



SCHOOL OF SCIENCE & TECHNOLOGY

Pervasive and Mobile Computing Systems

Postgraduate Dissertation

Communication Technologies for Man-Made Disasters and
Emergency Response: A Comprehensive Study

Vasileios Karagiannakis

Supervisor: Prof. Periklis Chatzimisios

Patras, Greece

September 2026

Theses / Dissertations remain the intellectual property of students (“authors/creators”), but in the context of open access policy they grant to the HOU a non-exclusive license to use the right of reproduction, customisation, public lending, presentation to an audience and digital dissemination thereof internationally, in electronic form and by any means for teaching and research purposes, for no fee and throughout the duration of intellectual property rights. Free access to the full text for studying and reading does not in any way mean that the author/creator shall allocate his/her intellectual property rights, nor shall he/she allow the reproduction, republication, copy, storage, sale, commercial use, transmission, distribution, publication, execution, downloading, uploading, translating, modifying in any way, of any part or summary of the dissertation, without the explicit prior written consent of the author/creator. Creators retain all their moral and property rights.



Μελέτη των τεχνολογιών επικοινωνίας για αντιμετώπιση
ανθρωπογενών καταστροφών και εκτάκτων καταστάσεων

Βασίλειος Καραγιαννάκης

Επιτροπή Κρίσης

Επιβλέπων Καθηγητής

Καθηγητής Περικλής Χατζημίσιος,

Διεθνές Πανεπιστήμιο της Ελλάδος

Συν-Επιβλέπων Καθηγητής

Καθηγητής Πέτρος Νικοπολιτίδης

Αριστοτέλειο Πανεπιστήμιο
Θεσσαλονίκης

Πάτρα, Σεπτέμβριος 2026

“To my beloved family, Olga, Mariniki and Eleftheria, whose love, patience and unwavering support gave me the strength and inspiration to complete this journey”

“I would like to express my sincere gratitude to my supervisor, Professor Periklis Chatzimisios, for his valuable guidance, continuous support, and constructive feedback throughout the development of this dissertation. His expertise and encouragement were instrumental in shaping this work and bringing it to completion”

Abstract

This dissertation investigates the evolving role of advanced communication technologies in supporting disaster management and emergency response operations during man-made disasters. Modern crisis environments are increasingly characterized by operational complexity, infrastructure interdependence, cyber-physical convergence and cascading failures affecting communication systems, transportation networks, healthcare infrastructures, energy systems and public safety operations simultaneously. In such environments, communication systems no longer function merely as information-transfer infrastructures, but increasingly operate as intelligent and resilient operational ecosystems enabling coordination, situational awareness, distributed decision-making and adaptive response management under highly unstable conditions.

A structured analytical framework was developed to evaluate contemporary literature according to disaster-management phases, technological challenges, evaluation methodologies, network-layer perspectives, operational relevance, architectural maturity, resiliency contribution, cybersecurity integration, AI-driven orchestration and deployment realism. The findings reveal that modern emergency communication research is progressively shifting away from isolated protocol optimization toward highly integrated cross-layer orchestration ecosystems combining networking, distributed intelligence, sensing, virtualization and adaptive operational coordination.

The analysis further demonstrates that simulation-based evaluation remains dominant across the literature, while real-world deployments and operational validation environments remain comparatively limited. In parallel, the findings identify major research trends involving AI-native networking, UAV-assisted resiliency, edge-enabled situational awareness and intelligent cyber-physical coordination, while also revealing persistent research gaps related to transport-layer adaptation, interoperability, cybersecurity integration, autonomous resiliency management and large-scale operational validation.

Keywords

Emergency Communications, 5G/6G Networks, Disaster Response, UAV-Assisted Communications, Edge Computing, Man-made Disasters

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τον εξελισσόμενο ρόλο των τεχνολογιών επικοινωνίας στη διαχείριση ανθρωπογενών καταστροφών. Τα σύγχρονα περιβάλλοντα κρίσεων χαρακτηρίζονται από αυξημένη πολυπλοκότητα, αλληλεξάρτηση κρίσιμων υποδομών, σύγκλιση κυβερνο-φυσικών συστημάτων και αλυσιδωτές αστοχίες που επηρεάζουν τα δίκτυα επικοινωνιών. Στο πλαίσιο αυτό, τα συστήματα επικοινωνιών δεν λειτουργούν πλέον μόνο ως υποδομές μεταφοράς πληροφορίας, αλλά ως ανθεκτικά επιχειρησιακά οικοσυστήματα που υποστηρίζουν τον συντονισμό, την επίγνωση κατάστασης, τη λήψη αποφάσεων και τη διαχείριση κρίσεων υπό ασταθείς συνθήκες.

Για την ανάλυση της βιβλιογραφίας αναπτύχθηκε ένα δομημένο πλαίσιο αξιολόγησης που περιλαμβάνει τις φάσεις διαχείρισης καταστροφών, τις τεχνολογικές προκλήσεις, τις μεθοδολογίες αξιολόγησης, τις προσεγγίσεις ανά επίπεδο δικτύου, την αρχιτεκτονική ωριμότητα, την ανθεκτικότητα, την κυβερνοασφάλεια και την αυτοματοποίηση μέσω τεχνητής νοημοσύνης. Τα αποτελέσματα δείχνουν ότι η σύγχρονη έρευνα στις επικοινωνίες έκτακτης ανάγκης μεταβαίνει από την απομονωμένη βελτιστοποίηση πρωτοκόλλων προς ολοκληρωμένα διαστρωματικά οικοσυστήματα που συνδυάζουν δικτύωση, κατανομημένη νοημοσύνη, αισθητήρες, εικονικοποίηση και προσαρμοσμένο επιχειρησιακό συντονισμό.

Η ανάλυση αναδεικνύει ότι οι προσομοιώσεις εξακολουθούν να αποτελούν την επικρατέστερη μέθοδο αξιολόγησης, ενώ οι δοκιμές πεδίου και οι επιχειρησιακές εφαρμογές μεγάλης κλίμακας παραμένουν περιορισμένες. Παράλληλα, αναδεικνύονται κρίσιμα ερευνητικά κενά που σχετίζονται με τη διαλειτουργικότητα, την κυβερνοασφάλεια, την αυτόνομη διαχείριση της ανθεκτικότητας και την επιχειρησιακή επικύρωση υπό ρεαλιστικές συνθήκες.

Λέξεις – Κλειδιά

Επικοινωνίες Έκτακτης Ανάγκης, Δίκτυα 5G/6G, Διαχείριση Καταστροφών, Δικτύωση με Τεχνητή Νοημοσύνη, Επικοινωνίες μέσω UAV, Υπολογιστική Ακμής, Ανθρωπογενείς Καταστροφές

Table of Contents

Abstract	v
Περίληψη.....	vi
Table of Contents	vii
List of Figures	ix
List of Tables.....	xi
List of Abbreviations & Acronyms	xii
1. Introduction	1
1.1 The Changing Nature of Disasters	1
1.2 Why Communications Systems Become the Backbone of Disaster Response.....	4
1.3 Motivation and Research Problem	7
2. Theoretical Background and Technological Foundations.....	11
2.1 5G Architecture and Mission-Critical Networking.....	17
2.2 MEC, Edge Intelligence and AI-Native Networking.....	23
2.3 NTN/UAV Integration and Non-Terrestrial Emergency Communications	30
2.4 OSI Mapping and Cross-Layer Integration in Emergency Communication.....	34
2.5 Disaster Communication and Operational Requirements	40
3. Research Methodology and Analytical Framework.....	47
3.1 Data Sources and Search Strategy.....	47
3.1.1 Inclusion and Exclusion Criteria	53
3.1.2 Academic Papers Refinement and Categorization	54
3.2 Analytical Dimensions and Classification Framework.....	55
3.2.1 Disaster Management Phase Classification	58
3.2.2 Key Research Challenges Classification.....	59
3.2.3 Evaluation Methodology Classification.....	61
3.2.4 Network Layer and OSI Perspective.....	63
3.3 Analytical Protocol, Evidence Extraction and Scoring Procedure.....	64
3.4 Alignment with Supervisory Evaluation Criteria.....	66
3.5 Research-Question Traceability and Roadmap	67
4. RQ1 Evaluation Methodologies and Their Effect on Generalizability	70
4.1 Methodological Framework	73
4.2 Statistical Analysis and Its Effect on Generalizability.....	76
4.2.1 Distribution of Primary Evaluation Methods	78
4.2.2 Mean Score by Validation Dimension	80
4.2.3 Validation Maturity Distribution.....	81
4.2.4 Interaction Between Method and Generalizability	83
4.2.5 Interpretation for RQ1	85
4.3 Quantitative Analysis of Evaluation Methodologies	87
4.4 Final Answer to RQ1	92
5. RQ2 Integration of Advanced Paradigms in Emergency Communication Systems...95	
5.1 Methodological Framework	96
5.2 Taxonomy of Advanced Paradigms	101
5.3 Functional Taxonomy of Advanced Paradigms	105
5.3.1 AI-Native Intelligent Communication Systems	107
5.3.2 Resilient Communication Infrastructures	111
5.3.3 Secure and Trustworthy Integration Frameworks.....	115
5.3.4 Cyber-Physical Mission-Critical Ecosystems	119

5.4	Final Answer to RQ2	125
6.	RQ3 Network Layer Perspectives in Crisis Communication Systems	130
6.1	Methodological Framework for RQ3 Evaluation	135
6.1.1	Network Layer Classification	140
6.1.2	Evaluation Dimensions	146
6.2	Quantitative Distribution of Research Attention Across Network Layers.....	150
6.2.1	Dominance of Cross-Layer Architectures.....	152
6.2.2	Data Link and Network Layer Attention	153
6.2.3	Transport-Layer Research Attention.....	155
6.2.4	Application-Layer Research Attention.....	156
6.3	Final Answer to RQ3	157
7.	Conclusions and Future Research Directions	160
7.1	Conclusions Related to RQ1	160
7.2	Conclusions Related to RQ2	163
7.3	Conclusions Related to RQ3	165
7.4	Conclusions Related to Stakeholder Communication Needs.....	168
7.5	Final Remarks	170
	References	173
	Appendix A: “Primary Research Papers Included in the Study”	183

List of Figures

Figure 1 Simplified architecture of a TETRA-based public safety communication system. Source: Author's synthesis based on [1].	11
Figure 2 Evolution of Mobile Communication Technologies from 1G to 5G and Their Relevance to Public Safety Communications. Source: Author's synthesis based on the reviewed literature [4], [13], and [28].	13
Figure 3 Layered LTE Network Architecture for Public Safety Broadband Communications. Source: Author's synthesis based on the reviewed literature [4].	14
Figure 4 LTE Evolved Packet Core (EPC) Architecture Supporting Mission-Critical Broadband Communications. Source: Author's synthesis based on the reviewed literature [4], [28].	15
Figure 5 High-Level 5G Network Architecture Supporting Mission-Critical Communications. Source: Author's synthesis based on the reviewed literature [29]–[31].	19
Figure 6 Core 5G Service Categories Supporting Mission-Critical Public Safety Communications. Source: Author's synthesis based on the reviewed literature [29]–[32].	20
Figure 7 SDN/NFV-Based Adaptive Architecture for Mission-Critical Public Safety Networks. Source: Author's synthesis based on the reviewed literature [29]–[34].	21
Figure 8 5G Network Slicing Architecture Supporting Differentiated QoS and Resource Isolation for Mission-Critical PPDR Communications. Source: Author's synthesis based on the reviewed literature [29]–[34].	22
Figure 9 End-to-End 5G-Enabled Mission-Critical Public Safety Ecosystem Integrating Network Slicing, Edge Computing, AI-Native Services, SDN/NFV Orchestration and Heterogeneous Communication Infrastructures for Resilient Disaster Response. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[34].	23
Figure 10 MEC Architecture Workflow for Mission-Critical Emergency Communications. Source: Author's synthesis based on references [29]–[35].	24
Figure 11 Edge Intelligence Pipeline for Real-Time Analytics and AI-Driven Decision Support in Mission-Critical Emergency Communications. Source: Author's synthesis based on references [29]–[35].	26
Figure 12 AI-Native Networking Architecture for Autonomous Network Orchestration in Mission-Critical Emergency Communications. Source: Author's synthesis based on the reviewed literature [29]–[35].	27
Figure 13 Integrated MEC-Enabled Disaster Communication Ecosystem Supporting AI-Driven Mission-Critical Emergency Response. Source: Author's synthesis based on references [29]–[35].	29
Figure 14 Integrated NTN-Enabled Emergency Communication Ecosystem. Source: Author's synthesis integrating concepts from the reviewed literature [35]–[38].	31
Figure 15 Space-Air-Ground Integrated Network (SAGIN). Source: Author's synthesis integrating NTN, SAGIN, UAV-assisted networking, MEC, 5G/6G mission-critical networking, cloud-edge concepts and the reviewed literature [36]–[44].	33
Figure 16 OSI Model Mapping for Emergency Communication Systems. Source: Author's synthesis based on the reviewed literature [36]–[44].	36
Figure 17 Cross-Layer Emergency Communication Architecture. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44].	37
Figure 18 Cross-Layer Operational Workflow Supporting Mission-Critical Emergency Communications. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44].	39

Figure 19 Operational Environment of Mission-Critical Disaster Communication Systems. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44]...	41
Figure 20 Mission-Critical Operational Requirements for Emergency Communication Systems. Source: Author's synthesis integrating mission-critical communication requirements from the reviewed literature [29]–[44].....	43
Figure 21 Integrated Disaster Communication Ecosystem. Source: Author's synthesis integrating terrestrial, aerial, NTN, edge/MEC, cloud, AI-native networking, IoT, and mission-critical communication concepts from the reviewed literature [29]–[44].....	45
Figure 22 Boolean Query Stratification Across Hazard Classes and Technology Generations. Author's illustration.....	49
Figure 23 Literature Review Workflow and Analytical Pipeline. Author's illustration.	50
Figure 24 Unified Analytical Framework and Orthogonal Classification Dimensions. Author's conceptual illustration.....	58
Figure 25 Distribution of Primary Evaluation Methods.	79
Figure 26 Mean Scores by Evaluation Dimension.....	81
Figure 27 Validation Maturity Distribution.	82
Figure 28 Primary Method vs Generalizability.....	83
Figure 29 Mean Dimension Scores.	85
Figure 30 Frequency Distribution in RQ2 Dataset.	104
Figure 31 Functional Taxonomy of Paradigms. Source: Author's own analysis and functional taxonomy derived from the systematic review dataset (RQ2).	107
Figure 32 AI Co-occurrence Patterns in RQ2 Dataset.	109
Figure 33 Resilient Communication Infrastructure Components in RQ2 Dataset.....	112
Figure 34 Security and Trust Paradigms in RQ2 Dataset.	117
Figure 35 Cyber-Physical Paradigms in RQ2 Dataset.	123
Figure 36 Evolution of Emergency Communication Architectures.....	131
Figure 37 Network Layer Perspectives in Crisis Communication Systems.	133
Figure 38 Cross-Layer Orchestration Ecosystem.	134
Figure 39 Multidimensional RQ3 Evaluation Framework.....	140
Figure 40 Distribution of Research Attention Across Network Layers.....	141
Figure 41 Evolution from Isolated Networking Layers to Cross-Layer Orchestration Ecosystems.....	146
Figure 42 Quantitative Distribution of Research Attention Across Network Layers.	152

List of Tables

Table 1 Systematic Search Strategy for the Identification and Selection of Relevant Studies	52
Table 2 Inclusion and Exclusion Criteria and Screening Workflow.....	54
Table 3 Simulation and Analytical Evaluation.	89
Table 4 Testbed and Field Validation.	90

List of Abbreviations & Acronyms

3GPP	3rd Generation Partnership Project
5GC	5G Core
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
BLE	Bluetooth Low Energy
CSI	Channel State Information
DMR	Digital Mobile Radio
DSA	Dynamic Spectrum Access
DTN	Delay-Tolerant Networking
EMI	Electromagnetic Interference
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
GCSE	Group Communication System Enablers
IoT	Internet of Things
ISAC	Integrated Sensing and Communication
KPI	Key Performance Indicator
LMR	Land Mobile Radio
LPWAN	Low-Power Wide-Area Network
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LTE	Long-Term Evolution
MCPTT	Mission Critical Push-to-Talk
MCS	Modulation and Coding Scheme
MEC	Multi-access Edge Computing
mmWave	Millimeter Wave

mMTC	Massive Machine-Type Communications
NFV	Network Function Virtualization
NTN	Non-Terrestrial Network
OSI	Open Systems Interconnection
P25	Project 25
PPDR	Public Protection and Disaster Relief
PRRM	Preparedness–Response–Recovery–Mitigation
ProSe	Proximity Services
PSLTE	Public Safety LTE
PTT	Push-to-Talk
QoS	Quality of Service
RAN	Radio Access Network
RAS	Reliability, Availability and Survivability
RF	Radio Frequency
SAGIN	Space-Air-Ground Integrated Network
SAR	Search and Rescue
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SMF	Session Management Function
TETRA	Terrestrial Trunked Radio
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communications
V2X	Vehicle-to-Everything
WSN	Wireless Sensor Network

1. Introduction

1.1 The Changing Nature of Disasters

Modern disasters no longer evolve as isolated operational incidents confined within a single geographical area or technological domain. Contemporary crisis environments are increasingly characterized by interconnected failures capable of simultaneously affecting communication infrastructures, transportation systems, healthcare services, energy networks, industrial facilities, governmental coordination mechanisms, and civilian populations [1], [2], [3]. As societies become progressively dependent on digital infrastructures and highly interconnected technological ecosystems, the operational impact of man-made disasters extends far beyond the initial triggering event itself [4], [5]. In many cases, the secondary and cascading consequences of a disaster become significantly more destructive than the original incident [6].

Industrial accidents, cyberattacks, transportation disasters, terrorist attacks, large-scale infrastructure failures, and hybrid threats increasingly expose the structural fragility of modern interconnected societies. A single disruption within one critical infrastructure domain can rapidly propagate across multiple operational sectors, creating highly dynamic crisis environments characterized by uncertainty, instability, and operational fragmentation. A cyberattack targeting energy management systems may simultaneously disrupt telecommunications and emergency coordination. A transportation accident involving hazardous materials may trigger evacuation operations, healthcare overload, communication congestion, and transportation paralysis within minutes. Similarly, terrorist attacks against urban infrastructures often generate simultaneous physical, digital, and psychological disruption affecting both operational coordination and civilian stability [6].

Unlike traditional disaster environments, modern crises evolve within highly interconnected cyber-physical ecosystems where communication systems, sensing infrastructures, cloud services, Internet of Things (IoT) platforms, transportation networks and critical infrastructures continuously interact in real time. This interdependence significantly increases operational complexity because failures rarely remain localized. Instead, they propagate rapidly across multiple infrastructures through cascading effects that can amplify operational disruption far beyond the initial area of impact.

One of the most defining characteristics of modern disaster environments is therefore the emergence of cascading failures. In contemporary crises, the collapse of one infrastructure frequently destabilizes several others simultaneously. Communication disruptions may affect emergency coordination. Energy failures may disable transportation systems and healthcare infrastructures. Cyberattacks may simultaneously disrupt industrial control systems, public services, and operational decision-making environments. As a result, emergency-response operations increasingly occur within unstable ecosystems where infrastructures continuously influence one another under rapidly evolving conditions [2].

Within these environments, maintaining situational awareness becomes one of the most critical operational requirements. Decision-makers must continuously monitor infrastructure status, responder deployment, communication availability, environmental conditions, civilian movement, and operational risks in real time. However, the operational complexity of modern disasters frequently overwhelms conventional coordination mechanisms. Information becomes fragmented, communication channels become congested, and operational visibility rapidly deteriorates as the crisis evolves [7].

For this reason, communication systems increasingly function as the operational backbone of modern disaster response ecosystems rather than as simple information-transfer infrastructures [8], [9]. During large-scale emergencies, communication networks support coordination among governmental authorities, emergency responders, healthcare services, military units, transportation operators and critical infrastructure providers simultaneously. They also enable real-time situational awareness, distributed decision-making, emergency alert dissemination, telemetry exchange, Unmanned Aerial Vehicle (UAV) coordination and operational resource management under highly degraded conditions [10].

The analysis of recent disasters demonstrates that communication collapse often becomes a major multiplier of the crisis itself. In many cases, the inability to maintain reliable communication continuity significantly accelerates operational disorganization and reduces the effectiveness of emergency response activities. When communication infrastructure fails, emergency services lose operational visibility, coordination between agencies becomes fragmented, resource allocation slows down, and decision-making processes become increasingly reactive rather than adaptive. Under such conditions, even relatively localized incidents may rapidly escalate into broader systemic crises [11].

This phenomenon has become increasingly visible across multiple categories of modern disasters. During large-scale cyberattacks, communication congestion and network instability may delay operational coordination and infrastructure recovery efforts. During terrorist incidents or transportation disasters, overloaded communication infrastructures may prevent responders from exchanging critical operational information in real time. Similarly, during industrial accidents or infrastructure failures, the simultaneous disruption of power grids and communication systems may severely reduce authorities' ability to coordinate evacuation procedures and public safety operations [\[12\]](#).

At the same time, modern disasters increasingly evolve within environments characterized by high mobility, dense urbanization, distributed sensing infrastructures and continuous digital interconnectivity. Emergency communication systems must therefore support not only voice communication, but also real-time video exchange, distributed telemetry, autonomous systems, IoT sensing, UAV coordination, AI-assisted analytics and continuous operational synchronization among multiple heterogeneous actors operating simultaneously under time-critical conditions [\[13\]](#), [\[14\]](#).

Consequently, the operational requirements imposed on modern emergency communication systems have expanded dramatically. Conventional communication architectures originally designed for stable civilian environments and predictable traffic conditions are no longer sufficient to support the complexity of modern disaster response operations. Future emergency communication ecosystems must operate under infrastructure degradation, cyber threats, intermittent connectivity, severe congestion, mobility disruptions and rapidly changing operational demands while simultaneously maintaining reliability, interoperability, resiliency and real-time situational awareness [\[15\]](#).

This transformation fundamentally changes the role of communication technologies within disaster management. Communication systems are no longer interpreted simply as supporting infrastructures facilitating information exchange between responders. Instead, they increasingly function as intelligent operational ecosystems integrating networking, sensing, distributed computing, orchestration and decision-support mechanisms within highly adaptive cyber-physical environments capable of supporting complex crisis management operations under extreme conditions.

1.2 Why Communications Systems Become the Backbone of Disaster Response

Effective disaster response is fundamentally dependent on communication. Regardless of the scale, type, or origin of a crisis, emergency operations cannot function without the continuous exchange of information between responders, coordination centers, governmental authorities, infrastructure operators and affected civilian populations. Communication enables coordination, coordination enables operational response and operational response ultimately determines the effectiveness of crisis management itself. When communication becomes fragmented or unavailable, the entire emergency-response ecosystem rapidly loses coherence [\[11\]](#).

In modern disaster environments, the importance of communication extends far beyond simple information exchange. Communication systems increasingly function as the operational backbone of disaster response ecosystems because they support nearly every critical emergency-management activity simultaneously. Resource allocation, situational awareness, responder deployment, evacuation coordination, medical support, infrastructure recovery, inter-agency synchronization, and public warning dissemination all depend on the continuous availability of reliable communication infrastructure operating under highly unstable conditions [\[16\]](#).

