencies, agreeing on the highest-risk failure scenarios, testing them jointly and addressing the gaps those tests reveal.

At the same time, industry bodies and standards organisations should accelerate work in areas where interoperability is most consequential: device behaviour, emergency fallback, roaming, location, callback, security controls and the transition from legacy CS networks to PS voice. Regulatory frameworks should reinforce this work through outcomes-based requirements, transparent reporting and proportionate independent assurance.

Measuring progress should be simple. When an individual reaches for a phone in an emergency, the complexity of the network behind that call should not become their problem. They should be able to trust that the communications system will connect them to help and that, if one part fails, the wider system has been designed, tested and governed to protect them.

This is the standard expected of critical infrastructure and that emergency calling must now meet. In support of this goal, there needs to be a change of culture in terms of openness and information sharing between industry players for the common good. Instead of issues remaining hidden to avoid embarrassment, the industry would benefit from an open, anonymised, no-blame mechanism for raising awareness and sharing knowledge, problems and solutions. The GSMA would be ideally placed to receive such information and pass it on, suitably anonymised.



Appendix 1: Network timers

Examples of the network timers used in mobile networks are shown in Table 4.

Domain	Examples	Typical purpose	Illustrative value/behaviour	Engineering caution
RRC	T300, T301, T311	Connection establishment and re-establishment	Values are broadcast/configured by the RAN and are commonly in the subsecond to multisecond range.	Repeated radio attempts can materially delay emergency fallback.
EPS NAS	T3410, T3411, T3417/T3417ext	Attach, retry and emergency bearer/ service handling	Specified timer sets vary by procedure and release. Network or UE may start/ restart them based on NAS responses.	Do not assume one fixed "emergency set-up timer".
Legacy mobility	T3245 and forbidden-PLMN handling	Controls abnormal/ forbidden network retry behaviour	Can inhibit or delay normal service attempts. Emergency service exceptions must be validated.	Check interaction with SIM status and limited service.
P-CSCF discovery	DNS, DHCP, PCO and TCP/ TLS connect timeouts	Obtain and reach primary/secondary P-CSCF	Typically provided at 4G/5G attach.	Test black hole, reject and partial-connect failure modes. Negative errors are faster than silent packet loss/no response due to retransmission strategy.
SIP over UDP	Timer A/E	Retransmission timer for INVITE/ non-INVITE messages	Starts at T1 (2 seconds) and grows according to SIP transaction rules (doubling with maximum of 16 seconds for non-INVITE)	Retransmissions can accumulate before fallback.
SIP over TCP	TCP SYN	SYN retransmission timer	OS dependent. Android default based on Linux core with retransmissions at 1 second and then doubling up to a maximum of 6 attempts, giving 127 seconds.	For UDP, retransmissions can accumulate before fallback.
SIP transaction	Timer B/F	Overall INVITE/ non-INVITE transaction timeout	Common default is 64xT1; at T1=2s this is about 128 seconds.	Transport, provisional responses and implementation can change the observed delay.
Registration	Expires/refresh timers	Maintain normal or emergency registration	Network-supplied and operator-specific	Emergency session initiation may be permitted without prior normal registration.
PLMN search	Cell selection/ reselection and scan intervals	Find home or alternative PLMN	Dependent on device and modem implementation	Full-band scans can dominate time-to-retry.
Application retry	Vendor/operator retry policy	Retry after recoverable set-up failure	No single universal value. Back off may be immediate, staged or coupled to a mobility state.	Avoid retry storms while minimising life safety delay.

Table 4: Network timers used in mobile networks

Appendix 2: Control/user and management separation

A lack of independent paths has contributed to several high-profile outages taking considerably longer to restore. This is also a consideration in part of the blast zone design.

Plane	Failure consequence	Resilience requirement
Data/forwarding	Customer and signalling traffic loss	Redundant paths, fast reroute (FRR), adequate buffers and capacity
Control	Loss of routing or label distribution; stale forwarding	Redundant routing processes/controllers, graceful restart used cautiously, CPU protection
Management	Loss of visibility or ability to recover	Independent OOB path, console access, redundant AAA/DNS/NTP and local break-glass
Telemetry/logging	Silent or poorly diagnosed failure	Buffered local logs, multiple collectors, time synchronisation, path-independent export
Automation/orchestration	Large-scale configuration error	Staged roll-out, validation, canaries, rate limits, rollback and approval controls

Transport/IP protocols

Packet transport should provide deterministic traffic engineering, service isolation and rapid local repair while avoiding unnecessary protocol complexity. MPLS, SR-MPLS and SRv6 can all support resilient designs when the failure domains and operational model are clear.

Capability	Traditional MPLS	Segment routing	Reliability consideration
Path computation	LDP/RSVP-TE or controller	IGP segments and SR policies	Controller dependence and fallback behaviour must be defined.
Fast repair	LFA, remote LFA, RSVP FRR	TI-LFA or protected SR policy	Coverage must be calculated for link, node and SRLG failures.
State	Per-hop label/signalling state varies by design	Reduced core signalling state	Edge and controller scale still require validation.
Traffic engineering	Explicit tunnels and constraints	Candidate paths, affinities and policies	Policy colour/intent errors can create broad blast zones.
Operations	Mature but potentially complex	Simpler core, newer tooling	Telemetry and staff competence are decisive.