Without communication, emergency responders lose the ability to coordinate operational actions in real time. Without coordination, disaster response operations become fragmented, delayed, and inefficient. Most importantly, without continuous situational awareness, operational decision-making becomes effectively blind. Authorities may no longer possess accurate visibility regarding infrastructure status, responder locations, civilian movement, operational risks, or the evolving dynamics of the crisis environment. Under such conditions, even highly trained emergency organizations struggle to maintain operational effectiveness [\[11\]](#).

Historically, emergency communication systems were primarily designed as voice-centric infrastructures intended to support relatively limited coordination requirements between emergency personnel and command centers [\[1\]](#). Conventional public safety communication networks focused mainly on radio coverage, voice reliability, and basic interoperability between operational units [\[13\]](#). For decades, these systems were considered sufficient

because emergency operations themselves were comparatively less dependent on continuous real-time data exchange and distributed operational synchronization [8].

However, the operational nature of disasters has changed dramatically. Contemporary emergencies increasingly unfold within highly interconnected digital environments involving cyber-physical infrastructures, distributed sensing systems, autonomous platforms, mobile operational units, cloud services and real-time data-driven coordination mechanisms. As a result, communication systems are no longer expected simply to carry voice traffic between responders. Instead, they must support continuous operational synchronization across highly heterogeneous ecosystems operating under severe time pressure and infrastructure instability [13], [15].

Modern emergency communication systems now support far more complex operational functions, including real-time video transmission, telemetry exchange, UAV coordination, distributed sensing, AI-assisted analytics, operational resource tracking, dynamic situational awareness generation and adaptive multi-agency coordination [17]. This transformation has fundamentally changed the role of communication infrastructures within disaster management. Communication systems increasingly function not merely as transport networks, but as intelligent operational ecosystems integrating networking, sensing, distributed computing, orchestration and decision-support capabilities within unified environments.

One of the most important operational requirements emerging from this transformation is interoperability. During large-scale disasters, multiple organizations must coordinate simultaneously, including police forces, firefighters, healthcare providers, civil protection agencies, military units, transportation authorities, and infrastructure operators [11]. Each organization may utilize different communication technologies, operational procedures and information-management systems. Consequently, emergency communication infrastructures must support seamless interoperability across highly heterogeneous operational domains in order to maintain coherent disaster response coordination [7].

At the same time, latency has become a critical operational parameter within modern crisis environments. Many emergency-response activities now depend on real-time information exchange and low-latency communication continuity [17]. Situational-awareness systems, autonomous UAV coordination, remote medical support, mission-critical voice services and distributed command-and-control mechanisms all require communication infrastructures

capable of minimizing delay under highly unstable networking conditions [17]. Even relatively short latency spikes or communication interruptions may significantly affect operational awareness and decision-making efficiency during time-sensitive disaster response operations [18].

Resilience and survivability have also emerged as foundational architectural requirements for modern emergency communication systems. Unlike conventional commercial networking environments, disaster response ecosystems must continue operating even when infrastructures become partially damaged, overloaded, fragmented, or exposed to cyber threats and environmental disruption. Communication systems must therefore support adaptive re-routing, backup connectivity, distributed coordination and infrastructure-independent operation capable of maintaining partial operational continuity even under degraded conditions [13], [15].

This requirement becomes especially important because communication infrastructure itself is frequently a victim of the disaster. Earthquakes may damage terrestrial communication facilities, cyberattacks may disrupt digital infrastructures, industrial accidents may affect power grids and communication availability simultaneously and large-scale emergencies may overload cellular networks beyond operational capacity. Under such conditions, maintaining communication continuity becomes one of the highest operational priorities because the collapse of communication systems often accelerates the broader collapse of coordinated emergency response [15].

Another defining characteristic of modern emergency communication ecosystems is the growing importance of distributed coordination. Contemporary disaster response operations increasingly involve decentralized operational environments where decision-making, sensing, computation and communication occur simultaneously across multiple distributed nodes rather than through a single centralized command structure. UAVs, mobile edge nodes, IoT infrastructures, autonomous systems, field responders and distributed operational centers continuously exchange information and coordinate actions in real time across highly dynamic environments [19].

As a result, communication systems increasingly evolve toward adaptive and orchestration-centric operational architectures capable of integrating heterogeneous infrastructures while dynamically responding to changing operational conditions. This evolution reflects a broader shift in disaster management philosophy itself. Future emergency communication

ecosystems will not simply provide connectivity between responders, they will increasingly function as intelligent coordination environments capable of supporting predictive situational awareness, adaptive operational management, autonomous resource orchestration and resilient distributed decision-making during highly uncertain crisis conditions [18].

Ultimately, the growing operational dependence on communication infrastructures demonstrates that communication is no longer a supporting component of disaster response. It has become the central operational foundation upon which modern crisis management ecosystems depend. The ability to maintain resilient, interoperable, adaptive and continuously available communication environments increasingly determines the effectiveness, speed and survivability of modern disaster response operations.

1.3 Motivation and Research Problem

Over the last decade, emergency communication research has expanded rapidly in response to the growing complexity of modern disaster environments. The increasing frequency of cyberattacks, critical infrastructure failures, industrial accidents, hybrid threats, transportation disasters and large-scale urban emergencies has intensified both scientific and operational interest in resilient communication ecosystems capable of supporting crisis-response operations under highly unstable conditions. As a result, contemporary literature now covers an exceptionally broad range of technologies, networking paradigms, orchestration mechanisms and operational coordination models associated with disaster communications [20].

At the same time, the evolution of 5G, the emergence of 6G-oriented architectures, advances in Artificial Intelligence (AI), edge computing, UAV-assisted networking, non-terrestrial communication systems, cyber-physical infrastructures and distributed sensing ecosystems have fundamentally transformed the technological landscape of emergency communications. Modern disaster response systems increasingly combine communication, sensing, computation, automation and intelligent orchestration within deeply interconnected operational environments. Consequently, emergency communication research has evolved into a highly multidisciplinary scientific domain involving networking, AI, cyber resilience, distributed systems, operational coordination, public safety engineering and crisis-management strategy simultaneously [21], [22].

Despite this rapid technological progress, the existing literature remains highly fragmented and difficult to analyze from a unified operational perspective. Many studies focus narrowly on isolated networking layers, specific protocols, or individual technologies without adequately examining how these mechanisms interact within broader disaster response ecosystems. In several cases, research contributions remain heavily specialized in specific technical domains such as routing optimization, Quality of Service (QoS) enhancement, UAV deployment strategies, edge orchestration, or AI-based resource allocation while providing limited discussion regarding their operational integration into realistic emergency-response environments [\[23\]](#).

This fragmentation becomes especially visible across the communication stack itself. Some studies investigate physical-layer resilience and spectrum survivability under degraded conditions, while others focus primarily on routing protocols for Mobile Ad hoc NETWORKS (MANETs), UAV-assisted communication, congestion management, transport-layer optimization, or application-layer situational-awareness systems. Although each of these contributions provides valuable technical insight, the related literature frequently lacks a unified analytical perspective that explains how these isolated mechanisms collectively contribute to resilient disaster response ecosystems.

A similar fragmentation also appears across the disaster-management lifecycle. Existing research often concentrates on specific operational phases independently rather than approaching disaster communications as a continuous and evolving operational process. Certain studies emphasize preparedness through training environments, simulation frameworks and early-warning communication systems. Others focus primarily on real-time emergency response coordination, mission-critical communication continuity, or post-disaster infrastructure recovery mechanisms. More recent research increasingly investigates mitigation-oriented approaches involving predictive analytics, AI-assisted risk assessment and proactive communication adaptation mechanisms. However, relatively few studies attempt to analyze how communication architectures support the full crisis lifecycle in an integrated and operationally coherent manner.

Another major challenge concerns the diversity of research priorities and evaluation perspectives across related literature. Existing studies investigate a wide range of operational and technical challenges including communication reliability, infrastructure resilience, latency-sensitive coordination, QoS continuity, cybersecurity, privacy

protection, interoperability, energy efficiency and sustainability [9]. However, these dimensions are often evaluated independently, making it difficult to identify broader technological trends and architectural transitions shaping the evolution of next-generation emergency communication systems.

The problem is further intensified by the absence of consistent evaluation methodologies across the field. A substantial portion of emergency communication research relies heavily on simulations, analytical models and theoretical optimization frameworks. Other studies utilize laboratory testbeds, emulation environments, pilot deployments, or cross-disciplinary policy-oriented frameworks combining technical and organizational perspectives. While this methodological diversity reflects the complexity of disaster environments, it also creates significant challenges regarding comparability, reproducibility, operational realism and the generalizability of research findings [20].

In parallel, modern emergency communication systems increasingly evolve beyond traditional networking infrastructures toward highly distributed cyber-physical ecosystems integrating IoT platforms, UAVs, edge computing, cloud orchestration, AI-native networking, blockchain-based trust mechanisms, digital twins and autonomous operational coordination [22]. Emerging paradigms such as Integrated Sensing and Communication (ISAC), Space-Air-Ground Integrated Networks (SAGIN), non-terrestrial networking (NTN), AI-driven orchestration and edge-native resiliency engineering indicate that future disaster response ecosystems will operate as intelligent multi-domain environments rather than conventional communication systems alone [24].

Another gap identified in the related literature concerns the relationship between emerging 6G paradigms and future disaster response ecosystems. While many recent studies discuss 6G technologies in terms of throughput, latency reduction, or spectrum efficiency, fewer studies investigate how 6G may fundamentally transform disaster management itself through AI-native orchestration, integrated sensing, distributed intelligence, semantic communication, autonomous coordination and cyber-physical operational awareness. Consequently, the role of 6G within future DisasterX ecosystems remains insufficiently explored from a holistic operational perspective [25], [26].

The related literature also reveals limited integration between technological innovation and stakeholder-oriented operational analysis. Public authorities, first responders, citizens, healthcare providers, military units and critical infrastructure operators all possess different

communication priorities during disasters. Nevertheless, many studies focus primarily on technological performance without adequately examining how communication systems address the heterogeneous operational needs of different disaster response actors operating simultaneously under crisis conditions.

These limitations collectively reveal a broader scientific gap within current emergency communication research. Although related literature contains substantial technological innovation, it remains fragmented across technologies, networking layers, operational domains, disaster-management phases and evaluation methodologies. As a result, a structured, multidimensional analytical perspective is needed to synthesize contemporary research trends while identifying recurring architectural transitions, validation weaknesses, operational gaps, and emerging technological trajectories.

This dissertation was therefore motivated by the need to provide a unified analytical framework for understanding how modern emergency communication systems evolve toward intelligent, resilient and orchestration-centric cyber-physical ecosystems. Rather than examining isolated communication technologies independently, the study approaches emergency communications as integrated operational environments where networking, sensing, distributed intelligence, orchestration and adaptive coordination continuously interact under highly dynamic disaster conditions.

To address these challenges, the dissertation examines three interrelated research questions: the evaluation methodologies used to validate communication solutions for man-made disasters and their impact on the realism and generalizability of findings; the integration of advanced paradigms, including AI-native networking, UAV-assisted relays, ISAC, blockchain-based trust mechanisms, and distributed orchestration; and the networking layers receiving the greatest research attention, along with the key architectural and operational gaps that remain unexplored.

Through this multidimensional approach, the dissertation goes beyond reviewing existing technologies to identify the broader transformation of emergency communications toward AI-native, highly orchestrated, and interconnected disaster response ecosystems.

2. Theoretical Background and Technological Foundations

Public safety communication systems are central to modern crisis management and disaster response, evolving from isolated voice-centric radio systems to broadband and interoperable communication environments. Historically, emergency responders—including police, fire brigades, emergency medical services, military units, coast guards, and civil protection authorities—relied primarily on narrowband Land Mobile Radio (LMR) systems designed for reliable mission-critical voice communication [10]. Early systems were predominantly analog, operating on dedicated spectrum and fixed architectures. Despite their reliability, they presented significant limitations in scalability, interoperability, mobility management, data transmission, and spectrum efficiency. As emergency operations became more complex, their inability to support multimedia services and real-time situational awareness became an increasingly important operational constraint.

These limitations drove the adoption of digital narrowband technologies such as Project 25 (P25), Terrestrial Trunked Radio (TETRA), TETRAPOL, and Digital Mobile Radio (DMR). Compared with analog systems, these technologies introduced encrypted digital voice, group communications, push-to-talk (PTT), device authentication, and improved spectrum utilization. P25 became particularly prominent in North America, while TETRA achieved widespread adoption in Europe and other international public safety environments. Figure 1 presents a simplified TETRA public safety communication architecture as an author's synthesis based on the reviewed literature [1].

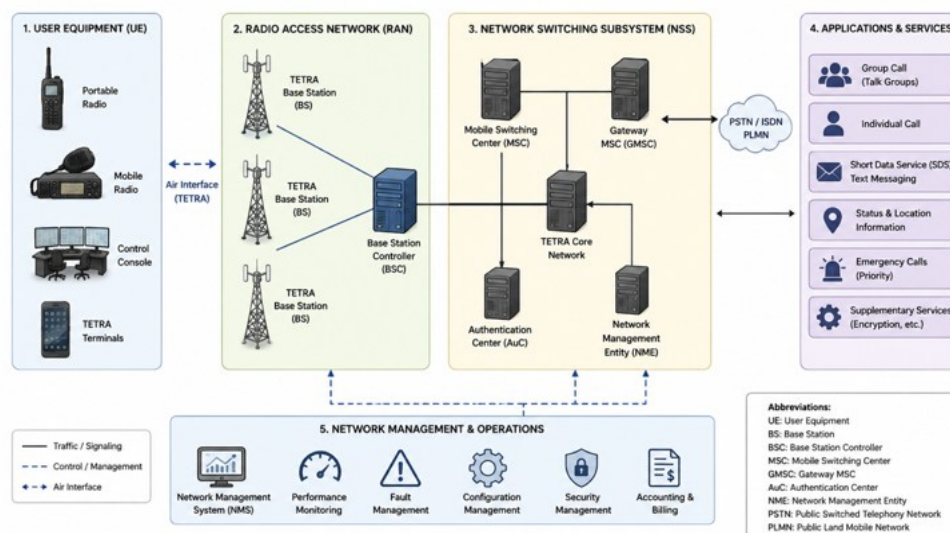


Figure 1 Simplified architecture of a TETRA-based public safety communication system. Source: Author's synthesis based on [1].

Despite these improvements, narrowband systems remained fundamentally voice-centric, with data capabilities far behind the rapidly evolving commercial cellular domain. Consequently, many public safety organizations continued relying on technologies developed decades earlier, while commercial networks progressed toward broadband multimedia services and high-speed mobile connectivity.

These limitations became particularly evident during large-scale disasters and multi-agency operations. Legacy systems provided limited support for multimedia services, real-time video and large volumes of operational data. Interoperability also remained a persistent challenge due to incompatible protocols and fragmented network infrastructures, while limited flexibility in resource allocation and traffic management constrained adaptation to rapidly changing conditions. Consequently, situational awareness and network scalability were often insufficient during periods of heavy communication demand [\[27\]](#).

Interoperability emerged as a critical operational challenge, as police, firefighters, healthcare responders and military organizations often relied on incompatible protocols, frequencies and vendor-specific infrastructures. This fragmentation hindered information exchange and coordination during joint operations. Events such as the September 11, 2001 attacks and Hurricane Katrina exposed these technological limitations and accelerated efforts toward interoperable broadband emergency communications. Mission-critical networks increasingly needed to support not only voice but also real-time data, geolocation, sensors, images and distributed situational awareness [\[17\]](#).

These limitations accelerated the migration from traditional LMR systems toward Long-Term Evolution (LTE)-based public safety broadband architectures. LTE introduced packet-switched broadband networking, reduced latency and IP-native service integration. Figure 2 presents the broader evolution from legacy mobile systems to broadband and intelligent networking ecosystems, synthesizing mobile communication technologies across generations (1G–5G) from multiple literature sources. Since no single publication presents this exact representation, the figure is classified as a literature synthesis rather than an adapted or reproduced figure [\[28\]](#).

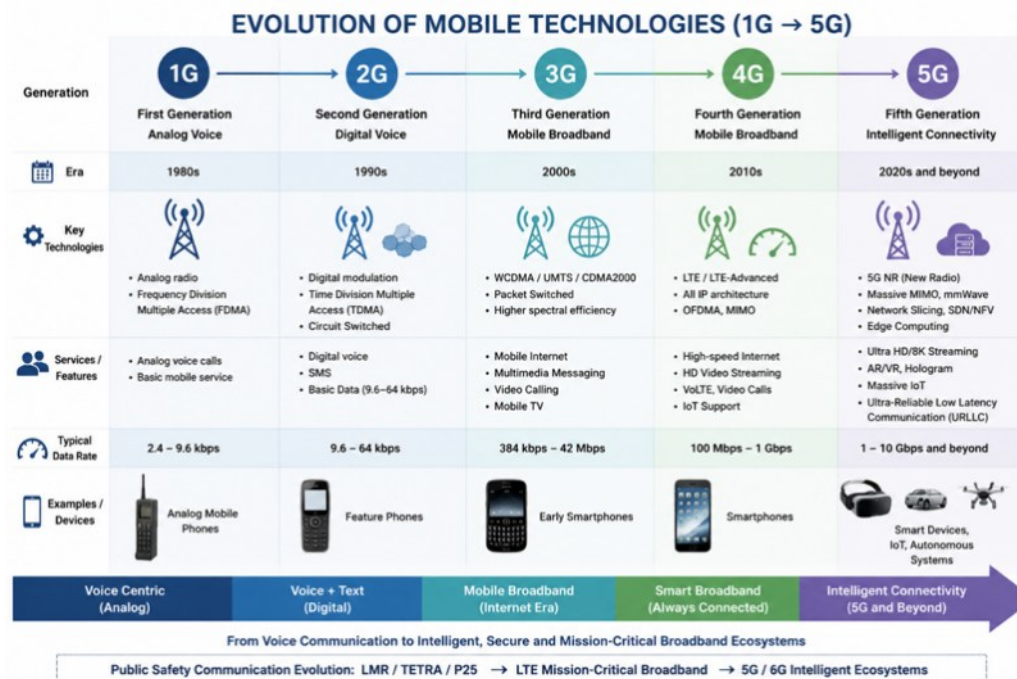


Figure 2 Evolution of Mobile Communication Technologies from 1G to 5G and Their Relevance to Public Safety Communications. Source: Author's synthesis based on the reviewed literature [4], [13], and [28].

Unlike legacy narrowband systems, LTE-based architectures could support multiple communication services simultaneously within a unified broadband environment. In addition to conventional voice communication, LTE infrastructures enabled real-time video transmission, telemetry exchange, IoT-based sensing, command-and-control applications and data-driven operational analytics. The use of packet-switched, IP-based networking also facilitated the integration of heterogeneous applications and information sources within a common communication infrastructure, allowing operational data to be distributed more effectively across different users and agencies. This broader communication capability significantly improved situational awareness and enabled emergency responders to exchange critical information more efficiently during complex disaster response operations. Furthermore, the increased bandwidth and service flexibility of LTE networks created a more scalable foundation for mission-critical applications requiring continuous access to multimedia and operational data. The layered structure of LTE public safety networking environments, including the interaction between communication infrastructure, service platforms and operational applications, is illustrated in Figure 3.

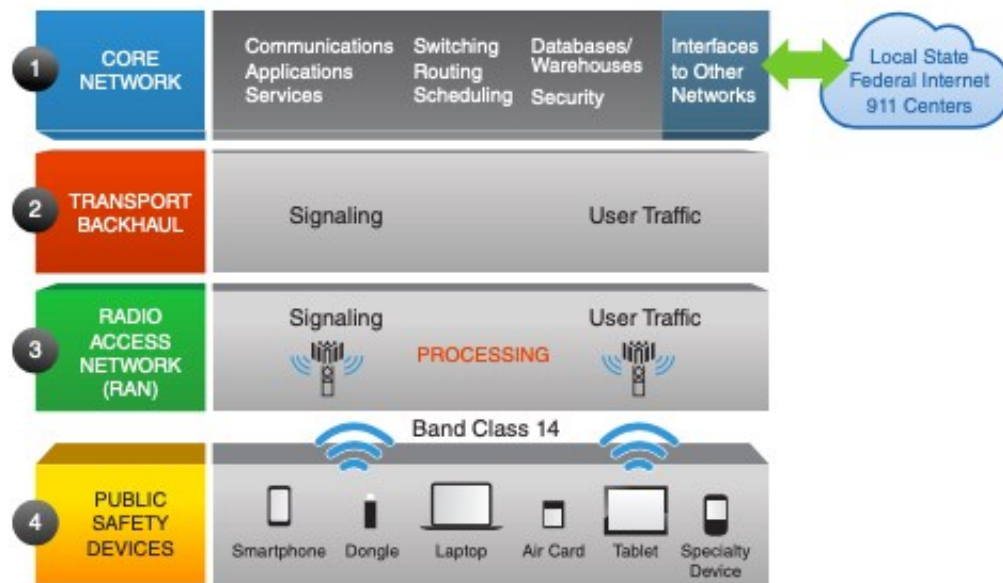


Figure 3 Layered LTE Network Architecture for Public Safety Broadband Communications. Source: Author's synthesis based on the reviewed literature [4].

The emergence of Public Protection and Disaster Relief (PPDR) broadband systems represented a major architectural milestone in the evolution of emergency communications [9]. PPDR systems extended traditional mission-critical networking by integrating broadband communication services specifically designed to support the operational requirements of emergency response environments. Beyond conventional voice services, these infrastructures enabled first responders to access real-time maps, biometric information, live video feeds, UAV imagery and distributed sensor data directly from the field. The integration of these heterogeneous information sources within a common broadband infrastructure enhanced information sharing between field personnel, command centers and cooperating agencies, supporting faster and more coordinated operational decision-making. Moreover, broadband PPDR architectures provided a flexible platform for deploying advanced mission-critical services while maintaining reliable connectivity across geographically distributed emergency operations. This evolution marked an important transition from primarily voice-oriented public safety networks toward integrated, data-intensive communication ecosystems capable of supporting increasingly complex emergency scenarios. Figure 4 presents the LTE/Evolved Packet Core (EPC) architecture supporting broadband mission-critical communications and public safety services.

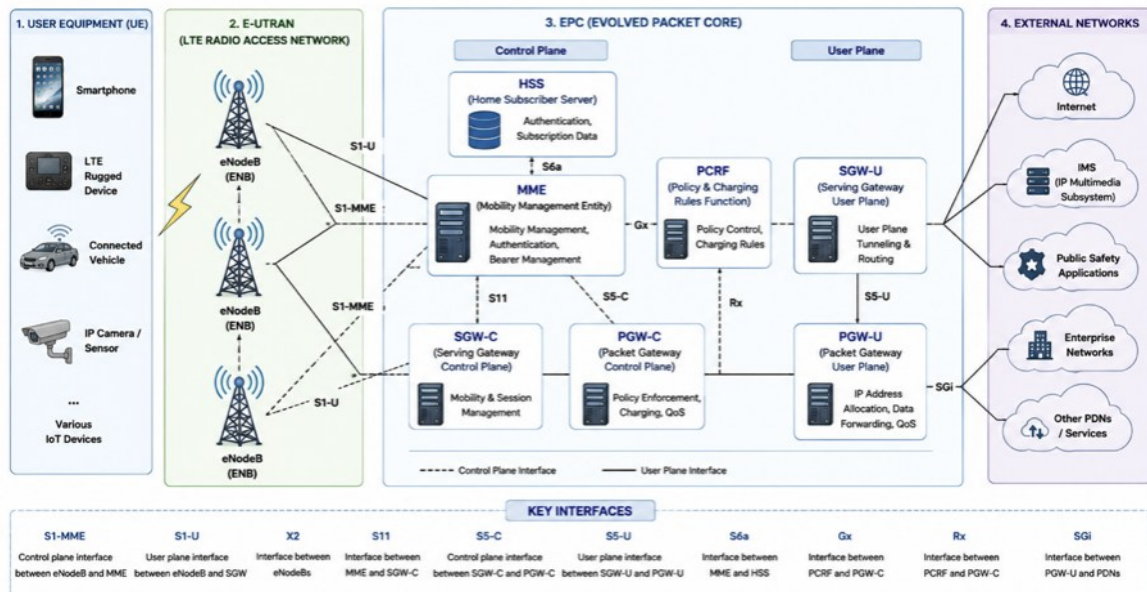


Figure 4 LTE Evolved Packet Core (EPC) Architecture Supporting Mission-Critical Broadband Communications. Source: Author's synthesis based on the reviewed literature [4], [28].