Network timers

Mobile networks depend on frequency and phase/time synchronisation. A transport path may pass packets while failing the radio service because

Risk	Impact	Controls
GNSS loss or interference	Loss of primary phase/time at grandmaster or site	Holdover, multisource timing, interference detection, alternative grandmaster
PTP path asymmetry	Phase error and radio degradation	Boundary clocks, calibrated paths, asymmetry monitoring and route constraints
Packet delay variation	Timing noise during congestion or reroute	Priority queue, capacity headroom, PTP-aware equipment
Timing loop or wrong source	Unstable frequency/time domain	SSM/QL policy, source priority, topology validation
Failover to unqualified path	Network is connected but timing SLA fails	Include timing in path policy and restoration testing



Appendix 3: Areas for additional standards work

There are several issues identified in this paper that could be addressed by additional standards work. These are collated here for convenience.

Emergency callback

This is possible if the asserted identity of the caller is available in the SIP P-Asserted-Identity header. The caller number is asserted by the P-CSCF and the related callback from the PSAP is not an emergency call (e.g. for roaming, call would be routed over the NNI to HPMN). In the roaming scenario, the emergency call is initiated via so-called anonymous call, which may or may not have an asserted identity. In some cases, the caller's number can be from the underlying packet core by the P-CSCF to obtain an asserted identity, but in other cases this is not possible. Therefore, callback is not always possible in the roaming scenario.

To address this issue, both the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) are working on a proposed solution that involves the P-CSCF creating a time-limited temporary identity to be used for callback. The related ETSI specification is TS 103 873[4] and the ITU-T specification is ITU-T Q.3647[5]. This work is ongoing, and liaison statements have been exchanged between the two groups as well as to 3GPP.

Location information

This is mandated by GSMA PRD IR.92[1] to be included in the emergency call SIP INVITE via the PIDF-LO message body. It is noted that issues have been encountered in terms of the network (incorrectly) discarding the INVITE due to its size, and the INVITE being delayed while the UE determined its location. In the latter case, the call attempt should not be delayed as the call itself is the primary concern (the location is of secondary importance). Standards bodies should therefore consider clarifying this point such that the INVITE is not delayed and the location information is conveyed subsequently during the active SIP session via a SIP UPDATE message with PIDF-LO message body. Due to the firewall issues encountered based on message size, consideration could also be given to whether this behaviour should be recommended in all cases to reduce the size of the INVITE message.

Emergency calling via VoWiFi

The 3GPP standards allow for emergency calling via VoWiFi. However, the standards (3GPP TS 23.167[2] annex J – "IMS Emergency Services using WLAN access to EPC") state that this is only permitted when 3GPP access for emergency call is not possible or available. This means it is possible for a UE to be connected in its HPMN via WiFi and to an ePDG that supports emergency calling, but the UE is obliged to switch over to a 3GPP access. This causes delay and consideration should be given to changing the network selection rules to enable the fastest response.

SIP retry timers

The SIP retry timers, whether via UDP or TCP, result in suboptimal behaviour in terms of failover and network selection in failure cases. This is true for both normal VoLTE and emergency

VoLTE, but is more of an issue in the latter case. Consideration should be given to significantly improving the failover behaviour for SIP emergency calls via use of reduced timers/retransmissions. It has also been observed that 3GPP standards have not always been implemented correctly for triggering retry/failover for emergency sessions. In particular, it appears that the emerg-request timer (introduced in 3GPP R19 to limit the duration until an emergency session is regarded to have failed) has not always been correctly implemented, resulting in extra delays before triggering retry/failover. It is also possible that further clarifications are needed in this area.

Liaison statements can be sent to 3GPP concerning these items.

Finally, it is noted that 3GPP SA1 has a study item, "Additional capabilities for emergency services", which is targeted at R21 and the output will be documented in 3GPP TR 22.846[6].

Appendix 4: Checklist

The following is a checklist of issues identified in this paper, grouped into the following categories:

- PLMN selection and emergency fallback
- Device SOS APN emergency call support
- PIDF-LO/location information
- SIP retry/retransmission and PLMN failover timing
- Network timing and synchronisation infrastructure
- Emergency callback and identity assertion
- Testing, interoperability and self-test access

PLMN selection and emergency fallback

Confirm the device/network does not remain camped on a Home PLMN (HPLMN) that cannot complete an emergency session. Verify that PLMN reselection is triggered on SIP-layer failure, not only NAS/RAN loss, when own network options have been exhausted.

Audit access-side firewall rules that could silently drop SIP signalling (not just SIP INVITE) without generating an explicit reject. Confirm silent-drop vs explicit-reject behaviour is distinguishable in monitoring.

Verify there is a welfare check/retrospective review process for failed emergency attempts, regardless of whether the failure was detected by conventional network alarms.

Device/SOS APN emergency call support

Establish whether any device population on the network blocks the SOS/emergency APN while supporting normal VoLTE, and whether CS fallback exists as a safety net in the affected market.