Simultaneously, LTE evolved to incorporate mission-critical functionalities previously associated exclusively with narrowband systems. Features such as Mission-Critical Push-to-Talk (MCPTT), Group Call System Enablers (GCSE) and Proximity Services (ProSe) enabled LTE architectures to gradually replicate and surpass many traditional TETRA and P25 operational capabilities. According to the related literature, LTE-based mission-critical systems introduced substantial improvements regarding flexibility, scalability and multimedia support while maintaining reliability and security requirements necessary for emergency operations [19].

Another major driver of broadband transition was the rapid proliferation of smart devices, distributed sensing infrastructures and IoT technologies. Modern emergency response operations increasingly rely on heterogeneous cyber-physical environments that combine sensing, communication and distributed computing technologies. These ecosystems commonly include wearable monitoring devices used by field responders, autonomous vehicles and drones supporting reconnaissance and logistics missions, smart surveillance systems for real-time situational awareness and environmental monitoring platforms capable of detecting hazardous conditions. At the same time, edge computing infrastructures enable localized data processing and rapid operational decision-making directly near affected areas, reducing dependence on centralized cloud services during critical incidents. The convergence of LTE, IoT, UAVs and edge computing technologies laid the foundation

for the emergence of 5G-enabled public safety ecosystems, which further expanded the capabilities of emergency communication infrastructures.

Legacy narrowband systems were not designed to support such distributed, data-intensive environments efficiently. The evolution toward 5G further transformed the conceptual foundations of public safety networking. Unlike previous generations, 5G was designed not simply as a communication technology but as a programmable, service-oriented and virtualized networking ecosystem. Emerging 5G public safety architectures introduced several capabilities that significantly expanded the operational flexibility of emergency communication systems. These included Ultra-Reliable Low-Latency Communication (URLLC) for time-sensitive applications, network slicing for traffic prioritization and service isolation and Software-Defined Networking (SDN) together with Network Function Virtualization (NFV) for adaptive and programmable network management. In parallel, massive Machine-Type Communications (mMTC) enabled the large-scale integration of IoT devices and distributed sensing infrastructures, while edge intelligence supported localized analytics and faster operational decision-making near the disaster area [\[22\]](#).

These technologies significantly improved the operational adaptability and resilience of emergency communication systems. Network slicing, for example, allows the creation of isolated virtual communication environments optimized specifically for mission-critical operations. During disasters, emergency services may therefore receive prioritized bandwidth allocation and protected communication resources independently from civilian traffic congestion. At the same time, the integration of Multi-Access Edge Computing (MEC) introduced distributed intelligence capabilities directly within communication infrastructures. Instead of relying exclusively on centralized cloud processing, operational data can now be analyzed near the network edge, reducing latency and improving autonomous decision-making under degraded network conditions [\[17\]](#).

The transition toward 6G-oriented public safety ecosystems extends this evolution even further. Current research trends emphasize AI-native networking, ISAC, semantic communications, digital twins, autonomous orchestration and intelligent cyber-physical coordination. Rather than functioning as passive transport infrastructures, future public safety networks are expected to evolve into adaptive and self-organizing ecosystems capable of predictive operational awareness and autonomous resilience management [\[25\]](#).

As a result, emergency communication systems now extend far beyond traditional radio infrastructures and are increasingly interpreted as integrated multi-layer ecosystems that combine communication, sensing, computation, orchestration and intelligent decision-support capabilities within highly dynamic disaster response environments. The following sections progressively analyze the technological evolution and architectural convergence that shaped modern emergency communication ecosystems, beginning with the transition toward 5G-enabled mission-critical networking infrastructures [\[13\]](#), [\[29\]](#).

2.1 5G Architecture and Mission-Critical Networking

The evolution from fourth-generation mobile communication systems toward fifth-generation networking infrastructures represents a major transition in public safety and emergency communication systems [\[4\]](#), [\[17\]](#). Unlike previous mobile generations, which primarily focused on improving throughput and connectivity, 5G introduces a service-oriented networking approach centered around virtualization, programmability, intelligent orchestration and service-oriented communication architectures. The increasing operational complexity of modern emergency response environments requires communication systems capable of supporting heterogeneous mission-critical applications, ultra-low latency services, massive sensing infrastructures and dynamic interoperability among multiple agencies and operational entities [\[30\]](#).

The emergence of 5G technologies is closely associated with the broader transformation of communication networks into highly adaptive digital ecosystems capable of integrating communication, computation, sensing and intelligent control mechanisms within unified operational environments. In contrast to legacy narrowband systems and early LTE infrastructures, 5G networks introduce service-based and software-centric architectures designed to support autonomous management, distributed intelligence and real-time orchestration under highly dynamic operational conditions [\[31\]](#).

This architectural shift is particularly important for PPDR operations, where communication systems must maintain reliability, interoperability, scalability and service continuity even during severe infrastructure degradation or large-scale disasters. In this context, 5G introduces a more flexible communication framework that can accommodate heterogeneous operational requirements and support diverse mission-critical services within a common network infrastructure. The architectural design of 5G is primarily structured around three complementary service categories. Enhanced Mobile Broadband (eMBB) focuses on high-

throughput communication services and bandwidth-intensive applications, while Ultra-Reliable Low-Latency Communications (URLLC) supports time-sensitive, mission-critical operations that require minimal delay and high reliability. In parallel, mMTC enables large-scale connectivity among IoT devices, sensors and distributed cyber-physical infrastructures operating simultaneously within complex communication environments. Collectively, these service categories allow 5G infrastructures to accommodate communication requirements ranging from high-bandwidth multimedia transmission to latency-sensitive control and massive sensor connectivity. Such capabilities are particularly relevant to PPDR scenarios, supporting applications such as real-time video transmission, UAV-assisted coordination, distributed sensing, remote monitoring and AI-driven situational awareness [\[30\]](#).

Beyond improvements in radio access and connectivity, the transition toward software-defined and virtualized communication infrastructures represents another important architectural evolution. Technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV) introduce programmable control mechanisms that reduce dependence on dedicated hardware and enable network functions and resources to be managed more dynamically. This programmability allows communication infrastructures to adapt their configuration according to changing operational conditions, traffic demand and service priorities. During emergency situations, network resources may therefore be dynamically reallocated to prioritize mission-critical traffic, maintain connectivity in affected areas and support rapid deployment or reconfiguration of communication services. Furthermore, the combination of virtualization and centralized network management provides a foundation for more resilient and adaptive communication architectures capable of responding to failures or sudden variations in network demand [\[13\]](#), [\[22\]](#). The high-level architecture of 5G-enabled mission-critical communication ecosystems is illustrated in Figure 5.

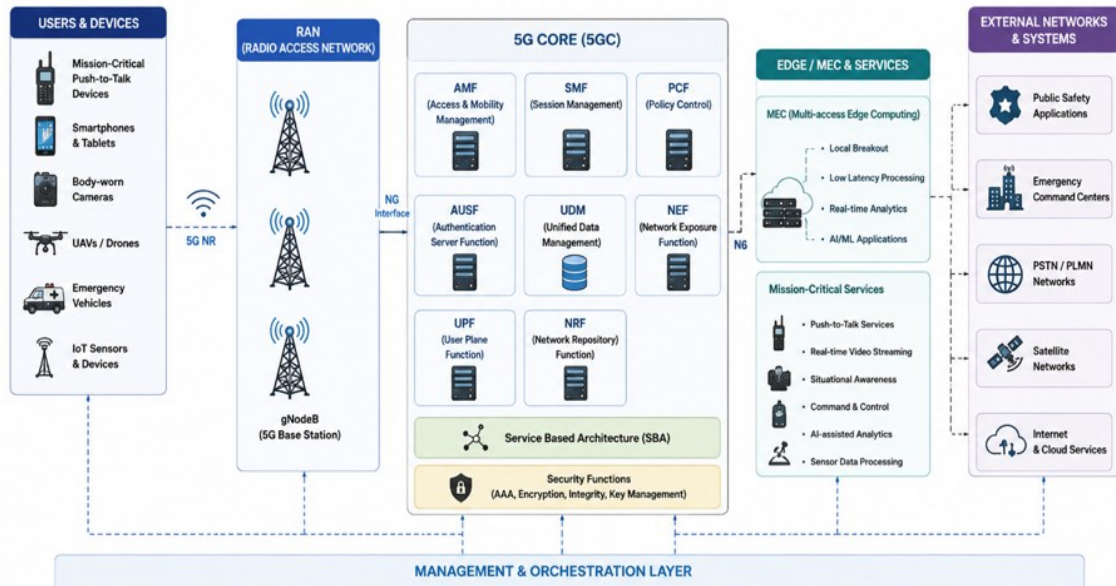


Figure 5 High-Level 5G Network Architecture Supporting Mission-Critical Communications. Source: Author's synthesis based on the reviewed literature [29]–[31].

Unlike conventional communication systems, 5G architectures are increasingly designed around distributed cloud-native infrastructures integrating Radio Access Networks (RAN), edge computing platforms, virtualization layers and intelligent orchestration mechanisms [4], [17]. The 5G Core (5GC) functions as the central management domain responsible for authentication, mobility management, traffic orchestration, service delivery and policy enforcement. Simultaneously, edge computing infrastructures positioned near the network edge support latency-sensitive applications requiring rapid processing and localized decision-making capabilities. This distributed operational model significantly enhances resilience and reduces dependence on centralized cloud infrastructures [32].

An important innovation introduced by 5G is the differentiation of service categories according to specific operational requirements. Enhanced Mobile Broadband (eMBB) supports bandwidth-intensive applications such as real-time video analytics and situational awareness platforms, while URLLC addresses latency-sensitive mission-critical operations and command-and-control services. In parallel, massive Machine-Type Communications (mMTC) enables large-scale connectivity among IoT devices and distributed sensing infrastructures within disaster response environments. Figure 6 presents the primary 5G service categories supporting mission-critical public safety operations.



Figure 6 Core 5G Service Categories Supporting Mission-Critical Public Safety Communications.
Source: Author's synthesis based on the reviewed literature [29]–[32].

The integration of SDN and NFV technologies further transforms public safety networking architectures by enabling programmable and highly adaptive communication infrastructures. Traditionally, communication networks relied on hardware-centric architectures where network functionality was tightly coupled with physical equipment [33]. In contrast, SDN separates the control plane from the data plane, allowing centralized orchestration and dynamic network management [34]. NFV complements this approach by virtualizing network services that traditionally required dedicated hardware appliances. These innovations significantly improve flexibility, scalability, fault tolerance and operational adaptability during emergency situations [35], [36]. Within disaster communication environments, SDN and NFV architectures provide a high degree of flexibility and adaptive network control. These technologies support rapid deployment of communication services, dynamic traffic steering and intelligent bandwidth allocation according to real-time operational demands. In parallel, they improve network recovery capabilities, enable more efficient congestion management and support continuous optimization of distributed communication resources during large-scale emergency operations.

This level of flexibility is particularly important during large-scale incidents when communication infrastructure may experience unpredictable traffic surges, partial failures, or rapidly changing operational conditions. Figure 7 illustrates an SDN/NFV-enabled architecture for adaptive public safety networking.

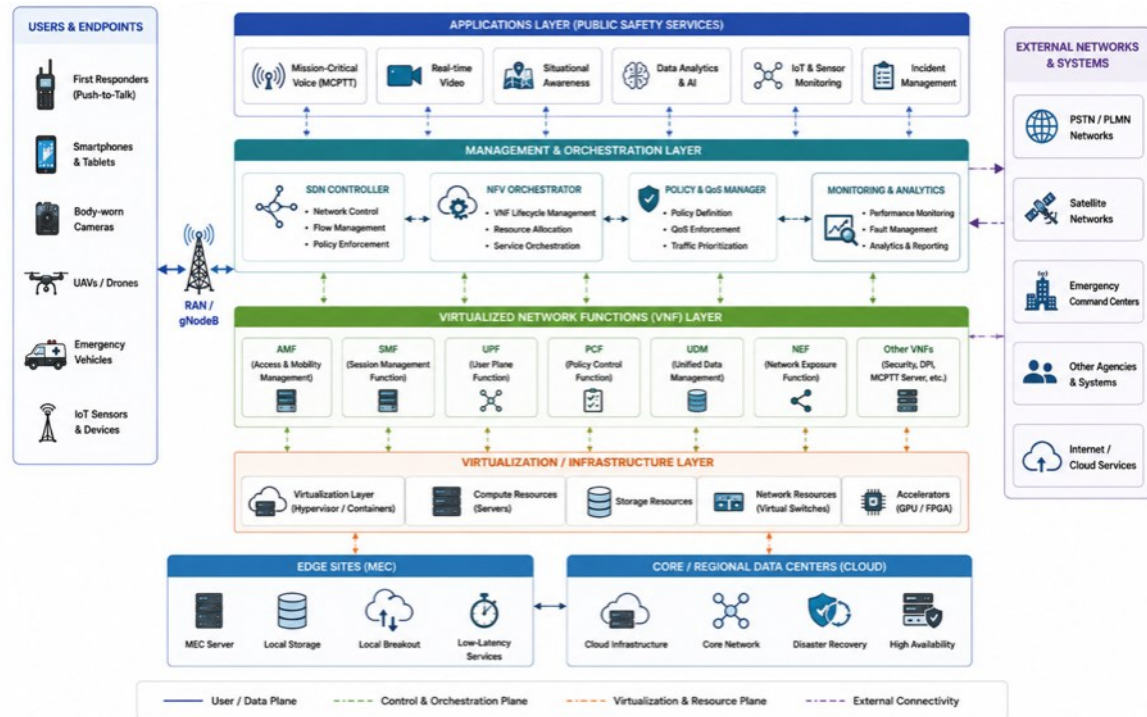


Figure 7 SDN/NFV-Based Adaptive Architecture for Mission-Critical Public Safety Networks. Source: Author's synthesis based on the reviewed literature [29]–[34].

Another transformative capability introduced by 5G communication systems is network slicing. Network slicing enables the creation of multiple logically isolated virtual networks operating over a shared physical infrastructure. Each network slice can be independently configured according to specific QoS requirements and operational priorities [32]. These parameters may include communication latency, transmission reliability, bandwidth availability, security policies and traffic prioritization mechanisms tailored to the needs of different emergency-response services and mission-critical applications.

For public safety operations, network slicing enables the allocation of dedicated communication resources exclusively to emergency responders and mission-critical applications. This ensures that critical communications remain operational even under severe congestion conditions caused by civilian traffic overload or infrastructure disruption. Figure 8 illustrates the role of network slicing in supporting prioritized PPDR communication services.

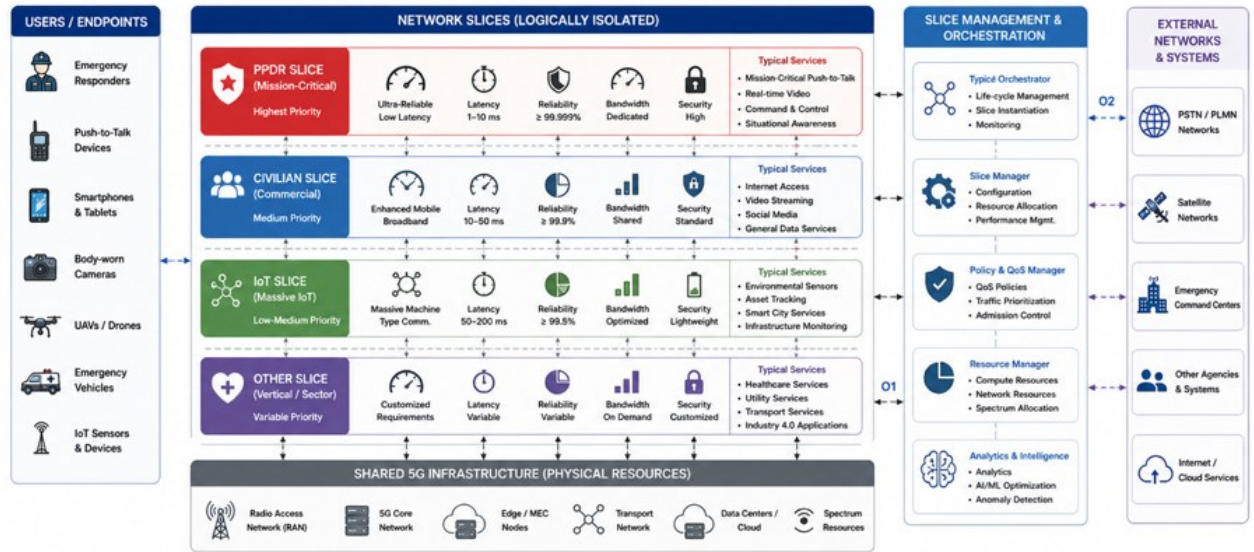


Figure 8 5G Network Slicing Architecture Supporting Differentiated QoS and Resource Isolation for Mission-Critical PPDR Communications. Source: Author's synthesis based on the reviewed literature [29]–[34].

The integration of 5G technologies within public safety ecosystems extends beyond traditional communication services and increasingly supports intelligent cyber-physical coordination environments. Modern emergency communication ecosystems combine several interconnected technological domains. UAV platforms may support aerial surveillance and temporary communication coverage, while IoT sensing infrastructures continuously monitor environmental conditions and critical infrastructure status [37]. At the same time, edge computing platforms process operational data locally to reduce latency, whereas satellite links provide communication continuity in areas affected by infrastructure disruption [38], [39]. These systems collectively support command centers, healthcare services and emergency responders through continuous real-time information exchange. These interconnected components collectively form highly adaptive mission-critical ecosystems capable of supporting distributed situational awareness, predictive analytics, intelligent orchestration and autonomous coordination under dynamic disaster response conditions. Across the related literature, 5G technologies are expected to play a central role in enabling future emergency communication infrastructures characterized by interoperability, resilience, scalability and intelligent operational management. Figure 9 illustrates an integrated 5G-enabled mission-critical public safety ecosystem.

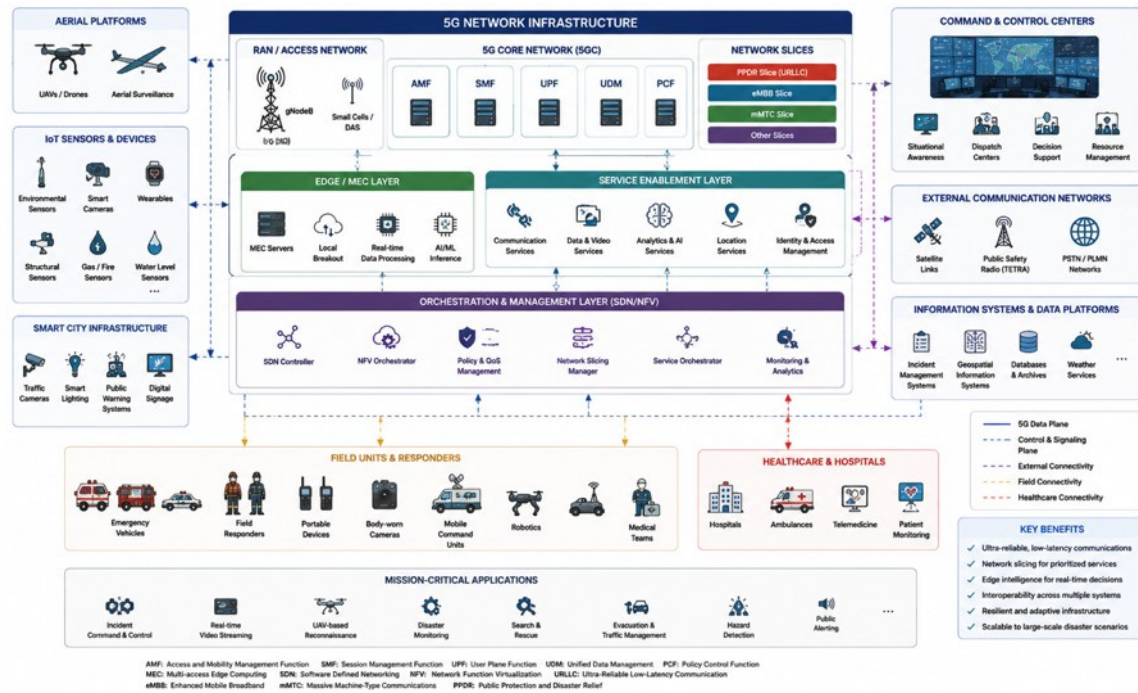


Figure 9 End-to-End 5G-Enabled Mission-Critical Public Safety Ecosystem Integrating Network Slicing, Edge Computing, AI-Native Services, SDN/NFV Orchestration and Heterogeneous Communication Infrastructures for Resilient Disaster Response. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[34].

Therefore, 5G extends beyond a conventional improvement in mobile communications and represents a systemic transformation toward intelligent, programmable, distributed and highly resilient communication ecosystems specifically designed to support the operational complexity of modern public safety and disaster response environments [29].

2.2 MEC, Edge Intelligence and AI-Native Networking

Modern emergency communication systems rely heavily on the integration of distributed computing, intelligent orchestration and low-latency networking infrastructures. Traditional cloud-centric architectures introduce significant limitations for mission-critical environments due to communication delays, centralized processing bottlenecks and dependence on stable backhaul connectivity. As disaster response operations require real-time situational awareness, autonomous coordination and rapid decision-making, the need for distributed edge-oriented computing paradigms has become increasingly important [13]. Across the related literature, edge computing and Industrial IoT ecosystems are designed to support scalable, resilient and latency-sensitive applications operating within highly dynamic cyber-physical environments. MEC represents a major architectural transition from centralized cloud processing toward localized distributed intelligence positioned at the

network edge. Instead of transmitting all operational data toward distant cloud infrastructures, MEC allows computational tasks to be processed closer to end devices, significantly reducing latency and improving operational responsiveness. This capability becomes particularly valuable in emergency communication environments that require continuous coordination among multiple distributed systems. Representative applications include UAV-assisted operations, autonomous emergency vehicles, IoT-based sensing infrastructures and real-time video analytics platforms used for situational awareness and tactical decision support during disaster response activities [19].

The integration of edge computing infrastructures within 5G ecosystems enables communication and computation to operate as tightly coupled operational domains. According to the reviewed literature, edge computing complements wireless communication by supporting scalable orchestration, localized analytics and distributed resource management across Industrial IoT environments. Figure 10 illustrates the operational workflow of a MEC-enabled emergency communication architecture.

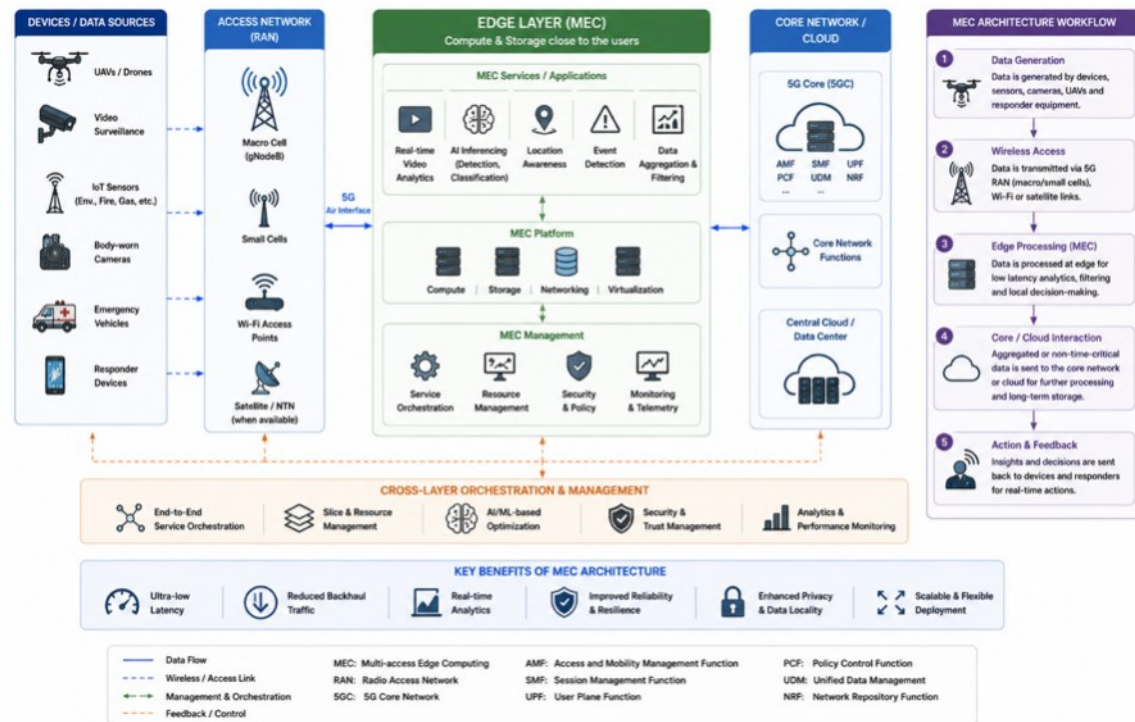


Figure 10 MEC Architecture Workflow for Mission-Critical Emergency Communications. Source: Author's synthesis based on references [29]–[35].

Within MEC architecture, data generated by field devices and distributed sensing infrastructures can be processed locally at edge nodes before transmission to centralized cloud systems. This localized processing approach reduces communication delays while

also limiting core network congestion and unnecessary bandwidth consumption. In mission-critical public safety environments, these capabilities support faster threat detection, localized AI inference, intelligent traffic prioritization and rapid situational assessment directly near the disaster area. At the same time, distributed processing across multiple edge nodes improves operational continuity and enhances overall system resilience during infrastructure-disrupted conditions. For example, UAV video streams used during disaster response operations may be processed directly at nearby MEC servers for object recognition, victim detection and hazard assessment without requiring transmission toward remote cloud infrastructures [\[37\]](#).

A key benefit of MEC infrastructure is its ability to support distributed edge intelligence and real-time analytics. Modern emergency communication systems rely on the continuous processing of heterogeneous data generated by multiple distributed sources. These data streams may originate from IoT sensors, wearable monitoring devices, surveillance platforms, environmental sensing systems, autonomous response technologies and broader cyber-physical infrastructures operating within the disaster area. The ability to collect, process and analyze this information in real time significantly improves situational awareness and supports faster operational decision-making during emergency-response activities.

Traditional centralized cloud architectures often fail to satisfy the strict latency and reliability requirements associated with such operational environments. Edge intelligence addresses this limitation by enabling machine learning inference and analytics directly at the network edge. Across the related literature, Industrial IoT ecosystems increasingly rely on distributed AI-enabled infrastructures capable of supporting predictive analytics, anomaly detection, intelligent automation and adaptive orchestration. Figure 11 illustrates the distributed edge intelligence workflow supporting real-time analytics.

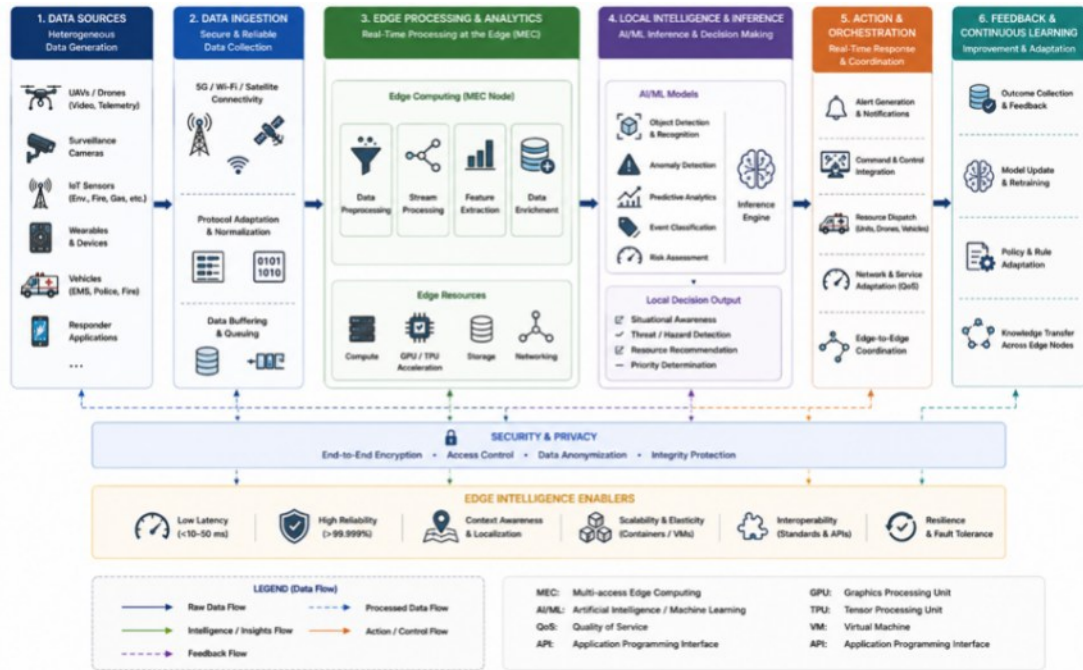


Figure 11 Edge Intelligence Pipeline for Real-Time Analytics and AI-Driven Decision Support in Mission-Critical Emergency Communications. Source: Author's synthesis based on references [29]–[35].

The emergence of AI-native networking further extends the capabilities of edge-enabled communication ecosystems. AI-native networking describes infrastructures in which AI mechanisms support network orchestration, optimization and adaptive resource management. Unlike static rule-based approaches, AI-native architectures continuously analyze network telemetry, traffic patterns and operational context to dynamically optimize network behavior. Within mission-critical environments, AI-driven mechanisms can support predictive resource allocation, intelligent congestion control and dynamic QoS enforcement according to real-time requirements. In parallel, these systems improve fault detection, support self-organizing network behavior and enable more efficient orchestration of distributed communication and computing resources across complex emergency-response infrastructures.

Machine learning algorithms can optimize routing decisions, bandwidth allocation, edge resource utilization and communication prioritization according to real-time operational conditions. Across the literature, machine learning increasingly enables intelligent IoT connectivity and adaptive cyber-physical infrastructures. Figure 12 presents the architecture of AI-native networking and intelligent orchestration.

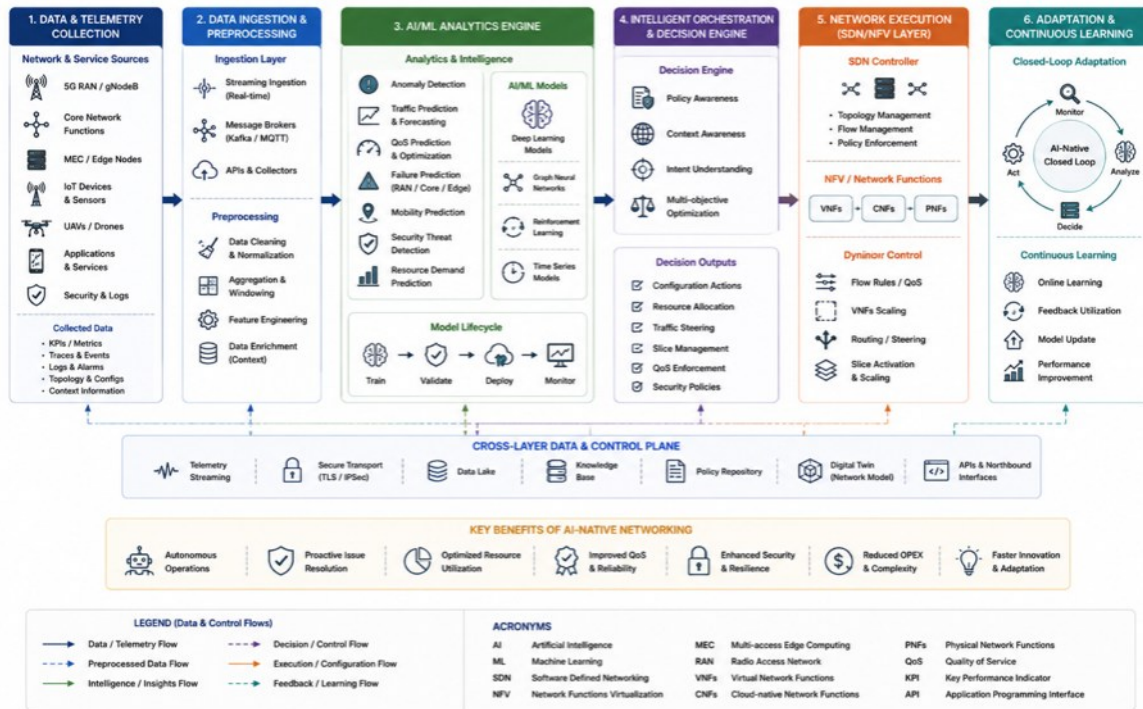


Figure 12 AI-Native Networking Architecture for Autonomous Network Orchestration in Mission-Critical Emergency Communications. Source: Author's synthesis based on the reviewed literature [29]–[35].

The convergence between MEC, distributed AI and 5G communication infrastructures is particularly important for disaster response ecosystems characterized by dynamic operational conditions and intermittent connectivity. During large-scale emergencies, communication infrastructures frequently operate under highly unstable conditions. Networks may experience partial infrastructure failures, severe congestion, degraded backhaul connectivity and rapidly changing traffic demands caused by the movement of responders, civilians and emergency assets across the affected area. These conditions significantly increase the complexity of maintaining reliable communication services, continuous information exchange and coordinated operational responses during disaster management activities [7], [13].

In such environments, localized edge intelligence can significantly improve network resilience by enabling autonomous processing and decision support even when centralized infrastructures become partially unavailable. By placing computing and analytical capabilities closer to operational users and data sources, MEC infrastructures can reduce dependence on continuous cloud connectivity and support faster processing of time-sensitive information. Edge-enabled emergency communication systems may therefore

continue supporting mission-critical services during periods of degraded or intermittent backhaul connectivity, while locally available computing resources can assist in maintaining essential communication and situational awareness functions.

Modern disaster communication ecosystems increasingly integrate MEC infrastructures with UAV systems, IoT platforms, command-and-control centers, healthcare infrastructures and autonomous sensing systems. This integration enables operational data generated by geographically distributed devices to be processed closer to the affected environment, reducing the need to continuously transfer large volumes of information toward centralized cloud infrastructures. UAVs equipped with cameras and environmental sensors may transmit operational data directly to nearby edge servers, where AI-based analytics engines process incoming information in real time. For example, a UAV deployed above a flooded urban area may stream live video feeds to nearby MEC nodes, where AI models identify blocked roads or isolated civilians and provide relevant information to emergency coordination systems [\[21\]](#), [\[37\]](#). Simultaneously, first responders equipped with wearable sensors and mobile communication devices can continuously exchange telemetry and situational awareness information through distributed edge-enabled communication architectures [\[7\]](#), [\[13\]](#), [\[19\]](#). The resulting architecture creates a distributed operational environment in which communication, sensing and computational resources cooperate across the network edge to support emergency coordination. Figure 13 illustrates an integrated MEC-enabled disaster communication ecosystem that supports distributed emergency operations.

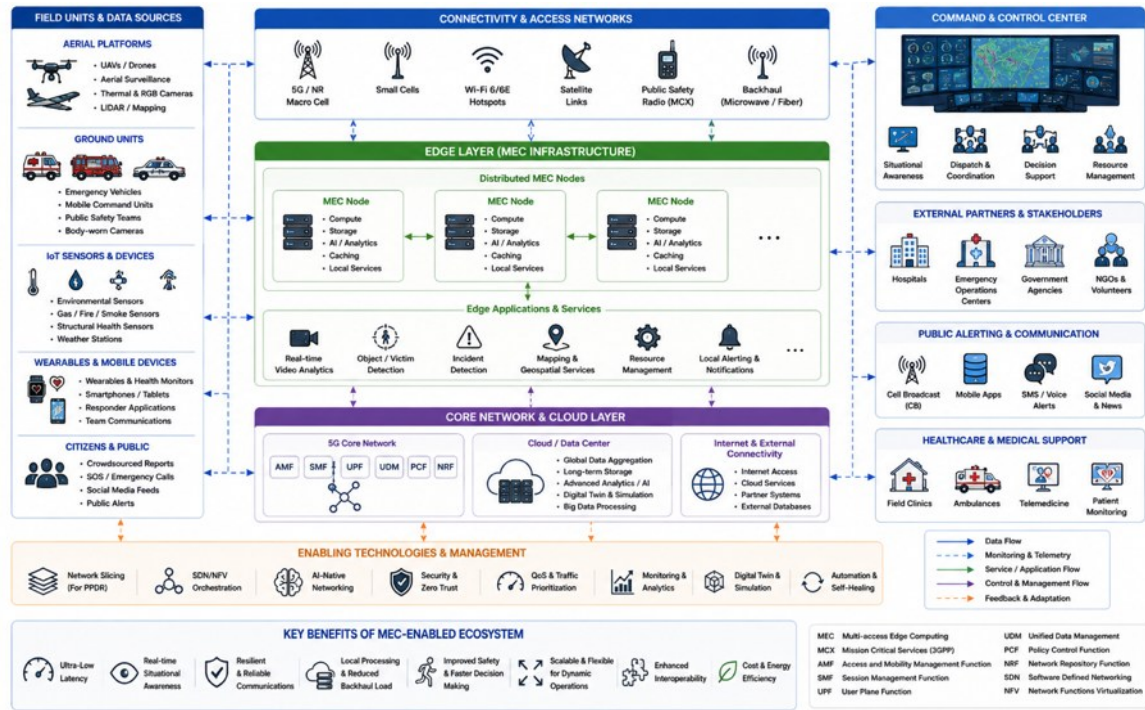


Figure 13 Integrated MEC-Enabled Disaster Communication Ecosystem Supporting AI-Driven Mission-Critical Emergency Response. Source: Author's synthesis based on references [29]–[35].

The operational importance of MEC and edge intelligence is expected to increase significantly in future 6G-oriented emergency communication ecosystems. Emerging communication architectures increasingly focus on intelligent and autonomous operational capabilities designed to improve resilience and adaptive coordination. Current research trends emphasize distributed AI-based orchestration, semantic communication models, autonomous cyber-physical coordination mechanisms and the integration of digital twins within emergency-response environments. At the same time, intelligent sensing infrastructures and self-healing networking mechanisms are expected to enhance system survivability and operational continuity under highly dynamic disaster conditions [24], [25]. As a result, MEC and AI-native networking should not be interpreted simply as complementary technological enhancements to existing communication systems. Instead, they represent foundational architectural paradigms supporting the transition toward intelligent, distributed, adaptive and resilient mission-critical MEC communication ecosystems capable of addressing the operational complexity of future disaster response environments [21].

2.3 NTN/UAV Integration and Non-Terrestrial Emergency Communications

The increasing operational complexity of modern disaster response environments has expanded the requirements imposed on emergency communication systems. Conventional terrestrial infrastructure may become partially unavailable during large-scale disasters due to physical damage and rapidly deteriorating operational conditions. Power outages, network congestion, backhaul failures and environmental disruption can significantly reduce communication availability, particularly in geographically isolated or heavily affected areas. Maintaining reliable connectivity therefore remains a major challenge for emergency communication systems [8]. Modern mission-critical communication ecosystems increasingly incorporate non-terrestrial platforms to extend network coverage, improve resilience and maintain communication continuity under dynamic operational conditions. Public safety systems are consequently evolving toward integrated broadband ecosystems that combine terrestrial, airborne and satellite communication infrastructures within unified operational architectures [38], [40].

NTNs integrate satellite systems, aerial platforms, High Altitude Platform Stations and UAVs with conventional terrestrial wireless infrastructures. By extending connectivity beyond ground-based networks, NTNs improve geographical coverage and reduce dependence on fixed infrastructure. They also provide communication redundancy, rapid deployment capabilities and greater operational flexibility when conventional networks are damaged or unavailable [23]. These characteristics are particularly important in remote, maritime, mountainous and post-disaster environments. The evolution toward 5G and future 6G ecosystems further accelerates the integration of NTN technologies with terrestrial broadband systems, enabling interoperability across heterogeneous networking domains. Such architectures may combine satellite communications, UAV-based relays, 5G infrastructures, edge computing, IoT sensing and AI-driven orchestration within a unified operational framework. Their coordinated operation can improve communication continuity, distributed situational awareness and adaptive resource management during complex emergency-response operations [39], [41]. A high-level non-terrestrial communication architecture integrating satellites, UAVs and terrestrial emergency communication infrastructures is illustrated in Figure 14.

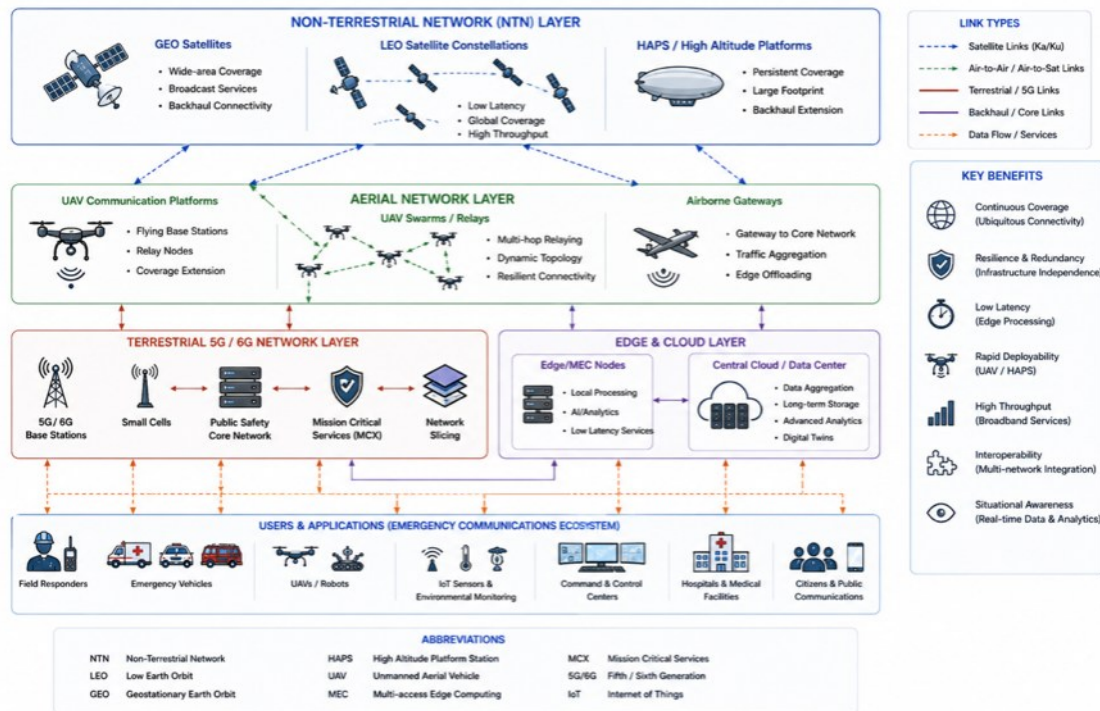


Figure 14 Integrated NTN-Enabled Emergency Communication Ecosystem. Source: Author's synthesis integrating concepts from the reviewed literature [35]–[38].

The role of UAVs within emergency communication ecosystems has expanded significantly during recent years. UAV-assisted communication systems can support multiple operational roles within disaster response environments. Depending on mission requirements, UAV platforms may function as flying base stations, airborne communication relays, temporary network gateways, or aerial sensing systems providing real-time situational awareness. In more advanced deployments, UAVs may also host mobile edge computing capabilities, allowing localized data processing and faster operational coordination directly near the affected area. Unlike fixed terrestrial infrastructure, UAV-based communication systems provide highly flexible and rapidly deployable operational capabilities suitable for disaster response scenarios requiring temporary communication restoration. Across the related literature, satellite and airborne communication systems increasingly function as complementary infrastructures supporting resilient public safety communications [37], [41]. In disaster response operations, UAVs equipped with communication payloads can rapidly establish temporary wireless coverage over affected regions where conventional infrastructure has collapsed. At the same time, UAV-mounted sensors and imaging systems significantly enhance situational awareness during emergency-response operations. These platforms can support real-time aerial surveillance, environmental monitoring, victim

localization, hazard assessment and infrastructure damage evaluation across affected areas. The ability to rapidly collect and transmit operational information from the field allows emergency coordination centers to make faster and more informed decisions under dynamic disaster conditions [\[40\]](#).

These operational capabilities significantly improve situational awareness and support rapid decision-making during emergency coordination activities. A major architectural trend within future emergency communication systems is the development of Space-Air-Ground Integrated Networks (SAGIN). SAGIN architecture combines multiple communication and computing layers within a unified operational framework. These environments integrate satellite communication systems, aerial networking platforms, terrestrial wireless infrastructure, edge and cloud computing resources, as well as distributed sensing ecosystems operating across the disaster area. By coordinating these heterogeneous domains, SAGIN architectures improve communication continuity, coverage flexibility and adaptive resource management during complex emergency-response operations [\[38\]](#). Unlike isolated communication domains, SAGIN enables interoperability and coordinated management across heterogeneous networking layers. This integrated model improves the resilience and flexibility of emergency communication systems under degraded conditions. By coordinating multiple communication layers, SAGIN enhances communication survivability, extends coverage and supports adaptive traffic routing. It also improves operational scalability and helps maintain service continuity during large-scale disaster response operations [\[39\]](#).

The integration of SAGIN with 5G and edge computing enables dynamic orchestration of communication resources according to operational and environmental conditions. AI-driven mechanisms can optimize routing, allocate bandwidth, prioritize mission-critical traffic and coordinate UAV positioning in response to evolving disaster scenarios. AI-assisted management can also improve edge resource utilization and satellite backhaul connectivity across distributed emergency communication infrastructures [\[41\]](#). Consequently, emergency communication infrastructures are evolving toward coordinated multi-layer networking models. Figure 15 presents the architecture of an integrated Space-Air-Ground communication ecosystem.