Confirm the device correctly reads and applies the local/extended emergency numbers list broadcast in NAS signalling, rather than treating a local emergency code as an ordinary dialled number.

Run a roaming partner statistics review comparable to the 100-day study. Compare the 4G/2G-3G split for ordinary calls against the split for emergency calls for the same roaming population.

Confirm there are OEM-MNO cooperation processes to identify, notify, modify by OTA-update or, where unavoidable, block affected device models, with defined interoperability testing before any unblocking.

PIDF-LO/location information

Confirm access-side SBC/firewall message-size thresholds for emergency SIP INVITE are set to at least 5,000–5,500 octets, not a default tuned only for ordinary VoLTE traffic. Monitor this threshold to align with any potential increases in the size of the SIP INVITE message (e.g. an increase in SDP message body due to the addition/support of immersive voice codecs).

Verify the firewall/SBC rejects on parsed message content where feasible, never purely on byte length, for any signalling path carrying emergency traffic.

Confirm devices are not configured to suppress PIDF-LO conditionally, based on serving network or own/home network heuristics, to compensate for known network non-support, as this masks the underlying network non-compliance.

Assess whether PIDF-LO acquisition is currently delaying sending of the SIP INVITE and confirm plans to move location to a subsequent SIP UPDATE within the active session, in line with any related standards clarification/change.

SIP retry, retransmission and PLMN failover timing

Confirm P-CSCF redundancy is actually being exercised by devices on failure and check for inefficient reselection causing prolonged retries before CSFB fallback.

Audit SIP-over-UDP retransmission timing (Timer A/E) against T1=2 seconds (s), doubling to a 16 second ceiling for non-INVITE, and confirm this is not compounding PLMN failover delay for emergency sessions specifically.

Audit SIP-over-TCP overall transaction timeout (Timer B/F, ≈64×T1 ≈128 s) and TCP SYN retransmission behaviour (OS-default: 1 second doubling, 6 attempts ≈127 seconds) for the device population in use.

Confirm device compliance regarding the emerg-request timer to promptly trigger retry/failover for emergency call sessions.

Confirm progress of the LS to 3GPP on reduced timers/retransmissions over both UDP/TCP for emergency SIP specifically, and track any resulting CR against your own deployed baseline.

The following is a checklist of issues identified in this paper, grouped into the following categories:

— PLMN selection and emergency fallback
— Device SOS APN emergency call support
— PIDF-LO/location information
— SIP retry/retransmission and PLMN failover timing
— Network timing and synchronisation infrastructure
— Emergency callback and identity assertion
— Testing, interoperability and self-test access

PLMN selection and emergency fallback

Confirm the device/network does not remain camped on a Home PLMN (HPLMN) that cannot complete an emergency session. Verify that PLMN reselection is triggered on SIP-layer failure, not only NAS/RAN loss, when own network options have been exhausted.

Audit access-side firewall rules that could silently drop SIP signalling (not just SIP INVITE) without generating an explicit reject. Confirm silent-drop vs explicit-reject behaviour is distinguishable in monitoring.

Verify there is a welfare check/retrospective review process for failed emergency attempts, regardless of whether the failure was detected by conventional network alarms.

Device/SOS APN emergency call support

Establish whether any device population on the network blocks the SOS/emergency APN while supporting normal VoLTE, and whether CS fallback exists as a safety net in the affected market.

Confirm the device correctly reads and applies the local/extended emergency numbers list broadcast in NAS signalling, rather than treating a local emergency code as an ordinary dialled number.

Run a roaming partner statistics review comparable to the 100-day study. Compare the 4G/2G-3G split for ordinary calls against the split for emergency calls for the same roaming population.

Confirm there are OEM-MNO cooperation processes to identify, notify, modify by OTA-update or, where unavoidable, block affected device models, with defined interoperability testing before any unblocking.

PIDF-LO/location information

Confirm access-side SBC/firewall message-size thresholds for emergency SIP INVITE are set to at least 5,000–5,500 octets, not a default tuned only for ordinary VoLTE traffic. Monitor this threshold to align with any potential increases in the size of the SIP INVITE message (e.g. an increase in SDP message body due to the addition/support of immersive voice codecs).

Verify the firewall/SBC rejects on parsed message content where feasible, never purely on byte length, for any signalling path carrying emergency traffic.

Confirm devices are not configured to suppress PIDF-LO conditionally, based on serving network or own/home network heuristics, to compensate for known network non-support, as this masks the underlying network non-compliance.

Assess whether PIDF-LO acquisition is currently delaying sending of the SIP INVITE and confirm plans to move location to a subsequent SIP UPDATE within the active session, in line with any related standards clarification/change.

SIP retry, retransmission and PLMN failover timing

Confirm P-CSCF redundancy is actually being exercised by devices on failure and check for inefficient reselection causing prolonged retries before CSFB fallback.

Audit SIP-over-UDP retransmission timing (Timer A/E) against T1=2 seconds (s), doubling to a 16 second ceiling for non-INVITE, and confirm this is not compounding PLMN failover delay for emergency sessions specifically.

Audit SIP-over-TCP overall transaction timeout (Timer B/F, ≈64×T1 ≈128 s) and TCP SYN retransmission behaviour (OS-default: 1 second doubling, 6 attempts ≈127 seconds) for the device population in use.

Confirm device compliance regarding the emerg-request timer to promptly trigger retry/failover for emergency call sessions.

Confirm progress of the LS to 3GPP on reduced timers/retransmissions over both UDP/TCP for emergency SIP specifically, and track any resulting CR against your own deployed baseline.

Network timing and synchronisation infrastructure

Identify any legacy NTP servers using a 10-bit (or otherwise short) week-counter field and confirm rollover behaviour has been tested, not assumed. The 1,024 week (19.7 year) overflow resets to a stale epoch (e.g. 2006).

Confirm no legacy or low-stratum NTP source can be inadvertently promoted to a master timer role via undocumented design/classification changes, and that such a change would trigger an ARB/change management review.

Confirm holdover capability and multisource timing (e.g. GNSS + PTP/1588) exist so loss of a single timing reference degrades gracefully rather than propagating incorrect time.

Confirm there are end-to-end session alarms for emergency call paths, distinct from ICMP/ping reachability alarms, as a timing fault can leave every component "up" while calls fail.

Emergency callback and identity assertion

Monitor standards progress in ETSI/ITU-T/3GPP regarding the P-CSCF, creating a temporary, globally routable SIP URI as an asserted caller identity for callback of anonymous roaming emergency calls, and track any resulting CRs against your own deployed baseline.

Verify the network's ability to retrieve an MSISDN from the packet core when SIP P-Asserted-ID is unavailable for roaming/anonymous emergency sessions.

Confirm that the network returns the 3GPP-IMS+XML body (introduced R14, 2017) to explicitly tell an inbound roamer to attempt anonymous call.

Confirm anonymous IMS emergency calls for inbound roamers are supported even where the network does not send the 3GPP-IMS+XML body (introduced R14, 2017) and check devices are not silently relying on undocumented fallback behaviour to mask this network gap.

Where VoWiFi is offered, confirm network selection does not delay call set-up by forcing a switch from an already connected ePDG/WLAN path back to 3GPP access before the call proceeds.

Monitor the progress of standards related to a device staying on WLAN to complete an emergency call if the ePDG has indicated support of emergency calling, and track any resulting CR against your own deployed baseline.

Testing, interoperability and self-test access

Confirm a representative set of foreign SIM/device combinations has been tested against the network's emergency call path, including location information delivery and callback number availability/length.

Confirm whether a spare emergency category or dedicated test number (e.g. 1280-style) exists to let engineers/test houses reach a test PSAP without disrupting live emergency services, and clarify authorisation/funding basis.

Confirm network and device interoperability is proven for all emergency use cases – domestic, roaming and limited service – ahead of any material deployment change.

Review existing test plans (e.g. GSMA PRD TS.11), particularly for failure/failover scenarios and address any functional gaps in test plans.

Confirm regular (6 or 12 monthly) testing of real devices and networks to confirm ongoing compliance to standards and/or identify issues to be rectified. Separately, test failure cases in a lab environment to test failover/retry resilience.



References

[1] 3GPP. TR 22.846: Study on additional capabilities for emergency services.

[2] 3GPP. TS 23.167: IP Multimedia Subsystem (IMS) emergency sessions.

[3] 3GPP. TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3.

[4] ETSI. TS 103 873: Emergency Communications Interconnect Requirements for Packet-Switched Originating Networks.

[5] GSMA. PRD IR.92 (VoLTE) – IMS Profile for Voice and SMS.

[6] ITU-T. Recommendation ITU-T Q.3647 – Signalling requirements for emergency services in an Internet protocol multimedia subsystem roaming environment.

Glossary

Term	Definition
2G	Second-generation mobile technology, commonly known as GSM. It mainly provides traditional voice calls and text messaging. Many operators are retiring 2G networks, although they can still provide an emergency call fallback in some markets.
3G	Third-generation mobile technology, commonly known as UMTS. It supports voice and mobile data and has often been used as a fallback for emergency calls from newer devices. Many operators are retiring 3G networks.
3GPP	3rd Generation Partnership Project. An international partnership that develops technical specifications for mobile networks, including 4G, 5G, voice services and emergency calling.
4G/LTE	Fourth-generation mobile technology. LTE stands for Long Term Evolution. It uses packet-based communications and commonly delivers voice through VoLTE.
5G	Fifth-generation mobile technology. It offers greater capacity, less delay and support for new services. Voice can be delivered using VoNR, although some 5G services still rely on 4G components.
5GC	5G Core Network. The 5G Packet Core Network.
5G NSA	5G Non-Standalone. A 5G deployment that continues to rely on a 4G core or 4G radio anchor for some functions, including voice in many networks.
5G SA	Authentication, Authorisation and Accounting. Systems that confirm a user or device is permitted to access a network and record relevant service activity.
AAA	Data Channel
Access network	The part of a communications network that connects a user's device to the wider network. In mobile networks, this generally means the radio network and cell sites.
Access point name (APN)	Network settings used by a device to establish a packet data connection. An emergency APN may be used to set up an emergency data session.
Aggregation site	A network location at which traffic from several cell sites or access networks is collected before being carried into the wider transport or core network.
AI	Artificial intelligence. A branch of computer science that allows machines and computers to copy human thinking, learning and problem solving.
All-IP	A network in which services, including voice, are delivered using Internet Protocol (IP) rather than traditional circuit-switched (CS) technology.