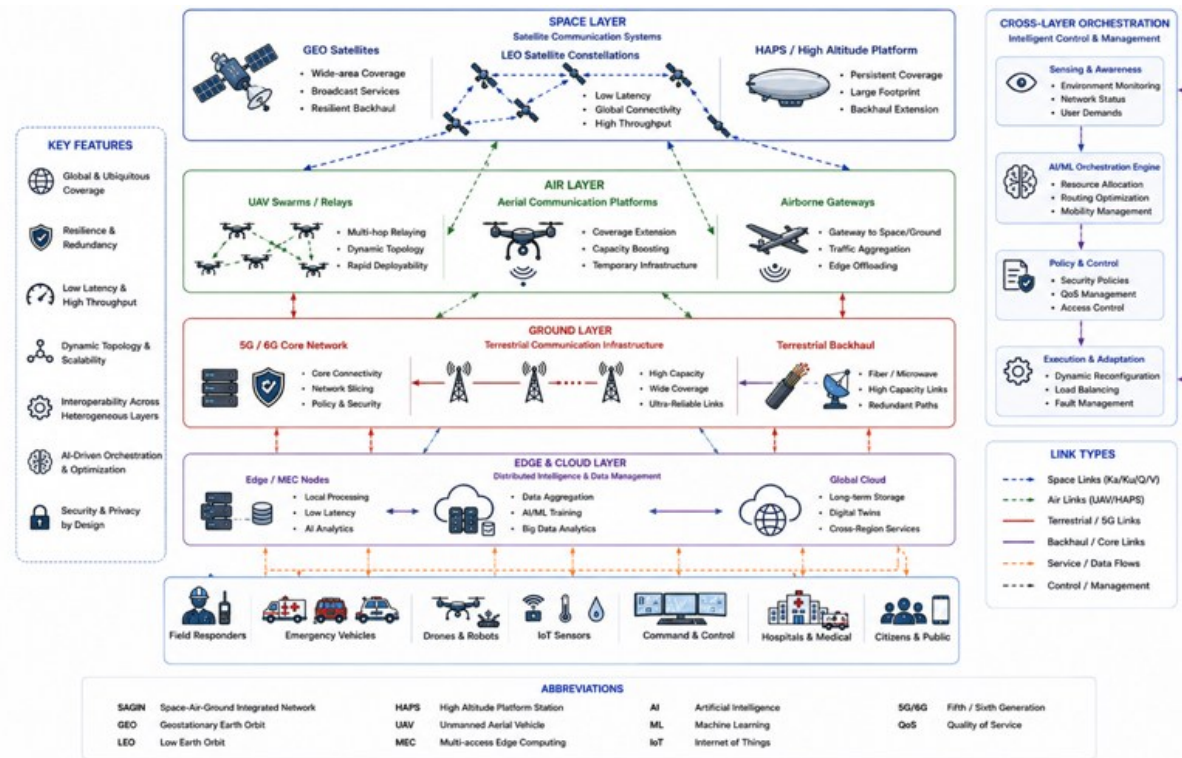


Figure 15 Space-Air-Ground Integrated Network (SAGIN). Source: Author's synthesis integrating NTN, SAGIN, UAV-assisted networking, MEC, 5G/6G mission-critical networking, cloud-edge concepts and the reviewed literature [36]–[44].

The operational importance of NTN infrastructures becomes particularly evident during large-scale disasters where terrestrial communication systems experience severe failures. Satellite communication systems may provide emergency backhaul connectivity when fiber or cellular infrastructures become unavailable. Similarly, UAV relays may restore local connectivity among isolated field responders, emergency vehicles, hospitals and command-and-control centers [37].

Across the related literature, satellite systems continue to play an important role in public safety communication ecosystems due to their infrastructure independence and broad geographical coverage capabilities. In parallel, modern wireless networking technologies increasingly support resilient and distributed communication architectures integrating edge computing, AI-enabled orchestration and IoT sensing infrastructures [13], [41].

The convergence between NTN infrastructures, MEC platforms and AI-native networking significantly enhances disaster response resilience. Localized edge processing deployed on UAV platforms or temporary mobile communication stations enables faster and more autonomous management of operational information directly near the disaster area. These capabilities support real-time analytics, distributed AI inference, low-latency situational

awareness and more efficient traffic management across emergency communication infrastructures. In addition, localized processing improves coordination among distributed response assets by reducing reliance on centralized cloud systems during infrastructure disruptions.

As a result, emergency communication ecosystems become less dependent on centralized cloud infrastructures and more capable of maintaining operational continuity under degraded connectivity conditions. Future sixth-generation emergency communication systems are expected to further expand the role of non-terrestrial networking technologies within disaster response environments. Current research directions focus on AI-native orchestration mechanisms, autonomous UAV swarm coordination, semantic communication models and the integration of sensing and communication functions within unified operational frameworks. In parallel, distributed digital twins and intelligent cyber-physical coordination systems are expected to improve situational awareness, autonomous decision-making and adaptive operational response across highly dynamic emergency scenarios [\[24\]](#), [\[42\]](#).

As a result, NTN/UAV integration should not be interpreted simply as a supplementary enhancement to existing public safety communication systems. Instead, it represents a major architectural shift toward highly resilient, adaptive, intelligent and infrastructure-independent emergency communication ecosystems capable of supporting the operational complexity of future disaster response environments.

2.4 OSI Mapping and Cross-Layer Integration in Emergency Communication

Modern emergency communication systems no longer operate as isolated networking infrastructures based exclusively on traditional layered communication principles. The increasing convergence between 5G, IoT, MEC, UAV systems, AI and non-terrestrial networking technologies has transformed mission-critical communication ecosystems into highly interconnected cyber-physical environments characterized by continuous cross-layer interaction and adaptive orchestration. The evolution of public safety communication systems increasingly depends on interoperability, broadband integration, intelligent coordination and dynamic resource management across heterogeneous communication domains.

The Open Systems Interconnection (OSI) model continues to provide a useful conceptual framework for understanding the operational organization of communication systems. However, modern public safety architectures increasingly blur the strict boundaries between traditional networking layers. In contemporary mission-critical environments, efficient emergency response increasingly depends on the coordinated interaction of multiple communication and computing layers. These ecosystems combine physical communication infrastructures, radio access networks, transport mechanisms, edge computing platforms, AI-assisted orchestration systems and application-level situational awareness services within a unified operational framework. The continuous exchange of information among these components supports faster coordination, adaptive resource management and improved operational awareness during disaster response activities [7], [8]. As a result, emergency communication systems increasingly evolve toward cross-layer architectures where communication, computation, sensing and orchestration continuously exchange operational information in real time.

The physical and data-link layers remain responsible for wireless connectivity, spectrum access, radio transmission and device communication. Within modern public safety ecosystems, these communication layers integrate a wide range of heterogeneous networking technologies. Such infrastructures commonly include 5G radio systems, LTE-based communication platforms, UAV-assisted relays, satellite communication links, IoT connectivity environments and wireless mesh networking architectures. The integration of these technologies improves communication coverage, interoperability and service continuity across complex and infrastructure-disrupted emergency environments [8], [13]. At the network and transport layers, technologies such as SDN, NFV, dynamic routing and traffic prioritization support reliable end-to-end connectivity and QoS enforcement for mission-critical applications. At the application layer, emergency communication systems integrate intelligent services for coordination, situational awareness and operational decision-making. These include AI-driven analytics, emergency coordination platforms, digital twins, autonomous orchestration and predictive decision-support tools processing real-time telemetry and distributed operational data [26]. Figure 16 illustrates the mapping of modern emergency communication technologies across the OSI architecture.

OSI LAYER	LAYER FUNCTION (EMERGENCY COMMUNICATION CONTEXT)	EMERGENCY COMMUNICATION TECHNOLOGIES & ENABLERS MAPPED TO OSI LAYERS							
		5G / LTE NETWORKS	MEC / EDGE COMPUTING	UAV SYSTEMS	NTN (SATELLITE / HAPS)	IoT / SENSORS & DEVICES	AI / ANALYTICS & ORCHESTRATION	SDN / NFV VIRTUALIZATION	
7 APPLICATION LAYER	Application services for mission-critical operations, situational awareness, and decision support	Mission-Critical Apps (MCA) Video Streaming GIS, Mapping	Situational Awareness Dashboards Local Applications	Video Analytics Aerial Monitoring Payload Apps	Emergency Broadcasting Global Services	Environmental Monitoring Asset Tracking	Predictive Analytics Decision Support Resource Mgmt.	Service Orchestration Network Slicing Policy Management	
6 PRESENTATION LAYER	Data representation, encryption, compression, and format translation	QoS Adaptation Header Compression Data Coding	Data Transcoding Encryption Data Reduction	Data Formatting Compression Image Encoding	Adaptive Coding Modulation Encryption	Data Serialization Compression Format Conversion	Data Normalization Feature Extraction Model Encoding	Data Abstraction API Translation Encoding Schemes	
5 SESSION LAYER	Session establishment, management, and coordination between communication endpoints	Session Control Authentication Authorization	Edge Session Mgmt. Context Sync State Handling	Link/Session Establishment Handover Mgmt.	Session Continuity Store-and-Forward Inter-Satellite Links	Device Sessions Keep-Alive Sleep / Wake Mgmt.	Context Awareness Session Prediction Behavior Modeling	Virtual Session Management Service Chains	
4 TRANSPORT LAYER	End-to-end transport, reliability, segmentation, flow and congestion control	TCP / UDP SCoP / QUIC QoS Enforcement	Low-Latency Transport Local Offload	Reliable / Unreliable Transport Multi-hop Support	Delay-Tolerant Transport High-Latency Control	Lightweight Transport (SDP) CoAP / MQTT	Traffic Prioritization Congestion Control Adaptive Flows	Transport Slicing Load Balancing Flow Steering	
3 NETWORK LAYER	Logical addressing, routing, mobility support, and network management	IP Routing (v4/v6) Mobility Mgmt. Network Slicing	Edge Routing Local Breakout Service Discovery	Dynamic Routing Aerial Mesh Topology Control	Global IP Routing Satellite Routing Backhaul Mgmt.	IPv6 / 6LoWPAN Mesh Routing Group Mgmt.	AI-based Routing Policy Optimization Anomaly Detection	SDN Controllers NFV Routing Intent-based Net.	
2 DATA LINK LAYER	Framing, MAC control, error detection/correction, link access management	MAC Scheduling HARQ RLC / PDCP	Virtual Switch LAN/WAN Mgmt. VLAN / QoS	MAC Adaptation Link Reliability Inter-UAV Links	DVB-S2 / RCS Link Adaptation ARQ / FEC	MAC Protocols IEEE 802.15.4 LoRa / NB-IoT	Link Quality Prediction Adaptive Scheduling Spectrum Use	SDN Data Plane Virtual Links Policy Enforcement	
1 PHYSICAL LAYER	Physical transmission of bits over radio, optical, or satellite channels	5G NR / LTE Radio Interface Massive MIMO	Edge Infrastructure Compute Nodes High-Speed Links	RF Links (Air-to-Air Air-to-Ground) Line-of-Sight	Ku/Ka band Satellite Links Optical Links (HAPS)	RF, BLE, LoRa, Wi-Fi, UWB Sensor Interfaces	Spectrum Sensing Interference Mgmt. Signal Prediction	Virtualized Radio Resource Pools Infrastructure Abstr.	

Figure 16 OSI Model Mapping for Emergency Communication Systems. Source: Author's synthesis based on the reviewed literature [36]–[44].

Unlike conventional communication environments where networking layers operate relatively independently, mission-critical public safety ecosystems increasingly require cross-layer coordination. Cross-layer integration enables the dynamic exchange of operational information among communication, computing and application layers to improve system efficiency and adaptability. This coordination can enhance network performance, reliability, latency management, interoperability, traffic handling and resource allocation under changing operational conditions. It also improves resilience during infrastructure failures and large-scale disasters, where communication demands and network conditions may change unpredictably [8], [13].

For example, network-layer congestion information may be used by AI-enabled orchestration systems to dynamically adjust routing, bandwidth allocation and edge resource deployment. Similarly, IoT telemetry may trigger adaptive prioritization mechanisms at lower network layers to ensure reliable transmission of mission-critical information [13], [19], [21]. The interaction between communication layers, orchestration mechanisms and distributed operational services is illustrated in Figure 17.

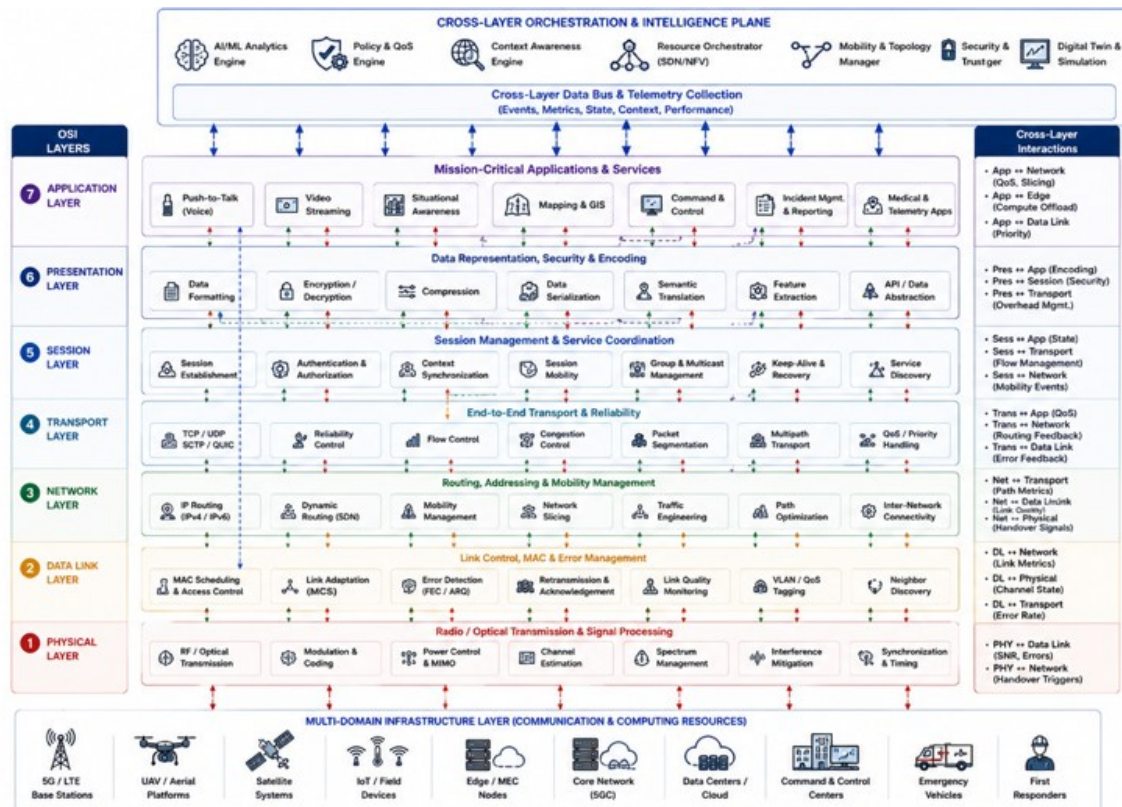


Figure 17 Cross-Layer Emergency Communication Architecture. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44].

The emergence of edge computing and AI-native networking further intensifies the importance of cross-layer integration. MEC infrastructures continuously interact with multiple communication and computing domains within modern emergency-response ecosystems. These interactions involve radio access networks, transport-layer communication systems, distributed IoT environments, UAV-assisted communication platforms and AI-driven orchestration mechanisms operating across the network edge. The coordinated exchange of information among these components supports localized analytics, adaptive resource management and faster operational response under dynamic disaster conditions. This convergence enables communication systems to perform distributed analytics, local AI inference, adaptive orchestration and intelligent traffic management directly at the network edge. Across the related literature, future emergency communication systems increasingly depend on heterogeneous broadband infrastructures integrating multiple operational layers within unified mission-critical ecosystems [29], [38].

The convergence between AI, edge computing, non-terrestrial networking and IoT infrastructures introduces a systemic operational transformation within public safety communication architectures. Instead of functioning as isolated technologies, these

paradigms increasingly operate as interdependent components of integrated cyber-physical ecosystems.

Within these environments, multiple distributed technologies support coordinated emergency-response activities. IoT sensors collect environmental and operational data, while UAV platforms extend coverage and provide real-time aerial situational awareness. Edge computing enables local data processing, allowing AI-based systems to perform predictive analytics, adaptive orchestration and rapid decision support with reduced latency. In parallel, NTN infrastructure provides resilient backhaul connectivity, while command-and-control centers coordinate operations through continuous information exchange across the communication ecosystem [37]. The interaction among these components improves the adaptability and survivability of emergency communication systems under degraded conditions, enhancing communication continuity, autonomous coordination and situational awareness during large-scale disaster response operations. One of the major advantages of cross-layer emergency communication architectures is their ability to support adaptive coordination under highly unstable operational conditions. During large-scale emergencies, communication infrastructures frequently experience partial failures, severe congestion, intermittent connectivity and rapidly changing traffic demands caused by the movement of responders and affected populations. Conventional communication architectures may struggle under such conditions because networking decisions often remain isolated within individual communication layers. Cross-layer approaches address this limitation by enabling continuous operational awareness and coordinated decision-making across the entire communication stack [29].

For example, AI-driven orchestration systems may dynamically prioritize emergency traffic according to real-time situational analysis while simultaneously coordinating UAV deployment, edge resource allocation, satellite backhaul utilization, network slicing policies and QoS enforcement mechanisms. This coordinated management approach improves operational flexibility and helps maintain reliable communication services during complex disaster response scenarios [22]. As a result, emergency communication ecosystems become significantly more resilient and operationally adaptive. A cross-layer disaster response workflow integrating sensing, orchestration, edge computing, UAV coordination and emergency response management is illustrated in Figure 18.

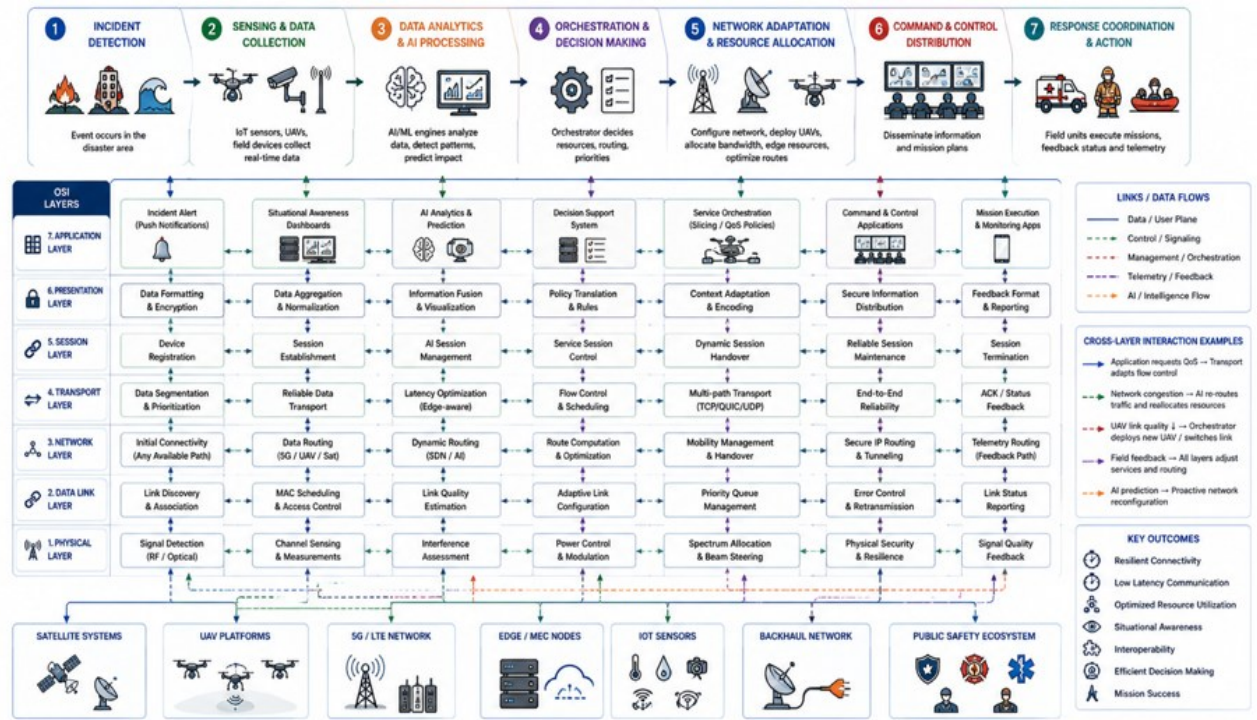


Figure 18 Cross-Layer Operational Workflow Supporting Mission-Critical Emergency Communications. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44].

The transition toward a cross-layer integrated architecture represents a major evolution in modern public safety communication systems. Future sixth-generation emergency communication ecosystems are expected to strengthen this convergence through technologies such as AI-native orchestration, semantic communication models, integrated sensing and communication capabilities, autonomous cyber-physical coordination, distributed digital twins and self-healing networking infrastructures [21], [24], [26].

As emergency communication environments become more complex and data-intensive, cross-layer integration is expected to play a central role in maintaining coordination, resilience and operational continuity across heterogeneous infrastructures. Rather than functioning solely as a mechanism for improving communication efficiency, cross-layer architectures increasingly provide the structural foundation for intelligent and interoperable mission-critical ecosystems capable of supporting the operational requirements of future disaster response scenarios [13], [25], [29].

2.5 Disaster Communication and Operational Requirements

Modern disaster environments are characterized by rapidly changing operational conditions, damaged infrastructures and the simultaneous involvement of multiple emergency-response actors. Unlike conventional communication scenarios, disaster response operations require resilient communication systems that can maintain operational continuity under highly unstable conditions. Communication infrastructures may be affected by partial network failures, severe congestion, intermittent connectivity, environmental disruption, cyber threats, physical destruction and unpredictable mobility patterns associated with the movement of responders and affected populations. These challenges significantly increase the complexity of maintaining reliable coordination and situational awareness during large-scale emergency operations [\[15\]](#).

According to the United Nations Office for Disaster Risk Reduction (UNDRR), disaster risk environments increasingly involve interconnected natural, technological, environmental and societal hazards operating within complex multi-hazard ecosystems. Furthermore, the increasing frequency of Natural Hazard Triggering Technological Disasters incidents demonstrates that natural disasters may directly trigger technological failures, industrial accidents and cascading infrastructure disruptions [\[43\]](#), [\[44\]](#).

As a result, the modern emergency communication systems can no longer be designed as isolated telecommunications infrastructures. Instead, modern emergency communication systems increasingly function as integrated disaster-management ecosystems that support a wide range of operational activities across the emergency-response cycle. These environments facilitate emergency coordination, situational awareness, healthcare communication, public safety operations and critical infrastructure monitoring, while also improving interoperability among multiple responding agencies. In more advanced deployments, intelligent orchestration mechanisms further support autonomous coordination and adaptive operational management under rapidly changing disaster conditions [\[5\]](#), [\[13\]](#).

The complexity of modern disaster communication operational environments involving heterogeneous actors, disrupted infrastructures and multi-domain coordination is illustrated in Figure 19.