Term	Definition
Anonymous emergency call	An emergency call made without the normal subscriber authentication or registration process, typically to enable an unauthenticated or roaming device to contact emergency services. Caller identity or callback information may be limited.
APN/SOS APN	An APN used for emergency packet data access. SOS APN is an informal term sometimes used for the emergency data connection a device uses to set up a packet-switched emergency call.
ARB	Architecture Review Board. A governance group that evaluates and approves technical designs to ensure they align with organisational standards and strategic goals.
ARP	Allocation and Retention Priority. A mobile network priority setting used to determine how a service is admitted, retained or pre-empted during congestion.
ARPU	Average Revenue Per User. A common telecommunications measure of average revenue generated per customer or service connection.
Backhaul	The connection that carries traffic from a cell site or local network to the operator's core network. It may use fibre, microwave links or other transmission technologies.
Backup platform	A secondary system intended to take over if the primary system fails. It only provides resilience if it has sufficient capacity and does not share critical dependencies with the primary system.
BCCP	Business Continuity and Crisis Planning. A process that protects an organisation from sudden disruptions and allows it to keep running.
Black hole cell/black hole condition	A situation in which a cell site continues to advertise mobile service even though an upstream fault means it cannot complete calls or data sessions. A user may see signal bars but be unable to reach emergency services.
Blast zone	The maximum area, number of customers or range of services that can be affected by a single fault, change or shared dependency failure.
Bring-your-own device (BYOD)	A device owned or chosen by the user rather than supplied by the operator. Such devices may not have been tested against every local emergency calling configuration.
Callback	The ability of an emergency call centre to call a person back if the original call is disconnected. This requires a usable number or temporary identity and a working return path.
Call flow	The sequence of signalling and service steps required to establish, route and complete a call.
Call set-up time	The time between initiating a call and establishing a usable connection to the receiving party or emergency call centre.
Camp-on/network camping	A device selecting and remaining registered on a particular mobile network. In an emergency, inappropriate camp-on behaviour can delay a device from seeking a working alternative network.
Capacity headroom	Network capacity is deliberately kept available so that services can continue when traffic is rerouted after a fault or demand rises sharply during an emergency.

Term	Definition
Carrier profile/carrier bundle	Settings supplied by a mobile operator or device manufacturer that control how a device behaves on a particular network, including voice and emergency calling features.
Cell site/base station	The physical mobile network location containing antennas, radio equipment, power and transmission connections that provide local mobile coverage.
Certificate	A digital credential used to prove the identity of a system or service and establish trusted encrypted communications. An expired or incorrectly deployed certificate can disrupt network functions.
Circuit-switched (CS)	Traditional telephone technology in which a dedicated voice path is established for the duration of a call. 2G and 3G voice services commonly use circuit switching.
Circuit-switched fallback (CSFB)	A process in which a 4G device moves to a 2G or 3G network to make a traditional voice call. Its availability falls as legacy networks are retired.
Cloud platform/cloud region	Computing infrastructure delivered as a shared service from data centres. A cloud region is a geographic grouping of such infrastructure. Shared cloud dependencies can create common points of failure.
Common mode failure	A single fault that disables more than one supposedly independent system because those systems share a dependency, such as power, software, a database, a firewall policy, a cloud service or a management path.
Conformance testing	Testing designed to check whether a device, network or service follows a specified technical standard. It may not by itself prove end-to-end emergency call performance under failure conditions.
Control plane	The network functions that make decisions about how traffic is connected, authorised and routed. A control plane fault can affect many services even if some data paths remain available.
Core network/mobile core	The central part of a mobile network that manages a device's connections, subscriber information, routing, policy and data sessions.
Customer premises equipment (CPE)	Equipment located at a customer's home or business, such as a router, modem or fixed wireless gateway.
Data centre	A facility that houses computing, storage and network systems. Mobile core, voice, location and emergency routing functions may operate in data centres or cloud environments.
Device fragmentation	The large variation in handset models, operating systems, chipsets, software versions and carrier settings that can cause devices to behave differently on the same network.
Device/handset/user equipment (UE)	The phone, smartwatch, modem or other device used to access a mobile network. UE is the technical term commonly used in mobile standards.
Disaster recovery (DR)	Plans, facilities and systems used to restore critical services after a major outage or loss of a primary site or platform.
DNS	Domain Name System. A system that translates service names into network addresses. If DNS fails, a device or network function may be unable to find the platform needed to complete an emergency call.

Term	Definition
DNN	Data Network Name. The 5G equivalent of an APN: a label that identifies the data network or service a device is connecting to.
DTH	Direct-to-handset or direct-to-device. A service, often satellite-enabled, that connects directly with ordinary mobile devices rather than requiring a separate satellite terminal.
E-CSCF	Emergency Call Session Control Function. An IMS function that recognises and routes packet-switched emergency calls and may obtain relevant location and routing information.
ePDG	Evolved Packet Data Gateway. A network function that allows a mobile device to connect securely to a mobile operator's core network over Wi-Fi. It is important for Wi-Fi calling.
Emergency call centre	The organisation or facility that receives emergency calls and arranges a response. In many countries, this function is performed by a PSAP.
Emergency calling	The ability to contact police, fire, ambulance or another designated emergency service through an emergency number, text, app or other approved channel.
Emergency-service hand-off	The transfer of an emergency call and relevant information from a telecommunications operator to the emergency call centre or PSAP.
End-to-end	Across the complete service path, from a person's device through the network and interconnect to the emergency call centre, including location and callback functions where relevant.
EPC	Evolved Packet Core. The 4G Packet Core Network.
ETSI	European Telecommunications Standards Institute. A standards organisation that develops telecommunications standards, including emergency communications work.
Failover	The process of moving a service from a failed or degraded system, route or network to an alternative.
Fail-safe/fail safely	Designing a service so that, when one path fails, it moves predictably to a safe alternative rather than leaving the user connected to a non-functioning service.
Fallback	An alternative method or network path used when the preferred service path is unavailable or unable to complete a call.
Firewall	A security system that controls network traffic according to defined rules. An overly restrictive or incorrect firewall rule can unintentionally block emergency signalling or voice traffic.
First responders	Police, fire, ambulance, emergency medical and other personnel who respond directly to an emergency.
Fixed line/fixed network	A communications service delivered to a fixed location, historically over copper telephone cables and now commonly over fibre or other fixed access networks.
FRR	Fast Reroute. A network technique that rapidly redirects traffic around a failed link or device.
GNSS	Global Navigation Satellite System. Satellite systems, including GPS, used for positioning and for accurate time and frequency synchronisation in networks.

Term	Definition
GSM	Global System for Mobile Communications. The technical family commonly associated with 2G mobile services.
GSM-R	Global System for Mobile Communications-Railway. A railway communications system based on GSM technology.
Handover	The transfer of a device connection or call from one cell, network technology, network path or operator system to another.
Holdover	The ability of a timing system to maintain accurate time for a period after it loses its primary timing reference.
Home network/home operator	The mobile operator with which a customer has their normal subscription.
IMS	IP Multimedia Subsystem. A standards-based platform used to control voice and multimedia sessions over 4G and 5G networks, including VoLTE, VoNR and packet-switched (PS) emergency calls.
Incident command	The defined leadership structure and decision-making process used to manage a significant service disruption.
Interconnect/ interconnection	The technical and commercial connection between separate networks or service providers, such as between a mobile operator and an emergency call centre.
Interoperability	The ability of devices, networks, platforms and organisations from different suppliers or operators to work together reliably.
IP	Internet Protocol. The rules used to route digital data across modern communications networks. Voice over 4G and 5G is generally carried as IP data.
IP address	A numerical identifier used to locate a device or service on an IP network.
IPsec	Internet Protocol Security. A set of security protocols used to encrypt and authenticate IP communications, commonly used for Wi-Fi calling connections.
IPv4 / IPv6	Versions 4 and 6 of Internet Protocol. IPv6 provides a much larger address space than IPv4. Both may be relevant to emergency call set-up and network interoperability.
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector. The United Nations body that develops international telecommunications standards.
LEO	Low-Earth Orbit. A relatively low satellite orbit used by many modern satellite communications systems.
Limited service	A device state in which normal subscription services may not be available, but emergency calling may still be permitted.
LMR	Land Mobile Radio. A category of professional two-way radio communications systems used by industrial, commercial and public safety organisations.
Location information	Data used to identify or estimate the caller's location so emergency services can send help. It may be derived from the mobile network, device, Wi-Fi, satellite or other sources.

Term	Definition
LTE	Long Term Evolution. The technical name for 4G mobile radio technology.
MCX	Mission Critical Services. A family of 3GPP standards for priority communications used by public safety and other critical users, including mission-critical push-to-talk.
MNO	Mobile Network Operator. A company that owns or operates a public mobile network and provides mobile services.
MOCN	Multi-Operator Core Network. A radio-sharing arrangement in which operators share radio access infrastructure while maintaining separate core networks.
MORAN	Multi-Operator Radio Access Network. A radio-sharing arrangement in which operators share certain radio access infrastructure while retaining separate spectrum and core network elements.
MPLS	Multiprotocol Label Switching. A method used in transport networks to direct traffic efficiently and reliably along predetermined paths.
NAS	Non-Access Stratum. Control plane signalling layer running directly between the UE and core network (EPC/5GC).
NAT	Network Address Translation. A process that maps one network address to another. Incorrect NAT behaviour can cause voice or media to fail even if call set-up succeeds.
N+1/N+2/N+3 resilience	A way of describing spare capacity or redundancy. N is the capacity or number of components needed for normal operation; +1, +2 or +3 indicates one, two or three additional units or paths available if failures occur.
Network slicing	A 5G capability that creates logically separate network services for different uses. It can support priority and separation but does not necessarily protect against shared physical or management failures.
Network time protocol (NTP)	A protocol used to synchronise the clocks of computers and network equipment. Incorrect time can affect network operation, logging, security and service coordination.
NG911/next-generation emergency calling	Modern emergency service systems that use IP networks and can support richer information than traditional voice calling, such as text, images, video and improved location data. Names and implementation differ by country.
Non-terrestrial network (NTN)	A communications network that uses satellites or other non-ground-based infrastructure. It can supplement terrestrial mobile coverage, especially in remote or disaster-affected areas.
OAM/OA&M	Operations, Administration and Maintenance. The people, processes and systems used to operate, monitor, configure and repair telecommunications networks.
OEM	Original Equipment Manufacturer. A company that designs or produces equipment or devices, such as a handset manufacturer.
Open-market device (OMD)	A handset sold without a specific mobile operator's configuration or certification. It may have different network and emergency calling behaviour from operator-supplied devices.