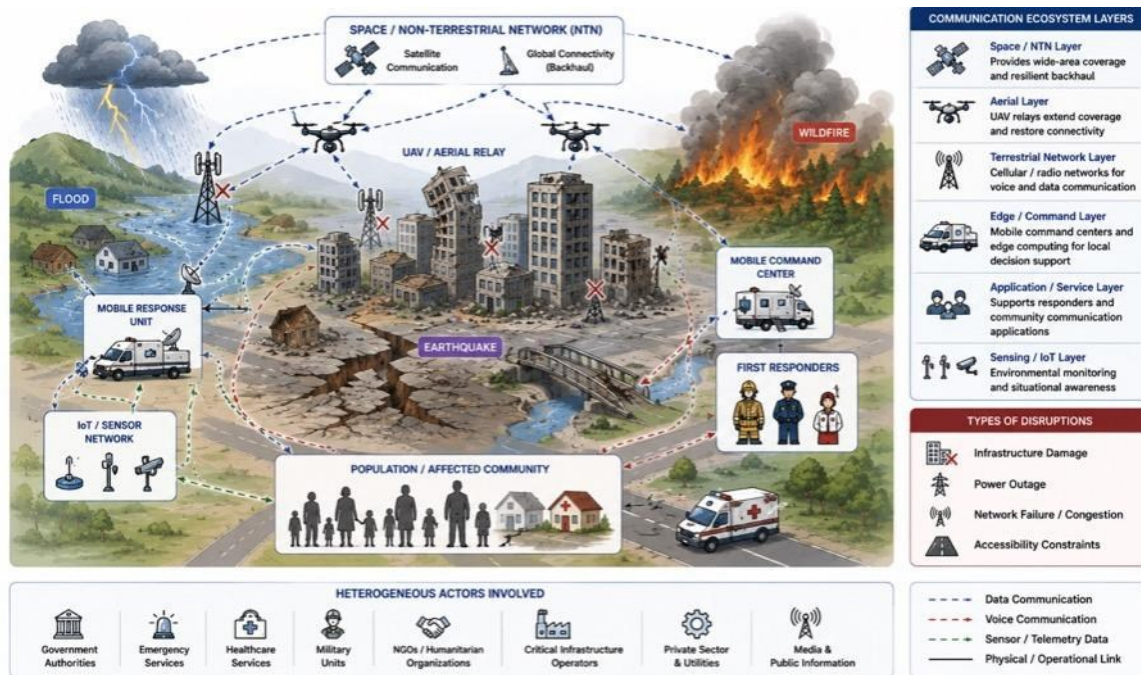


Figure 19 Operational Environment of Mission-Critical Disaster Communication Systems. Source: Author's synthesis integrating concepts from the reviewed literature [29]–[44].

Large-scale disasters often produce cascading effects across multiple critical infrastructures simultaneously, significantly increasing the complexity of emergency-response operations. Disruption in one infrastructure domain may rapidly affect others, creating interconnected failures that complicate communication, coordination and resource deployment. For instance, earthquakes may damage communication towers and power grids, floods can isolate transportation and healthcare infrastructure, and industrial accidents may trigger toxic releases requiring large-scale evacuations. In parallel, cyberattacks may disrupt emergency coordination systems, while wildfires can overload communication networks and emergency-response services across extensive geographical areas [3], [15].

The UNDRR Hazard Information Profiles classify such events within interconnected hazard ecosystems involving technological, environmental, chemical, biological and societal dimensions. This multi-hazard perspective emphasizes the interdependencies among critical infrastructures and the possibility that localized disruptions may propagate across multiple operational domains. Consequently, emergency communication systems must remain functional even when portions of the supporting infrastructure become degraded, congested or temporarily unavailable. This multi-hazard operational environment highlights the growing importance of resilient and interoperable communication architectures capable of maintaining coordination and information exchange under degraded conditions [8], [13].

As a result, mission-critical communication systems must support a combination of survivability, reliability, scalability, and low-latency communication capabilities, while also enabling infrastructure redundancy, autonomous coordination, and intelligent resource orchestration across distributed emergency-response infrastructures. These requirements become particularly important in disaster scenarios, where network conditions may change rapidly, communication resources can become severely constrained, and parts of the underlying infrastructure may become damaged or completely unavailable. Under such conditions, communication systems must maintain essential connectivity while dynamically adapting to changes in network topology, traffic demand, resource availability, and operational priorities. This adaptability is fundamental for supporting the continuous exchange of critical information among emergency responders, coordination centers, autonomous platforms, and distributed sensing systems.

Traditional communication infrastructures frequently fail to satisfy these requirements because they depend heavily on centralized architectures and fixed terrestrial infrastructures, which may represent critical points of failure during large-scale emergencies. Damage to base stations, backhaul links, power infrastructure, or centralized processing facilities can significantly reduce network coverage and disrupt communication services precisely when they are most needed. Furthermore, conventional architectures may provide limited flexibility for rapidly reallocating communication and computational resources according to evolving emergency conditions.

Modern emergency communication ecosystems increasingly address these limitations through the integration of advanced networking, computing, and sensing technologies within unified operational environments. These architectures commonly combine 5G broadband infrastructures, MEC platforms, AI-assisted orchestration mechanisms, UAV-based communication systems, NTN connectivity, and IoT sensing environments. Rather than operating as isolated technological components, these technologies can form complementary communication and computing layers that enhance the flexibility and resilience of the overall emergency-response architecture. UAVs and NTN systems can extend or temporarily restore connectivity in areas where terrestrial infrastructure is unavailable, while MEC platforms can provide computational capabilities closer to affected areas and operational users.

At the same time, AI-assisted orchestration mechanisms can support more adaptive coordination of heterogeneous network resources and services across dynamically changing environments. The integration of IoT sensing infrastructures further strengthens situational awareness by enabling distributed collection of environmental and operational information from affected areas. In parallel, cloud-edge coordination mechanisms facilitate distributed processing, adaptive resource management, and service continuity across geographically dispersed emergency-response infrastructures [38]. This combination of communication, computation, sensing, and intelligent orchestration reflects a broader transition from static and infrastructure-dependent communication networks toward adaptive, distributed, and resilient emergency communication ecosystems.

Collectively, these capabilities can improve the ability of mission-critical communication systems to maintain essential services under dynamic, resource-constrained, and infrastructure-disrupted conditions. They also provide the architectural flexibility required to coordinate heterogeneous technologies and resources according to changing operational demands throughout different stages of emergency response. Figure 20 illustrates the primary operational requirements of mission-critical emergency communication systems.



Figure 20 Mission-Critical Operational Requirements for Emergency Communication Systems.
Source: Author's synthesis integrating mission-critical communication requirements from the reviewed literature [29]–[44].

One of the defining operational characteristics of disaster response environments is the need for continuous coordination among multiple heterogeneous stakeholders. Large-scale emergency operations often involve public safety agencies, firefighting units, healthcare services, military organizations, transportation authorities, humanitarian actors, critical infrastructure operators and governmental coordination centers operating simultaneously within the affected area. These stakeholders may rely on different communication technologies, operational procedures and information systems, making interoperability a fundamental requirement for effective multi-agency coordination. The ability to exchange information efficiently and maintain reliable communication across organizational and technological boundaries is therefore essential for coordinated decision-making, resource allocation and effective emergency response under rapidly changing conditions [8], [13]. This coordination becomes particularly critical when infrastructure damage, network congestion or rapidly evolving hazards require resources and operational priorities to be continuously reassessed.

As a result, modern disaster communication ecosystems are gradually evolving toward integrated cyber-physical environments in which communication, sensing, computation and orchestration mechanisms interact continuously in real time. Rather than operating as isolated technological components, these systems form interconnected operational environments capable of collecting, processing and distributing information across multiple agencies and geographical locations. Within these settings, IoT sensors monitor environmental conditions, infrastructure status and evolving hazards, while UAV systems provide temporary communication coverage and aerial situational awareness across affected areas [37]. The continuous exchange of information between sensing platforms and communication infrastructures provides emergency responders with a more comprehensive representation of conditions within the disaster zone.

At the same time, MEC platforms provide localized analytics and edge intelligence, while AI-driven systems support predictive orchestration and adaptive optimization. Non-terrestrial networks enhance resilience through alternative backhaul connectivity under degraded conditions. In parallel, command-and-control centers coordinate emergency operations, while healthcare systems exchange real-time medical and operational information. An integrated disaster communication ecosystem combining 5G, MEC, AI, IoT, UAV, NTN and emergency coordination infrastructures is illustrated in Figure 21.

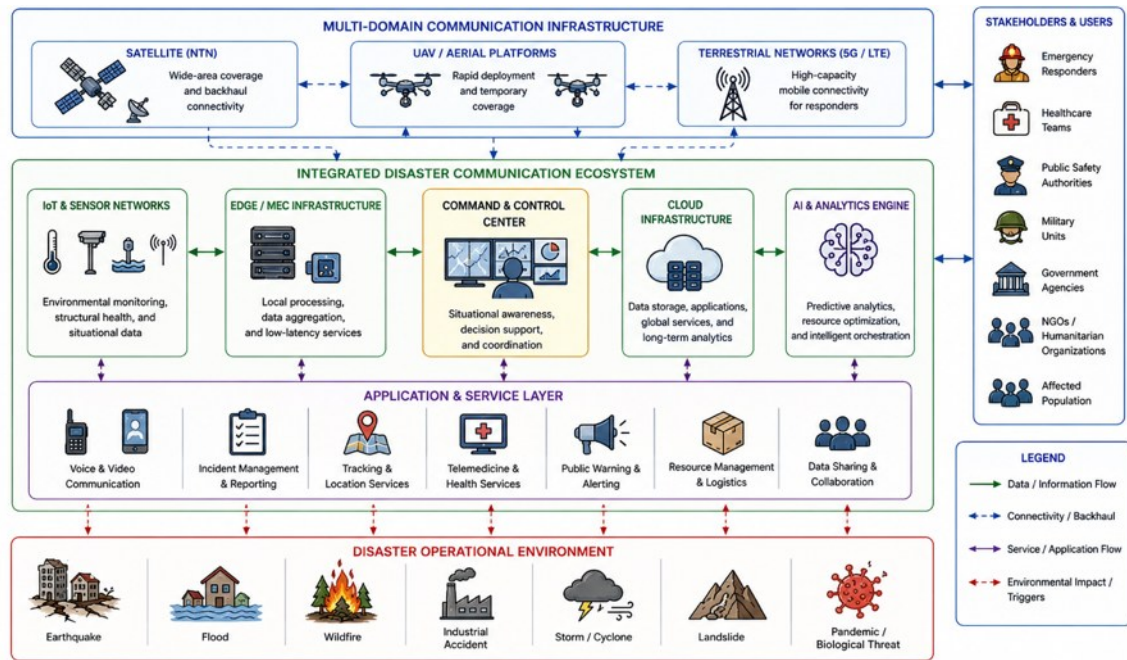


Figure 21 Integrated Disaster Communication Ecosystem. Source: Author's synthesis integrating terrestrial, aerial, NTN, edge/MEC, cloud, AI-native networking, IoT, and mission-critical communication concepts from the reviewed literature [29]–[44].

The convergence between communication infrastructures and intelligent orchestration mechanisms significantly improves operational resilience during degraded or infrastructure-denied environments. AI-native emergency communication ecosystems can dynamically adapt network behavior according to real-time operational conditions and evolving disaster response requirements. AI-driven orchestration mechanisms may prioritize mission-critical traffic, optimize routing decisions, allocate edge computing resources and coordinate UAV deployment across affected areas. In parallel, these systems can manage network slicing policies, predict congestion conditions before service degradation occurs and support more autonomous coordination among distributed emergency-response infrastructures [21], [29]. Similarly, edge computing infrastructures significantly reduce communication latency by enabling local processing of operational information directly near the disaster area. This capability is particularly important for time-sensitive applications such as autonomous vehicles, emergency robotics, telemedicine systems, real-time video analytics, hazard detection platforms and distributed situational awareness services. By processing data closer to the point of collection, edge computing systems support faster operational response and reduce dependence on centralized cloud infrastructures during critical emergency situations.

The integration of non-terrestrial communication infrastructures further improves communication survivability by reducing dependence on damaged or unavailable terrestrial networks. In disaster environments where conventional infrastructures may become partially inoperative, UAV relays and satellite communication systems can help maintain operational continuity and extend communication coverage across affected areas [\[37\]](#), [\[38\]](#). Future emergency communication ecosystems are expected to strengthen this technological convergence even further through the adoption of semantic communication models, integrated sensing and communication capabilities, distributed digital twins, autonomous UAV swarms and intelligent cyber-physical coordination mechanisms. In parallel, self-healing networking infrastructures and AI-driven disaster prediction systems are expected to improve adaptive response capabilities, operational resilience and proactive emergency management across highly dynamic disaster scenarios. As a result, modern emergency communication systems should no longer be interpreted simply as networking infrastructures responsible for data transmission. Instead, they increasingly function as intelligent operational ecosystems enabling resilient coordination, distributed situational awareness, adaptive orchestration and autonomous decision support across highly dynamic disaster response environments [\[24\]](#), [\[26\]](#).

The evolution toward integrated disaster communication ecosystems, therefore, represents a foundational transformation in the design philosophy of future mission-critical communication systems. This transformation combines networking, computation, sensing, AI and operational coordination within unified resilient architectures capable of addressing the increasing complexity of modern disaster response operations [\[21\]](#), [\[29\]](#).

3. Research Methodology and Analytical Framework

This chapter presents the methodological framework used for the identification, classification and critical assessment of recent research on communication technologies for man-made disasters, with particular emphasis on 5G and emerging 6G systems. The proposed methodology aims to establish a coherent analytical foundation that supports systematic literature synthesis, cross-comparison between heterogeneous studies and evidence-driven conclusions aligned with the research questions of the thesis.

3.1 Data Sources and Search Strategy

The literature review was conducted using five major scientific databases: ACM Digital Library, IEEE Xplore, ScienceDirect, Scopus and Web of Science. These databases were selected to ensure broad coverage of peer-reviewed research across computer science, telecommunications and interdisciplinary public safety domains. Their combined use also allowed the study to capture both technical and application-oriented perspectives on disaster communication systems in a systematic and balanced manner.

The temporal scope of the review was limited to research papers published between 2019 and March 2026 to capture developments associated with mature 5G deployments and emerging research directions toward 6G [29]. This period was selected to align the review with contemporary network architectures, ongoing standardization activities and evolving paradigms in mission-critical and public safety communications.

A structured keyword-based search strategy was applied during the title and abstract screening stages using Boolean operators (**AND**, **OR**) to construct controlled and traceable query combinations. The initial search phase focused on the intersection between man-made disasters and next-generation communication technologies using the primary query combinations “man-made disasters” AND “5G” and “man-made disasters” AND “6G” across all five databases. This stage aimed to establish a baseline corpus of studies examining the role of advanced mobile networks in technologically induced or human-driven crisis scenarios.

In a second-stage refinement process, the initially broad category of man-made disasters was divided into analytically distinct and operationally meaningful sub-domains in order to improve thematic precision, reduce semantic over-extension and increase the consistency of the literature retrieval process. More specifically, the original category was separated into

four hazard classes: industrial, nuclear, technological and transportation-related disasters. This stratification was introduced because the generic term “man-made disasters” encompasses a wide range of heterogeneous events that differ substantially in their causes, operational characteristics, infrastructure dependencies and communication requirements. Treating man-made disasters as a single aggregated category may therefore introduce conceptual dilution and retrieval noise, particularly because terminology and indexing practices vary across scientific databases and disciplinary fields. Relevant publications may not explicitly use the general term “man-made disaster”, even when they investigate specific events such as industrial accidents, nuclear emergencies, technological failures or transportation incidents. Consequently, relying on the aggregated category alone could exclude relevant studies indexed primarily by their specific hazard domain. By isolating domain-specific hazard typologies, the second-stage strategy was designed to improve thematic consistency while simultaneously accounting for disciplinary variations in terminology and publication indexing.

This refinement provided a more structured approach for examining the relationship between specific hazard categories and emerging communication technologies. Rather than treating anthropogenic hazards as uniformly represented in the literature, each sub-domain was examined independently and subsequently integrated into a broader Boolean expression. This preserved the conceptual scope of man-made disasters while increasing the granularity of the retrieval process.

Each sub-domain was then combined with the technology-related terms “5G” and “6G” using standardized Boolean operators. The same query structure was applied across the selected databases, with minor syntactic adjustments where necessary. This maintained consistent search logic and enabled comparison of retrieval results across databases. The structured queries were formulated as follows:

- **("industrial" AND ("5G" OR "6G"))**
- **("nuclear" AND ("5G" OR "6G"))**
- **("technological" AND ("5G" OR "6G"))**
- **("transportation" AND ("5G" OR "6G"))**
- **((("industrial" OR "nuclear" OR "technological" OR "transportation") AND ("5G" OR "6G"))**

The first four queries were designed to examine each hazard class independently, thereby allowing domain-specific literature patterns to be identified without interference from the broader man-made disaster terminology. The final combined query served as an integrative search expression, capturing publications associated with at least one of the four hazard categories while maintaining an explicit connection with 5G or 6G communication technologies. This configuration reflects a deliberate balance between **recall and precision** within the literature retrieval process: **The OR operator increased recall** by capturing publications associated with alternative but conceptually related hazard domains and with either 5G or 6G technologies. **The AND operator increased precision** by requiring the contextual co-occurrence of the selected disaster typologies and next-generation communication technologies.

Through this two-stage procedure, the search strategy progressed from broad conceptual exploration to a more granular and domain-sensitive framework. Initial queries using “man-made disasters” provided broad coverage, while subsequent hazard-class stratification improved thematic precision and reduced reliance on a single umbrella term. This refinement strengthened the alignment between the review’s conceptual scope and the terminology used to retrieve relevant literature. The overall procedure is summarized in the two-stage search strategy visualization, illustrating the progression from baseline 5G/6G queries to hazard-specific stratification.

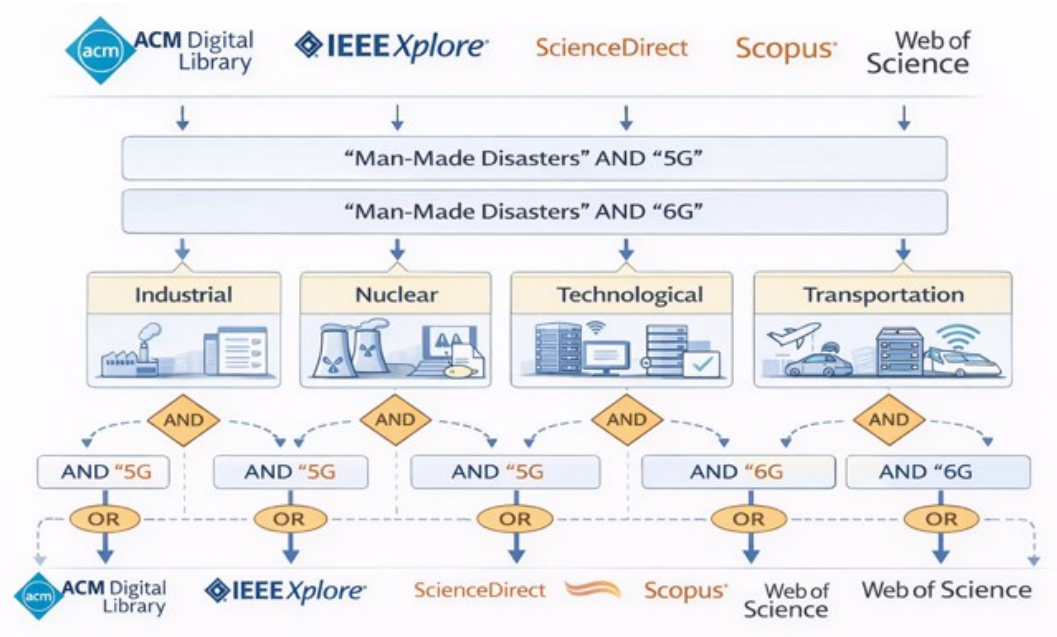


Figure 22 Boolean Query Stratification Across Hazard Classes and Technology Generations. Author's illustration.

To reduce database-specific indexing variability, each query was executed across title, abstract and keyword fields whenever available. Quotation marks were consistently applied to prevent token fragmentation, while standardized logical grouping preserved Boolean operator precedence. The same query structure was maintained across all selected databases to ensure methodological consistency and reproducibility. No adaptive query expansion was performed after the initial execution, thereby limiting post hoc bias and result-driven modification of search terms. The refinement process served two main analytical purposes. First, it enabled the identification of domain-specific 5G and 6G applications, including industrial monitoring, nuclear safety infrastructures, intelligent transportation networks and infrastructure-failure mitigation mechanisms. Second, it improved the retrieval of architectural studies focusing on resilient network slicing, MEC, NTN integration and URLLC mechanisms within specific technological hazard environments. The second-phase Boolean stratification therefore increased thematic granularity while maintaining consistency across databases, strengthening the overall validity of the literature review. Figure 23 illustrates the methodological workflow. The process begins with multi-database identification and Boolean querying, followed by screening, deduplication and full-text eligibility assessment. The retained studies are then refined and categorized to form the final corpus, from which evidence is extracted and graded. This structured process links literature retrieval and evaluation to the comparative matrices presented in Appendix A.

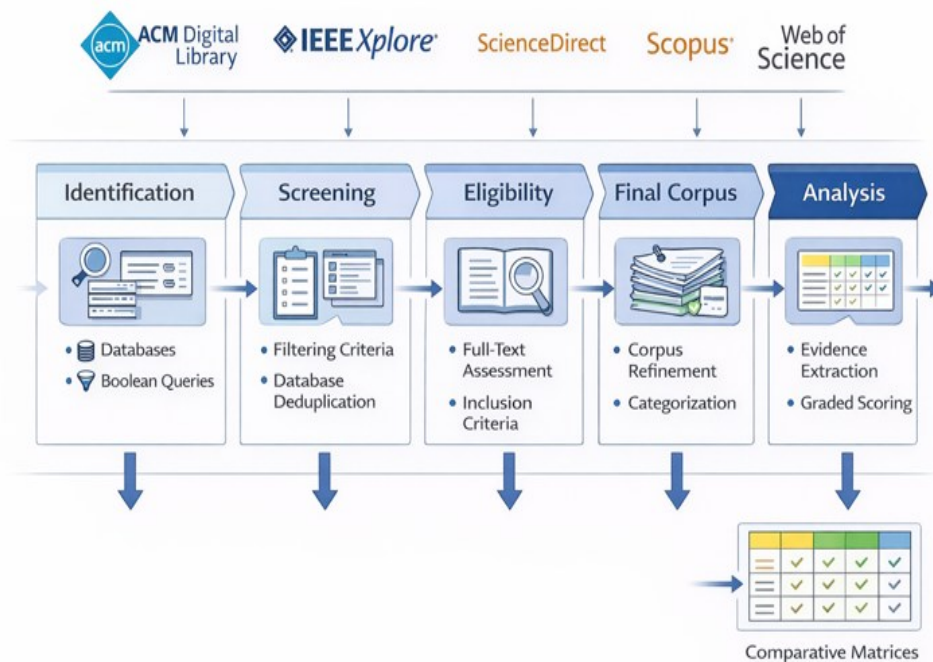


Figure 23 Literature Review Workflow and Analytical Pipeline. Author's illustration.

To ensure a transparent, systematic, and reproducible literature selection process, a structured keyword-based search strategy was developed. The search methodology followed a multi-stage approach designed to progressively refine the literature from a broad collection of potentially relevant studies to a focused set of publications addressing advanced mobile communication technologies in the context of man-made disasters. This progressive refinement was intended to balance broad literature coverage with sufficient thematic specificity, while reducing the risk of excluding relevant studies due to variations in terminology across different research domains.

Initially, broad search terms were employed to identify research linking 5G and 6G technologies with human-induced disaster scenarios. This initial stage established a comprehensive baseline and captured studies explicitly referring to man-made disasters within advanced communication environments. Subsequently, the search scope was refined by introducing specific categories of technological hazards, including industrial, nuclear, technological, and transportation-related disasters. The inclusion of these individual hazard categories enabled a more granular exploration of the literature and reduced reliance on the general term “man-made disasters,” which may not be consistently adopted across different scientific communities.