Term	Definition
Operational support system (OSS)	Software and tools used by an operator to manage, monitor, provision and maintain its network and services.
Orchestration	Software-driven coordination of network, cloud and service functions. It can improve speed and consistency, but an incorrect automated change can affect many systems quickly.
Out-of-band (OOB) management	A separate management path used to access and recover network equipment when the main production network is unavailable.
Over-the-air (OTA) update	A software, firmware or settings update delivered remotely to a device over a mobile or Wi-Fi connection.
Over-the-top (OTT)	A means of delivering audio, video, media and communication services over the internet via a third-party app instead of an MNO.
P25	Project 25. A digital two-way communication device built for public safety and critical infrastructure agencies.
Packet core	The central network platform that establishes and manages packet data connections for mobile devices.
Packet-switched (PS)	A communications method in which voice and data are divided into digital packets and carried over an IP network. It is the foundation of 4G and 5G services.
P-CSCF	Proxy Call Session Control Function. An IMS function that acts as a device-facing entry point for voice session signalling.
PIDF-LO	Presence Information Data Format Location Object. A standard format for carrying location information in IP-based communications, including some emergency call scenarios.
PLMN	Public Land Mobile Network. A mobile operator's public cellular network, identified by a mobile network code and country code.
Power resilience	The ability of a site or platform to continue operating through the loss of normal electricity supply, using batteries, generators, fuel and other backup arrangements.
P/PE	Provider/Provider Edge. Two distinct router roles in an MPLS network.
Priority and pre-emption	Controls that give some users or services preferential access to network capacity during congestion and may remove lower-priority traffic where permitted. They do not restore a network that has failed completely.
PSAP	Public Safety Answering Point. The emergency call centre that receives emergency calls and dispatches or coordinates police, fire, ambulance or other public safety responses.
Public safety mobile broadband (PSMB)	Mobile broadband communications used by emergency responders and public safety agencies, often using dedicated, shared or commercial LTE/5G networks.
QoS	Quality of Service. Network mechanisms that manage the performance and priority of different traffic types, such as voice, data or public safety communications.

Term	Definition
Radio access network (RAN)	The mobile network equipment that connects devices over radio signals to the wider network, including cell sites, antennas and radio baseband equipment.
Radio network/radio site	See Radio access network and Cell site. These terms describe the part of the network that provides a wireless connection to a handset.
Rate limiting	A control that restricts the volume of requests or traffic accepted by a system. It can protect a service from overload or attack but must not mistakenly block legitimate emergency traffic.
Real-time text (RTT)	Text transmitted during a communications session as it is typed, rather than after a complete message has been sent. It can support accessible emergency communications.
Recovery point objective (RPO)	The maximum acceptable amount of data loss after a disruption, measured in time.
Recovery time objective (RTO)	The target maximum time allowed to restore a service after disruption.
Redundancy	Duplication of equipment, routes, power supplies or systems so that a service can continue if one element fails. Redundancy is not sufficient where backup paths share the same critical dependencies.
Registration	The process by which a device establishes its presence and permissions with a mobile network or voice platform. Emergency registration may follow different rules from ordinary service registration.
Resilience	The ability of a service to prevent failures where possible, continue operating during disruption, limit the impact of faults and recover quickly when failure occurs.
Roaming	Use of a mobile service through a network other than the customer's home operator, usually while travelling. Emergency call arrangements for roaming can differ from normal voice and data roaming.
RRC	Radio Resource Control. The signalling used between a device and the radio network to establish, manage and release a radio connection.
RTP/RTCP	Real-time Transport Protocol and Real-time Transport Control Protocol. Protocols commonly used to carry and monitor voice or other real-time media over IP networks.
Routing	The process of selecting the network path and destination for a call or data session. In emergency calling, routing must deliver the call to the correct emergency service organisation.
SBC	Session Border Controller. A device or software function that secures and manages voice session connections between networks. Incorrect SBC configuration can block or disrupt emergency calls.
SDP	Session Description Protocol. Information exchanged during an IP voice call to describe how voice media should be sent and received.
Service assurance	Monitoring and testing that assesses whether a service is actually working for users, rather than only whether individual network components are reachable.