In the final stage, the retrieved studies were further filtered according to their primary contribution and technical relevance to the objectives of the review. Publications were distinguished between conceptual works, including surveys, reviews, frameworks, and taxonomies, and technically oriented studies focusing on network architectures, communication systems, deployment strategies, resilience mechanisms, resource management, and performance evaluation. This classification facilitated a more structured assessment of both the conceptual development of the field and the technological solutions proposed for supporting communication under disaster conditions.

Overall, this staged search procedure improved the comprehensiveness, thematic relevance, and consistency of the selected literature while maintaining methodological rigor throughout the review process. It also provided a systematic mechanism for progressively moving from broad technology–disaster associations toward studies directly aligned with the research objectives of the dissertation. Table 1 summarizes the overall search methodology, the successive stages of literature refinement, and the corresponding Boolean query structures.

Search Stage	Objective	Thematic Scope	Keywords	Boolean Logic	Methodological Role in the Study
Identification	Establish a comprehensive initial corpus of relevant literature	Man-made disasters and next-generation mobile networks	Man-made disasters, 5G, 6G	(“man-made disasters” AND “5G”) (“man-made disasters” AND “6G”)	Captures foundational studies linking technologically induced or human-driven crises with advanced mobile communication infrastructures
Screening	Refine the corpus by disaggregating the broad disaster category into targeted sub-domains	Industrial, Nuclear, Technological, transportation-related disasters	Industrial, nuclear, technological, transportation 5G, 6G	(“industrial” OR “nuclear” OR “technological” OR “transportation”) AND (“5G” OR “6G”)	Enables systematic retrieval of domain-focused studies addressing communication architectures and network design across distinct classes of technological hazards
Eligibility (Synthesis-Oriented)	Prioritize meta-studies and high-level analytical frameworks	Public safety, disaster communication, research taxonomies	Public safety, disaster, taxonomy, survey, communication, 5G, 6G	(public safety OR disaster) AND (“5G” OR “6G”) AND (taxonomy OR survey OR communication)	Identifies surveys and taxonomy-driven contributions that support theoretical grounding, cross-comparison and structured literature synthesis
Eligibility (System-Oriented)	Isolate technically detailed and implementation-oriented studies	Network architecture, deployment strategies, operational performance	Man-made disasters, technological disasters, network, system, performance, 5G, 6G	(man-made OR technological disasters) AND (“5G” OR “6G”) AND (network OR system OR performance)	Selects system-level and applied research for evaluating architectural choices, performance metrics and operational feasibility in crisis communication environments

Table 1 Systematic Search Strategy for the Identification and Selection of Relevant Studies

3.1.1 Inclusion and Exclusion Criteria

To ensure consistency and transparency throughout the screening process, a structured set of inclusion and exclusion criteria was applied across all stages of literature selection. The screening workflow progressively refined the initial corpus into a technically coherent dataset aligned with the analytical objectives of the current thesis.

At the first screening level, eligibility was limited to peer-reviewed scientific publications, including journal articles, conference proceedings and recognized survey or review papers published in English. This criterion ensured linguistic consistency and maintained a uniform academic quality threshold across the selected studies. Grey literature sources, including non-refereed technical reports, white papers, editorial commentary, workshop abstracts and presentation-only material, were excluded in order to maintain consistency in scholarly quality and peer-review standards.

The second screening stage focused on thematic and technical relevance. Selected publications were required to demonstrate a clear focus on communication technologies, network architectures, or system-level design approaches within man-made or technological disaster environments, with direct relevance to 5G or emerging 6G paradigms. Studies approaching disaster scenarios exclusively from social, organizational, legal, or policy-oriented perspectives, without a substantial technical or communication-focused component, were excluded from the final corpus.

The third screening stage involved duplicate detection and record consolidation across all selected databases. Records retrieved multiple times were initially identified through automated title and abstract matching procedures, followed by manual verification to confirm semantic equivalence and eliminate false positives. This process preserved corpus integrity and prevented the over-representation of recurring studies during subsequent analytical stages.

Taken together, these filtering stages produced a technically coherent dataset aligned with the thesis's research questions. The resulting corpus supports cross-comparison, evidence-based synthesis and structured mapping across disaster communication lifecycle phases and network-layer dimensions, as summarized in Table 2.

Screening Step	Objective	Inclusion Criteria	Exclusion Criteria	Operational Procedure	Methodological Contribution
Publication Type and Language Filtering	Ensure academic quality and consistency	Peer-reviewed journal articles, conference papers and recognized survey/review publications written in English	Grey literature, non-refereed reports, editorials, workshop abstracts, presentation-only materials, non-English publications	Filter by publication metadata and source classification at database level	Establishes a uniform scholarly baseline and ensures cross-source comparability
Technical and Thematic Relevance Assessment	Align corpus with thesis scope and research questions	Explicit focus on communication technologies, network architectures, or system-level designs in man-made or technological disaster contexts under 5G/6G paradigms	Studies limited to social, organizational, policy, or legal perspectives without substantive technical or communication analysis	Abstract and full-text screening using keyword and content validation	Ensures technical depth and conceptual coherence across the selected literature
Duplicate Detection and Consolidation	Preserve dataset integrity	Unique records representing distinct studies	Repeated entries across multiple databases or minor title variations of the same work	Automated title/abstract matching followed by manual semantic verification	Prevents over-representation and maintains analytical accuracy
Final Corpus Validation	Confirm methodological alignment	Studies supporting analytical mapping across PRRM phases, OSI layers, or system evaluation dimensions	Marginally relevant studies lacking analytical traceability to the research framework	Cross-check against analytical framework and classification tables	Strengthens traceability between methodology and downstream analysis

Table 2 Inclusion and Exclusion Criteria and Screening Workflow.

3.1.2 Academic Papers Refinement and Categorization

Following the initial title and abstract screening stages, the retained publications underwent a structured manual review process to verify their alignment with the defined research scope and selection criteria. This stage focused on consistency with the previously established selection criteria by examining the technical depth of each study, the clarity of the proposed systems or architectures and the relevance of the communication technologies to man-made or technological disaster environments. Particular attention was given to clearly defined research objectives, methodological clarity and explicitly stated contributions in order to

ensure that the refined corpus could support comparative analysis and evidence-based synthesis.

The finalized corpus was subsequently organized into two primary categories: research articles and survey or taxonomy-oriented studies. Primary research articles were defined as contributions proposing, implementing, or evaluating specific architectures, protocols, algorithms, or system deployments within 5G- or 6G-enabled disaster communication environments. In contrast, the survey and the taxonomy papers were treated as meta-level studies that synthesize existing literature, propose classification frameworks, or map research trends and gaps across broader technological and application domains.

This categorical separation enabled a differentiated yet coherent analytical workflow. Primary research articles were examined through criterion-driven assessments focusing on lifecycle alignment, network-layer mapping and evaluation methodologies, whereas survey and taxonomy papers were analyzed according to their classification logic, coverage breadth and identification of structural research gaps. This dual-path analysis provided the methodological basis for applying a Preparedness–Response–Recovery–Mitigation (PRRM) analytical framework¹, together with systematic OSI and network-layer mapping and comparative assessment of evaluation methods. This approach ensured that the resulting findings remained traceable to explicitly defined analytical dimensions within a methodologically consistent dataset.

3.2 Analytical Dimensions and Classification Framework

The analytical framework of this study provides a structured basis for comparing heterogeneous research contributions across both technical depth and disaster-management relevance. To support this objective, each publication in the refined corpus is evaluated across a set of clearly defined analytical dimensions. These dimensions support consistent evidence extraction, the identification of cross-cutting patterns and the mapping of findings to the research questions of the thesis.

¹ In this study, the Preparedness–Response–Recovery–Mitigation (PRRM) framework refers to an analytical organization of the established disaster management cycle around four core phases: preparedness, response, recovery and mitigation. Preparedness encompasses activities undertaken before an emergency to strengthen readiness and response capacity; response includes immediate actions during and directly after an event to protect life and maintain essential functions; recovery concerns the restoration and reconstruction of affected systems and communities; and mitigation comprises measures intended to reduce or prevent future disaster impacts. The PRRM designation is used here as an analytical construct for systematically mapping communication technologies and research contributions across these disaster-management phases.

The first analytical dimension classifies the reviewed studies according to their position within the disaster management lifecycle using the PRRM framework [5], [12]. Rather than treating disaster communication as a homogeneous operational domain, this dimension distinguishes the specific stage at which each technological contribution is intended to provide operational value. Studies addressing pre-disaster activities, including training, simulation, early-warning communication, preparedness planning and communication readiness, are classified under Preparedness. Research focusing on real-time coordination, emergency information exchange, mission-critical communication and dynamic resource allocation during active incidents is assigned to Response. Studies concerned with post-event infrastructure restoration, network re-establishment, service recovery and longer-term reconstruction are classified under Recovery, whereas approaches emphasizing proactive risk reduction, predictive monitoring, infrastructure hardening and communication mechanisms designed to reduce future disaster impacts are associated with Mitigation. Where a study addresses more than one phase, primary and secondary lifecycle relevance can be identified to preserve its multi-stage contribution. This lifecycle-oriented classification therefore provides both a temporal and functional perspective, enabling systematic assessment of how advanced communication technologies contribute before, during and after man-made and technological disaster events.

The second analytical dimension examines the principal technical and operational challenges influencing the design, deployment and viability of next-generation disaster communication systems. Each study is evaluated according to the extent to which it addresses reliability and resilience, including fault tolerance, redundancy, service continuity and recovery from partial infrastructure failure. Particular attention is also given to latency and Quality of Service (QoS), since mission-critical traffic may require differentiated prioritization and predictable communication performance under congestion or rapidly changing network conditions. Security and privacy constitute another analytical category, encompassing authentication, access control, secure information exchange and protection of sensitive operational data. In addition, interoperability is examined across heterogeneous communication technologies, organizational domains and responding agencies, reflecting the need for coordinated operation within multi-agency emergency environments. Finally, energy efficiency and resource availability are considered particularly relevant in scenarios where power supply, computing capacity or communication infrastructure may be

constrained or degraded [7]. This dimension complements the PRRM lifecycle classification by identifying not only when a technological solution contributes to disaster management, but also which technical or operational problem it is designed to address.

At the architectural level, the reviewed studies are further mapped to the OSI model in order to identify the primary and secondary networking layers targeted by each approach. This classification distinguishes between physical-layer innovations such as resilient spectrum utilization, non-terrestrial networking and energy-aware transceivers, data-link and network-layer mechanisms including routing, mobility management and topology control within ad hoc or heterogeneous environments, transport-layer solutions focused on congestion control and latency-sensitive communication and application-layer systems such as alerting platforms, sensor dashboards and decision-support tools. Studies integrating multiple networking layers are categorized as cross-layer or holistic approaches, reflecting broader trends toward AI-assisted and adaptive communication architectures.

Finally, each publication is evaluated according to its validation methodology, distinguishing between theoretical or simulation-based analyses, controlled testbed or laboratory implementations, field trials and pilot deployments and cross-disciplinary approaches integrating technical, organizational and regulatory considerations [45], [46]. This dimension provides an indication of empirical maturity and practical relevance, allowing differentiation between conceptual proposals and validated real-world systems.

Taken together, these analytical dimensions establish a unified classification framework for consistent cross-comparison between primary research articles and survey or taxonomy studies. The framework aligns lifecycle positioning, technical challenges, architectural focus and methodological rigor within a unified evaluative structure. This supports consistent evidence synthesis and structured comparative analysis across the reviewed literature. Each publication is therefore evaluated according to PRRM lifecycle positioning, key research challenges, OSI-layer focus and validation methodology in order to support consistent cross-comparison and evidence-based synthesis.

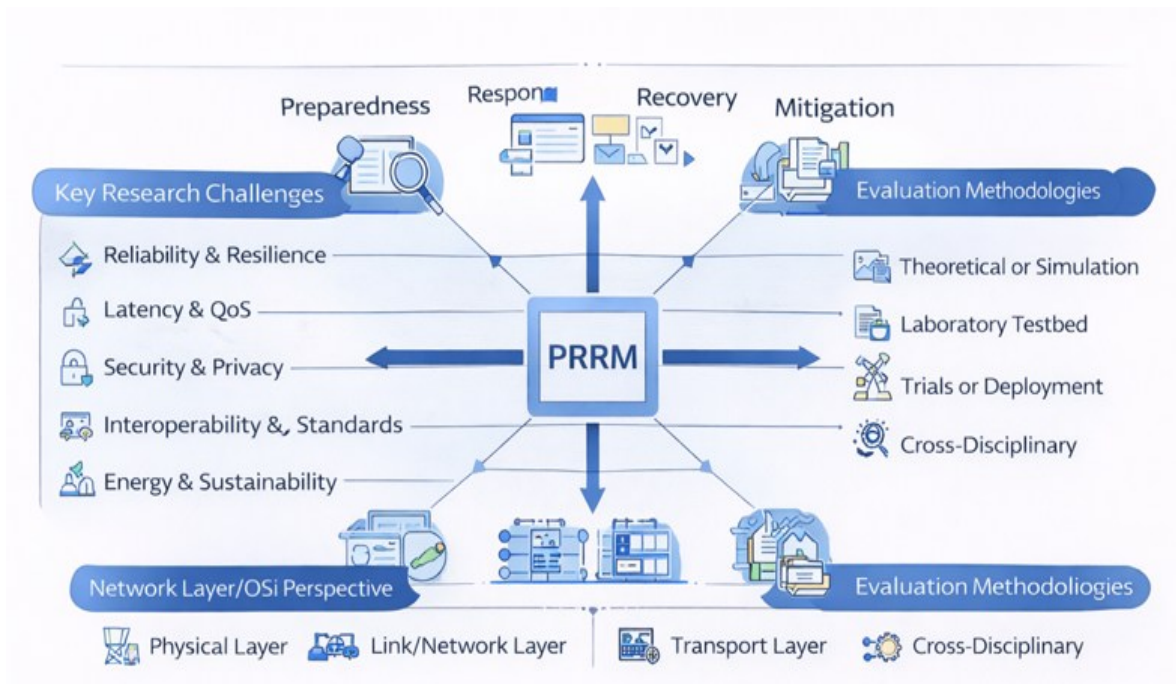


Figure 24 Unified Analytical Framework and Orthogonal Classification Dimensions. Author's conceptual illustration.

3.2.1 Disaster Management Phase Classification

The first analytical dimension operationalizes the disaster management lifecycle as a structured classification framework for mapping each research contribution to a dominant phase of crisis engagement [12]. Instead of treating disaster communication systems as static technical artifacts, this approach conceptualizes them as dynamic operational enablers whose functional role evolves throughout the different stages of a man-made disaster. Each study in the corpus is therefore assigned to a primary phase, Preparedness, Response, Recovery, or Mitigation based on the explicit objectives, system functions, and evaluation scenarios described in the methodological and results sections, as presented below:

- Preparedness:** Studies classified under the Preparedness phase primarily focus on pre-incident activities, including training environments, simulation platforms, and early-warning communication mechanisms designed to improve situational awareness and operational readiness before the onset of a disaster. These contributions commonly examine data acquisition pipelines, alert dissemination architectures, and predictive or scenario-based modeling frameworks intended to reduce response latency and strengthen coordination capabilities under future crisis conditions.

- **Response:** Studies classified under the Response phase address the real-time operational demands of active disaster scenarios. This category encompasses systems and protocols designed for mission-critical communication, including resilient routing mechanisms for degraded network environments, priority-aware traffic management strategies, and adaptive QoS mechanisms supporting command-and-control operations, first-responder coordination, and real-time sensor or video-data exchange under strict latency and reliability constraints.
- **Recovery:** Studies mapped to the Recovery phase focus on post-event communication and networking strategies that support infrastructure restoration, service continuity, and long-term operational resilience. These contributions typically examine architectures for re-establishing connectivity in damaged network topologies, integrating temporary or non-terrestrial communication platforms, and enabling data-driven assessment tools that support reconstruction planning and long-term performance evaluation.
- **Mitigation:** Studies classified under the Mitigation phase adopt a proactive and forward-looking perspective through predictive communication models, risk-aware network design, and data-driven forecasting mechanisms aimed at reducing the impact of future man-made disasters. These studies frequently integrate historical data analysis, AI-assisted decision-support mechanisms, and cross-layer optimization strategies to inform policy development, operational planning, and resilient system design before a crisis materializes.

This lifecycle-oriented classification provides both a temporal and functional perspective on how communication technologies are positioned across different stages of disaster management. By anchoring each contribution to a dominant operational phase, while allowing secondary phase associations where explicitly justified, the framework supports fine-grained comparative analysis and facilitates the identification of structural imbalances or underexplored areas within the existing body of research.

3.2.2 Key Research Challenges Classification

The second analytical dimension examines the core research challenges that influence the design, deployment and operational viability of communication systems in man-made disaster environments. Rather than viewing individual studies as isolated technical solutions, this dimension situates each contribution within a broader problem landscape shaped by persistent operational constraints, performance trade-offs and systemic

vulnerabilities emerging under crisis conditions. Each study is therefore assessed according to its explicit or implicit engagement with a structured set of challenge categories, enabling consistent cross-comparison and the identification of dominant research trends and unresolved gaps as follows:

- **Reliability and Resilience:** This category [15], [20] focuses on mechanisms that ensure communication continuity under adverse and rapidly evolving conditions. This includes fault-tolerant architectures, network and infrastructure redundancy strategies, and survivability-oriented designs capable of addressing node failures, link degradation, and partial network collapse. Studies in this category frequently emphasize adaptive routing, multi-connectivity, and heterogeneous network integration to preserve service availability during and after disruptive events.
- **Latency and Quality of Service (QoS):** This dimension examines the ability of communication systems to support time-critical and mission-sensitive operations. Contributions mapped to this category typically address priority-aware traffic management, real-time data delivery, and performance guarantees for applications such as command-and-control operations, live video transmission, and sensor-driven situational awareness. Particular emphasis is placed on how network architectures and protocol designs manage congestion, scheduling, and resource allocation under strict latency constraints.
- **Security and Privacy:** This category encompasses approaches designed to protect data integrity, confidentiality, and trust within highly dynamic and potentially hostile operational environments. This includes authentication and authorization mechanisms, secure key-management schemes, intrusion-detection systems, and privacy-preserving data dissemination models. Studies in this area frequently examine the balance between strong security guarantees and the operational requirement for rapid, low-latency communication during emergency-response activities.
- **Interoperability and Standards:** This dimension addresses the integration of heterogeneous systems across organizational, technological, and jurisdictional boundaries. Contributions classified within this category examine cross-agency communication frameworks, compliance with established or emerging standards, and architectural approaches enabling seamless interaction between legacy infrastructures, public safety networks, and next-generation 5G or 6G platforms.

This dimension is particularly important for evaluating the scalability and real-world applicability of proposed solutions within multi-stakeholder disaster-response ecosystems.

- **Energy Efficiency and Sustainability:** This category reflects the operational constraints associated with prolonged deployments and infrastructure-degraded environments. This includes energy-aware network architectures, power-efficient communication protocols, and resource-management strategies aimed at extending system lifetime under battery-constrained or off-grid conditions. Studies in this area often examine trade-offs between performance, coverage, and energy consumption, particularly in mobile, aerial, or temporary networking infrastructures.

By structuring the analysis around these challenge categories, this dimension provides a problem-centric perspective that complements the lifecycle-based classification framework. It enables the systematic identification of the technical and operational barriers most frequently addressed in the related literature, highlights underexplored research areas and reveals how emerging communication paradigms prioritize competing objectives within the broader context of disaster-management research.

3.2.3 Evaluation Methodology Classification

The third analytical dimension examines the evaluation methodologies employed by each study as an indicator of both technical maturity and the level of real-world validation. Rather than assessing performance claims in isolation, this dimension positions each contribution along a continuum of empirical rigor, ranging from conceptual and model-driven analyses to fully deployed and operationally validated systems. This approach enables a transparent comparison of how evidence is generated, validated and contextualized across heterogeneous research designs.

- **Theoretical and Simulation-Based Studies:** Studies within this category are characterized by analytical modeling, formal performance evaluation, and the use of network simulators or emulation environments to investigate system behavior under controlled and repeatable conditions. Contributions typically focus on protocol design, algorithmic performance, or architectural feasibility, using synthetic traffic models, parameterized scenarios, and sensitivity analyses to evaluate scalability,

latency, reliability, and resource utilization without direct exposure to real deployment constraints.

- **Laboratory-Oriented Testbed Experiments:** This category includes studies that move beyond abstract modeling by implementing prototypes or partial system realizations within controlled experimental environments. These contributions often employ hardware-in-the-loop configurations, SDN platforms, or small-scale experimental networks to validate functional correctness, interoperability, and performance under semi-realistic operating conditions. This category reflects an intermediate level of technical maturity in which theoretical assumptions are tested against practical integration and implementation challenges.
- **Field Trials and Pilot Deployments:** Studies within this category evaluate communication systems in operational or near-operational environments. This includes temporary or permanent real-world deployments, the involvement of end users such as first responders or infrastructure operators, and the collection of empirical performance data under dynamic and unpredictable conditions. Contributions within this category provide the strongest level of validation by exposing systems to environmental variability, user behavior, and organizational constraints that cannot be fully reproduced in laboratory settings [\[45\]](#), [\[46\]](#).
- **Cross-Disciplinary Frameworks:** This category encompasses studies that combine technical evaluation with policy, legal, organizational, or ethical considerations. These contributions frequently examine regulatory compliance, governance models, data-protection requirements, and socio-technical impacts alongside conventional system-performance metrics, reflecting the broader ecosystem in which disaster communication technologies are deployed and operated.

By differentiating contributions across these methodological categories, this dimension enables a structured assessment of validation realism and practical relevance. It supports the identification of gaps between conceptual innovation and operational deployment, while also highlighting areas where additional empirical validation or interdisciplinary integration is required to advance the state of the art in disaster communication research.

3.2.4 Network Layer and OSI Perspective

The fourth analytical dimension examines each contribution through the perspective of network architecture, using the OSI model as a structured reference framework for identifying the primary and secondary layers targeted by proposed solutions. This perspective enables a systematic comparison of how design choices, control mechanisms and performance optimizations are distributed across the communication stack, as well as how these architectural decisions align with the operational demands of man-made and technological disaster environments [4], [8].

- **Physical Layer:** Studies classified within the physical layer focus on resilient spectrum utilization, non-terrestrial and satellite connectivity, and energy-aware transceiver design. Contributions in this category typically address link robustness under interference, coverage extension in infrastructure-degraded environments, and power-efficient radio operation for mobile or temporary network nodes, including unmanned platforms and rapidly deployable base stations.
- **Data Link and Network Layers:** This category captures mechanisms related to topology formation, routing, and mobility management within dynamic and heterogeneous communication environments. This includes ad hoc and mesh-networking protocols, delay-tolerant networking strategies, and fault-aware routing schemes designed to maintain connectivity across highly mobile or partially disconnected nodes. Studies mapped to this category frequently emphasize adaptive path selection, neighbor discovery, and interoperability between legacy and next-generation network segments.
- **Transport Layer:** Contributions classified within the transport layer are evaluated according to their treatment of congestion control, end-to-end reliability, and latency sensitivity. This category includes protocol designs and traffic-management mechanisms that support prioritized data flows, maintain performance under bursty or degraded network conditions, and balance throughput with the strict timing requirements of mission-critical applications.
- **Application Layer:** This category focuses on end-user and system-level platforms, including alert dissemination systems, situational-awareness dashboards, and citizen-facing communication tools. Studies in this domain frequently integrate data fusion, visualization, and decision-support components that transform network-level

capabilities into actionable operational information for responders, infrastructure operators, and affected populations.