Term	Definition
Service-level monitoring	Monitoring of service outcomes for the end user, such as whether an emergency call connects, routes correctly, carries two-way voice and provides location or callback data.
Shared network/network sharing	An arrangement in which two or more operators share some network infrastructure, such as towers, radio equipment, spectrum, transport or core platforms.
Signalling	The control messages that establish, manage and end a call or data session. Signalling failure can stop a call even if a device has radio coverage.
SIM/eSIM	(electronic) Subscriber Identity Module. A secure chip or virtual equivalent that identifies and authenticates a user on a mobile network.
SIP	Session Initiation Protocol. A protocol used to establish, modify and end voice and multimedia sessions over IP networks, including many IMS calls.
SIP INVITE	The SIP message used to begin a voice or multimedia session. A firewall or policy error that rejects an emergency SIP INVITE can stop the call before it connects.
SLA	Service Level Agreement. A formal contract between a service provider and a customer that defines the expected level, quality and availability of a service.
Sleep cell/sleeping cell	A cell site that appears operational but is not providing the service expected, often because of a fault that is not detected by normal network monitoring.
SMS	Short Message Service. Standard mobile text messaging. In some markets, SMS can be used to contact emergency services, subject to national arrangements.
Software-defined network function	A network capability implemented largely in software rather than as a dedicated hardware appliance. This can improve flexibility but can also spread configuration errors more quickly.
SR	Segment Routing. A source-routing architecture to steer packets efficiently and programmatically across a network.
SR-MPLS/SRv6	Segment Routing over MPLS and Segment Routing over IPv6. Methods for steering traffic through a network. They can support resilient designs but require careful operational control.
SSM/QL	Synchronization Status Messaging with Quality Level. A signalling protocol used to communicate the precision and reliability of clock reference signals across a telecommunications network.
Standby system	A secondary system held ready to take over from the main system during a failure.
Synthetic testing/ synthetic transaction	An automated test that imitates a real user action, such as attempting an emergency call, to verify the complete service path before customers report a problem.
SyncE	Synchronous Ethernet. A method for distributing precise timing across ethernet networks.
Systemic failure	A failure caused by the interaction of multiple technologies, dependencies, processes or organisations, rather than by a single isolated component fault.

Term	Definition
TCP	Transmission Control Protocol. A connection-oriented transport protocol used over IP.
Technology sunset/ 2G/3G sunset	The planned withdrawal of an older network technology. A sunset must be managed carefully where devices or emergency services still depend on that technology.
Telemetry	Operational data collected from network equipment and services, such as performance measures, alarms, logs and call records.
Temporary identity	An identifier that can be used to enable an emergency call centre to call a person back when their normal telephone number is unavailable.
TETRA	Terrestrial Trunked Radio. A global LMR open standard engineered for digital trunked two-way radio systems.
Text-to-911/ emergency text	A service that allows people to contact emergency services by text message. The precise name, availability and capability differ between countries.
Time synchronisation/ timing	The distribution of accurate time and frequency across a network. Mobile radio systems depend on precise timing. A timing failure can impair service even when data connections appear available.
Timer/timeout	A configured period after which a device or network function retries an action, changes path or reports failure. Poorly coordinated timers can delay emergency call fallback.
Transport network	The network that carries traffic between access sites, core platforms, data centres and interconnection points. It commonly includes fibre, microwave, routing and transmission systems.
Two-way voice	A call condition in which both parties can hear and speak to each other. A call may appear connected but still fail if voice works in only one direction.
UDP	User Datagram Protocol. A connectionless transport protocol used over IP.
UE	User Equipment. See Device/handset/user equipment (UE).
Unauthenticated call	A call made when a device cannot complete the normal process of proving its subscriber identity. Emergency calling may be permitted without normal authentication.
User plane/data plane	The part of a network that carries customer traffic, including voice media and data, as distinct from the control plane that establishes and manages the connection.
Vendor concentration	Dependence on a small number of suppliers for critical network equipment, software, cloud services or operational tools. It can create a common point of failure.
Virtualisation	Running network functions as software on shared computing infrastructure rather than dedicated physical equipment. It can improve flexibility and efficiency but may introduce shared dependencies.
Voice over LTE (VoLTE)	Voice calling via 4G LTE packet network using IMS.

Term	Definition
Voice over New Radio (VoNR)	Voice calling delivered over a 5G Standalone network using IMS.
VoWiFi/Wi-Fi calling	Voice calling delivered through a Wi-Fi connection while using the operator's mobile voice service. Emergency capability and location support vary by device, operator and jurisdiction.
VPN	Virtual Private Network. An encrypted connection used to securely link a user or organisation to a private network over another network.
Wi-Fi	A local wireless networking technology commonly used in homes, workplaces and public venues. It may provide an alternative route for calling or messaging but depends on local power, broadband and Wi-Fi equipment.
Wilting a site	An informal term for withdrawing or reducing a cell site's advertised availability when it cannot provide a usable service, so devices are encouraged to select another available network.
WLAN	Wireless Local Area Network. A network using wireless connectivity via WiFi.
XML	Extended Mark-up Language. A text-based format used to store, structure and transport data between different software and hardware systems.
Zero-touch automation	Automated network operation or configuration with little or no manual intervention. It can improve speed but requires safeguards, staged roll-out and rollback capability for life-safety services.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK

Email: info@gsma.com