- **Cross-Layer and Holistic Approaches:** This category captures studies that explicitly integrate multiple layers of the communication stack within a unified architectural or control framework. These contributions frequently employ adaptive optimization strategies, SDN paradigms, and AI-assisted orchestration mechanisms to coordinate resource allocation, security policies, and QoS objectives across the physical, network, transport, and application layers [13], [47]. This category reflects the broader transition toward intelligent and self-adaptive communication ecosystems capable of responding dynamically to evolving disaster conditions.

By mapping each study across these architectural dimensions, the classification provides a transparent view of where technical innovation is concentrated within the communication stack and where structural gaps remain. It also supports a layered synthesis of evidence linking low-level radio and routing mechanisms with higher-level application outcomes, enabling a comprehensive and traceable assessment of how network-design choices influence operational performance within disaster-management environments.

3.3 Analytical Protocol, Evidence Extraction and Scoring Procedure

For each analytical dimension, a uniform and repeatable evaluation protocol was applied, combining structured evidence extraction, traceable classification, graded scoring, comparative mapping and synthesis procedures. This integrated approach was designed to transform heterogeneous research contributions into a structured and comparable evidence base, enabling both fine-grained technical assessment and higher-level analytical synthesis. In the first stage, a concise yet technically grounded summary was produced for each study. These summaries captured the core research problem, the proposed system, framework, or methodology and the primary application context within man-made disaster environments. Particular emphasis was placed on identifying the architectural scope, the targeted communication layers and the stated performance objectives, thereby establishing a common descriptive baseline for the subsequent stages of analysis.

The second stage focused on evidence extraction and traceability through explicit criterion-based mapping across all analytical dimensions. Each study was systematically aligned with

the relevant disaster-management lifecycle phase, research-challenge category, OSI or network-layer focus and evaluation methodology. These classifications were supported by direct references to specific sections, figures, tables, or architectural descriptions within the original publications, ensuring that all analytical judgments remained anchored to verifiable source material.

In the third stage, graded scoring, comparative mapping and synthesis procedures were applied to evaluate the relative depth and intensity of each study's engagement with the defined analytical criteria. Instead of relying on binary classification schemes, the framework employed graded qualitative levels to distinguish between marginal, moderate and strong contributions across each dimension. The resulting scores were aggregated into comparative matrices and synthesis tables to support cross-study comparison, trend identification and the structured integration of findings.

A dedicated metadata-driven protocol was additionally applied to survey and taxonomy-oriented studies in order to preserve their role as meta-level contributions rather than treating them as system-level implementations. For these works, structured metadata fields were extracted, including publication year, literature coverage period, classification dimensions, technology scope, disaster typology and the presence of comparative tables, taxonomies, or research-gap analyses. These metadata elements were subsequently used to position each survey within the broader research landscape and to enable cross-survey comparison based on analytical breadth, temporal coverage and methodological depth. The complete structure of these metadata fields, together with the associated scoring matrices and comparative tables, is provided in Appendix A, which serves as the primary reference for the tabular representations and column definitions used throughout the analysis.

Collectively, this protocol establishes a methodologically coherent workflow linking evidence extraction, traceable classification, graded scoring, comparative mapping and metadata-informed synthesis within a unified analytical process. It provides a transparent foundation for integrating both primary technical studies and meta-analytical survey contributions into a consistent analytical narrative, while also supporting the identification of dominant research trajectories, methodological imbalances and underexplored areas within the evolving landscape of disaster communication systems.

3.4 Alignment with Supervisory Evaluation Criteria

The adopted methodology demonstrates a high level of rigor through the application of a systematic multi-database search strategy, a clearly defined temporal scope and explicitly operationalized selection criteria. The analytical separation between primary research articles and survey or taxonomy-oriented contributions prevents category conflation and supports valid comparative analysis between studies of similar methodological orientation. In addition, the use of multiple orthogonal analytical dimensions including lifecycle positioning, key research challenges, evaluation methodology and OSI-based architectural mapping enhances internal consistency and reduces interpretative ambiguity, thereby strengthening the overall validity of the resulting synthesis.

Reproducibility is supported through the explicit documentation of data sources, Boolean-based keyword strategies, temporal boundaries and stepwise analytical procedures. A uniform evaluation protocol was applied across the entire corpus, combining structured technical summaries, evidence-anchored criterion mapping and graded comparative assessment. This standardized process enables independent replication of both the classification and scoring procedures. Transparency is further reinforced through the systematic linkage between analytical claims and verifiable references to specific sections, figures, tables, or architectural descriptions within the reviewed literature, while consolidated tabular representations are provided in the supporting appendices.

The methodology extends beyond a conventional descriptive literature review by incorporating a multi-dimensional and critically comparative analytical structure. Each contribution is evaluated according to lifecycle relevance, technical and operational challenges, validation realism and architectural positioning within the communication stack. This layered analytical perspective enables the identification of implicit assumptions, methodological constraints and structural imbalances across the research landscape, including the overrepresentation of specific paradigms and the relative underexploration of particular disaster phases, stakeholder groups or network layers.

Conceptual coherence is achieved through the integration of disaster-management lifecycle theory, network-architecture models and evaluation-methodology typologies within a unified analytical framework. The alignment between the PRRM model, OSI-based architectural mapping and validation-rigor assessment establishes a consistent conceptual foundation that supports structured synthesis and cross-dimensional comparison. This

integration avoids fragmented or purely thematic interpretation by situating each technical contribution within both a temporal and architectural context.

Finally, the use of multiple authoritative scientific databases, combined with complementary and systematically constructed keyword strategies, ensures broad and representative coverage of the relevant research landscape. The balanced inclusion of taxonomy-driven survey studies alongside application-oriented primary research mitigates bias toward either abstract conceptualization or narrowly scoped technical implementation. As a result, the methodology supports a comprehensive understanding of both overarching research trends and detailed system-level developments within the broader domain of communication technologies for man-made disasters.

3.5 Research-Question Traceability and Roadmap

To ensure that the related literature review produces findings that are analytically actionable rather than merely descriptive, the analytical framework was explicitly aligned with the thesis research questions. Each analytical dimension was operationalized through evidence-based mappings and graded assessments, while the resulting structured outputs were consolidated into the comparative tables presented in Appendix A. This design establishes a clear traceability chain linking raw literature evidence to research-question-driven analysis and defines the scope and structure of the empirical synthesis developed in the following chapters.

RQ1: What are the dominant evaluation methodologies (simulation, testbeds, field trials) used to validate communication solutions for man-made disasters and how do they affect the generalizability of findings?

The evaluation-methodology dimension constitutes the primary analytical axis for addressing RQ1, establishes the evidentiary foundation for the comparative assessment of validation practices across related literature. Each contribution is systematically categorized according to its validation paradigm, including simulation-based or theoretical analyses, controlled laboratory testbeds and empirical validation through field trials or pilot deployments. This structured categorization enables a consistent and reproducible mapping of evaluation methodologies across the corpus.

In Chapter 4, these methodological classifications are synthesized through quantitative aggregation and comparative analysis to identify prevailing validation patterns within the related literature. Particular emphasis is placed on examining how different methodological

choices influence the external validity of reported findings, especially their ability to generalize across heterogeneous man-made disaster scenarios. By correlating validation strategies with observed levels of generalizability, the analysis provides a critical assessment of the strengths and limitations associated with current evaluation practices. The resulting comparative evidence provides a robust basis for assessing the strengths and limitations of current validation practices, while supporting evidence-based conclusions regarding the generalizability of communication technologies across diverse man-made disaster scenarios.

RQ2: How do recent research contributions integrate advanced paradigms such as AI-native networking, ISAC, UAV-assisted relays, or blockchain-based trust frameworks into emergency communication systems?

RQ2 shifts the analysis toward technological convergence, examining how contemporary emergency communication systems incorporate emerging paradigms such as AI-native networking, ISAC, UAV-assisted relaying and blockchain-enabled trust mechanisms. Rather than evaluating technologies individually, the framework investigates how these capabilities are architecturally integrated to enhance operational performance.

Chapter 5 synthesizes these elements by systematically identifying where and how such paradigms are operationalized within emergency communication systems, including their roles in control-plane intelligence, cross-layer optimization, distributed trust management and edge-driven orchestration. Beyond functional placement, the analysis also evaluates the depth of integration and the maturity of validation approaches associated with each paradigm across the reviewed literature.

Comparative analysis across studies further highlights recurring architectural patterns, convergence trends and gaps between conceptual proposals and empirically validated implementations. The resulting synthesis provides a comprehensive view of current technological convergence, enabling a systematic assessment of architectural maturity, integration depth and emerging innovation trends across the reviewed literature.

RQ3: Which network layers receive the most research attention for crisis communication and where do significant gaps remain?

RQ3 adopts an architectural perspective, using OSI-based classification to reveal how scholarly attention is distributed across network layers. Instead of evaluating individual

technologies, this analysis identifies concentrations of research activity, underexplored architectural domains and opportunities for future investigation.

In Chapter 6, these layer-level classifications are aggregated across the corpus to produce a comparative distribution of research attention, highlight underrepresented layers and cross-layer interactions and identify recurring architectural blind spots within current disaster communication research. By systematically mapping research attention across OSI layers, the analysis establishes a clear evidence base for identifying architectural imbalances and defining priorities for future emergency communication research.

4. RQ1 Evaluation Methodologies and Their Effect on Generalizability

The evaluation of communication systems designed for man-made disaster scenarios constitutes a foundational yet inherently complex stage within the broader system-development lifecycle. Unlike conventional networked environments, emergency communication infrastructures operate under conditions characterized by uncertainty, infrastructure degradation, dynamic topology changes and the simultaneous involvement of heterogeneous stakeholders, including first responders, public safety agencies and civilian populations. Within such environments, the validity of a proposed communication solution cannot be inferred solely from theoretical design assumptions or performance under controlled conditions. Instead, it must be rigorously assessed through evaluation methodologies capable of capturing both technical performance and operational viability. As a result, how these systems are evaluated directly influences not only their perceived effectiveness but also the extent to which findings can be generalized across diverse disaster contexts.

At the core of this challenge lies a fundamental tension between analytical tractability and environmental realism. Communication systems designed for emergency scenarios are frequently evaluated using methodologies that prioritize one dimension at the expense of the other. Highly controlled approaches, such as simulation-based studies, enable systematic exploration of network parameters, scalability conditions and algorithmic behavior within reproducible environments. In contrast, field deployments and real-world trials provide critical insights into the interaction between technical systems and operational constraints, including regulatory requirements, human behavior, environmental uncertainty and inter-agency coordination. However, these approaches are typically constrained by cost, limited scalability and reduced repeatability. As a result, the current evaluation landscape remains fragmented, with no single methodology capable of providing fully comprehensive validation.

The importance of addressing this fragmentation becomes particularly evident when considering the operational consequences associated with communication-system failure during disaster scenarios. Disruptions in communication infrastructure may lead to delayed response coordination, resource misallocation, reduced situational awareness and diminished operational effectiveness under time-critical conditions. As a result, evaluation

must extend beyond conventional performance metrics such as throughput, latency, or packet-delivery ratio to incorporate broader dimensions including resilience, adaptability, survivability and operational usability under stress conditions. In this context, evaluation should not be interpreted solely as a technical benchmarking exercise, but rather as a socio-technical process shaped by the interaction between system architecture, environmental conditions and human decision-making.

A recurring observation throughout the related literature is that evaluation methodologies are often applied in isolation, without systematic integration across multiple validation layers. Many studies rely exclusively on simulation environments in which network topology, traffic patterns and failure conditions are predefined and frequently idealized. Although these approaches remain valuable for comparative analysis and early-stage validation, they inherently abstract away the uncertainty and variability characterizing real disaster environments. Conversely, studies employing experimental testbeds or operational deployments often focus on highly specific use cases or geographically localized environments, thereby limiting the broader applicability of their findings. This methodological fragmentation creates a research landscape in which performance claims are frequently difficult to compare, reproduce, or extrapolate across operational contexts.

The increasing complexity of modern communication paradigms further intensifies these evaluation challenges. Emerging technologies such as edge computing, UAV-assisted networking, NTN and AI-driven network management introduce additional layers of variability, interdependence and architectural complexity. These systems frequently operate across multiple networking layers while simultaneously interacting with both physical and virtualized infrastructure components. As a result, meaningful evaluation requires not only the assessment of isolated components but also the analysis of system-level behavior under dynamic and unpredictable operational conditions. Traditional evaluation approaches focusing primarily on isolated metrics or subsystem-level performance are therefore often insufficient to capture the broader interactions shaping real-world operational effectiveness. Within this context, generalizability emerges as a central concern for the present research question. Generalizability refers to the extent to which the findings of a study can be transferred beyond the specific conditions under which they were originally obtained. In emergency communication research, this includes the applicability of results across different disaster types, geographical regions, network configurations, operational

requirements and organizational structures. However, generalizability is not a uniform property, rather, it is strongly influenced by the evaluation methodology employed. Simulation-based studies may support broader parameter-space exploration while lacking empirical grounding, whereas field-based studies provide stronger contextual realism but often remain constrained in scope, scalability and reproducibility. Understanding how different evaluation methodologies shape this trade-off is therefore essential for assessing the overall contribution and practical relevance of existing research.

The need for a structured comparative assessment of evaluation methodologies is further reinforced by the absence of standardized validation frameworks within the field. Unlike more mature engineering domains, where benchmarking standards and testing protocols are well established, the evaluation of disaster communication systems remains largely ad hoc and methodologically fragmented. Researchers often select evaluation approaches based on resource availability, implementation feasibility, or narrowly defined research objectives rather than a unified validation strategy. This lack of standardization complicates cross-study comparison and limits the accumulation of cumulative scientific knowledge, as findings cannot always be consistently benchmarked or integrated.

Against this background, the present chapter systematically examines the dominant evaluation methodologies used to validate communication solutions for man-made disasters and analyzes how these methodologies influence the generalizability of findings. The analysis is grounded in an extensive literature corpus encompassing simulation-based studies, experimental testbeds, field deployments, AI-assisted evaluation environments and meta-analytical approaches. By synthesizing evidence across these methodological categories, the chapter seeks to identify recurring patterns, methodological biases and critical research gaps shaping the current state of the field.

More specifically, the chapter first establishes a structured taxonomy of evaluation methodologies before examining their respective characteristics, strengths and limitations. It subsequently introduces a unified evaluation pipeline capturing the progression from conceptual modeling to real-world deployment, highlighting both the stages at which validation commonly occurs and the areas where significant methodological gaps persist. The following sections then analyze statistical trends across the related literature, evaluate methodological limitations and compare how different validation approaches influence the

generalizability of reported findings. Finally, the chapter synthesizes these observations to identify major research gaps and propose future research directions.

Through this structured analytical approach, the chapter not only addresses the research question directly but also contributes to a more coherent understanding of how evaluation practices shape the development, validation and operational deployment of communication systems within disaster environments. By explicitly linking methodological choices with their implications for generalizability, the analysis establishes a critical foundation for improving both the scientific rigor and the practical relevance of future research in emergency communication systems.

4.1 Methodological Framework

This study follows a structured analytical approach to examine how communication solutions for emergency scenarios are evaluated and how these evaluation choices influence the generalizability of reported findings. The analysis is grounded in a carefully selected body of literature identified through a systematic review process, ensuring consistency in both study selection and analytical assessment.

Each study included in the dataset satisfies predefined inclusion criteria aligned with the research question, particularly the validation of communication systems in emergency, mission-critical, or disaster-related environments. Emphasis is placed on studies that clearly describe their evaluation methodology, including simulation, controlled testbed experimentation, or real-world deployment.

Unlike conventional narrative reviews, the dataset was developed incrementally and assessed through a unified analytical framework, improving methodological consistency and enabling comparison across heterogeneous studies. It therefore provides the empirical basis for both statistical analysis and conceptual synthesis.

To systematically analyze validation practices, each study is classified according to the evaluation methodology employed. Following the structure adopted in prior large-scale research efforts ([\[15\]](#), [\[20\]](#)), evaluation approaches are categorized into three primary classes:

- simulation-based evaluation
- testbed-based experimentation
- real-world field trials

Beyond these primary categories, particular attention is given to studies employing hybrid validation strategies that combine multiple evaluation approaches, such as simulation integrated with experimental testing or operational deployment. This classification reflects the typical progression of communication-system research, where theoretical concepts are initially explored through simulation, subsequently examined within controlled experimental environments and ultimately assessed under real operational conditions [48]. By distinguishing between studies relying on a single validation method and those incorporating multiple stages of evaluation, the analysis enables a more nuanced interpretation of validation practices and supports the identification of prevailing methodological tendencies across the related literature.

Within this framework, each study is examined using a consistent set of analytical criteria designed to capture both the nature and rigor of the evaluation process. This structured approach supports comparative assessment across validation strategies and provides deeper insight into their methodological robustness and overall completeness. The primary analytical features include:

- presence of simulation, testbed and field evaluation
- identification of hybrid validation strategies
- scale of experimentation (e.g., number of nodes or deployment size)
- validation depth and methodological completeness
- scoring metrics reflecting evaluation rigor and operational relevance

The scoring framework developed for the dataset plays a central role in quantifying the strength of each study's validation methodology. Each contribution is evaluated across multiple dimensions, including methodological completeness, evaluation realism and practical applicability, enabling the calculation of an aggregate validation score. This structured encoding process transforms qualitative descriptions of evaluation procedures into quantifiable analytical variables, thereby supporting statistical aggregation and comparative analysis.

The structured dataset further enables the application of statistical techniques for identifying trends and patterns across evaluation methodologies. The analysis focuses on four primary dimensions. First, the frequency distribution of evaluation methods is examined to determine the prevalence of simulation-based, testbed-oriented and field-based approaches. Second, the occurrence of hybrid validation strategies is analyzed to assess the extent to

which studies combine multiple methodological paradigms. Third, the relationship between evaluation methodology and validation strength is investigated by correlating it with the scoring framework, enabling assessment of whether more realistic validation approaches are associated with stronger methodological rigor. Finally, where applicable, temporal and structural trends are examined, highlighting the evolution of validation practices and the increasing adoption of experimental evaluation environments. This quantitative perspective enables the transition from descriptive reporting to evidence-driven analytical interpretation, supporting the identification of dominant methodological practices and emerging research tendencies.

A central objective of this study is to examine how different validation methodologies influence the generalizability of research findings. To address this objective, a conceptual assessment framework is introduced linking each evaluation methodology to four key dimensions:

- realism of the evaluation environment
- level of experimental control
- reproducibility of results
- generalizability of findings

Simulation-based approaches provide high levels of control and reproducibility but often depend on simplified assumptions that limit their ability to capture real-world operational complexity. Experimental testbeds introduce greater realism, although they frequently suffer from reduced reproducibility due to hardware dependencies and environmental variability. Field trials provide the highest level of operational realism but are typically constrained in terms of experimental control and repeatability. This trade-off between realism and reproducibility has consistently emerged in the related literature as a fundamental challenge in communication-system evaluation and serves as a central interpretative axis throughout the present analysis. By explicitly linking evaluation methodologies with generalizability outcomes, the proposed framework enables the transformation of descriptive statistical observations into broader analytical insights directly addressing the research question.

Despite its structured design, the proposed methodology remains subject to several limitations. First, the classification of evaluation methodologies and the scoring of studies involve a degree of expert judgment, potentially introducing limited subjectivity into the

analytical process. However, consistency is maintained through the systematic application of predefined evaluation criteria across the entire dataset. Second, the analysis is constrained by the selected literature corpus and may therefore not capture every recent development within the field. Nevertheless, the size, diversity and thematic breadth of the dataset provide a representative overview of current evaluation practices. Third, the abstraction of complex validation procedures into discrete analytical categories and numerical scores may not fully capture all nuances of experimental design and operational context. Although this limitation is inherent in most quantitative meta-analytical approaches, it is partially mitigated through complementary qualitative interpretation.

The adopted framework extends existing evaluation-oriented studies by integrating statistical analysis with a generalizability-centered analytical perspective. While prior work has primarily focused on the distribution of evaluation methodologies, the present study advances the discussion by explicitly linking validation strategies with their influence on the reliability, transferability and practical applicability of research findings. By combining structured data extraction, quantitative aggregation and conceptual modeling within a unified analytical process, the methodology establishes a robust foundation for examining evaluation practices in emergency communication systems. More importantly, this approach enables a deeper understanding not only of which methodologies are employed across related literature, but also of how and why these methodological choices shape the scientific validity and operational relevance of reported results.

4.2 Statistical Analysis and Its Effect on Generalizability

The present statistical analysis examines a corpus of 107 studies included in the RQ1 dataset, with the objective of systematically identifying the dominant evaluation methodologies used in communication research for man-made disasters and emergency scenarios. More importantly, the analysis investigates how these methodological choices influence the generalizability of reported findings. The assessment is grounded in the established scoring dimensions simulation-oriented evaluation, testbed experimentation, field validation and cross-disciplinary framing together with the categorical variables of primary evaluation methodology, validation-maturity characterization and generalizability profile.

The first major finding is the strong predominance of simulation-driven validation approaches within related literature. Simulation-based studies account for 42 out of 107 contributions (39.3%), while Conceptual studies represent an additional 29 contributions

(25.1%). In contrast, strictly field-based studies are limited to only 8 cases (7.5%), whereas purely analytical contributions account for just 2 studies (1.9%). This distribution strongly supports the central premise of RQ1, namely that research on disaster communication systems predominantly evolves within controlled, abstract, or partially synthetic evaluation environments rather than through operationally grounded validation contexts.

The second major finding concerns the distribution of generalizability categories. Institutional, Analytical and Technical forms of generalizability appear relatively balanced across the dataset, accounting for 33, 26 and 26 studies respectively. However, the prominence of Institutional generalizability should not be interpreted as evidence of widespread operational validation. Instead, it primarily reflects a recurring tendency to position technical proposals within broader organizational, governance, or policy-oriented frameworks without empirically validating them under realistic operational conditions. As a result, the related literature demonstrates substantial institutional awareness while simultaneously exhibiting limited operational substantiation.

A third important observation emerges from the average values associated with the primary scoring dimensions: simulation (2.61/5), testbed experimentation (0.98/5), field validation (0.67/5) and cross-disciplinary framing (3.64/5). This profile is particularly revealing. Simulation clearly constitutes the dominant evaluation pillar across related literature, although not with complete methodological uniformity [15], [20]. At the same time, the comparatively low scores associated with testbed experimentation and field validation indicate that the transition from abstract or numerical validation toward empirical and operational substantiation remains incomplete. In practical terms, the related literature demonstrates strong emphasis on conceptual and algorithmic exploration, while comparatively fewer studies validate their findings under realistic deployment conditions. Finally, the distribution of validation maturity indicates that the field cannot be characterized as methodologically immature. Among the 107 studies with explicit maturity characterization, 35 are classified as Very Strong, 15 as Strong, 26 as Moderate and 26 as Weak and 5 as Unspecified. This result reveals a more nuanced reality than simple maturity categorization might suggest. Although a significant portion of the related literature demonstrates substantial sophistication in algorithmic design, architectural modeling, or analytical formulation, this sophistication does not necessarily translate into realistic

operational validation. In other words, methodological maturity within the field often reflects technical complexity rather than empirical realism under actual disaster conditions.

4.2.1 Distribution of Primary Evaluation Methods

The first analytical dimension concerns the distribution of primary evaluation methodologies across the dataset. As illustrated in Figure 25, simulation-based approaches clearly dominate, accounting for 42 studies (39.3%). This predominance is not incidental but reflects a structural characteristic of research in disaster communication systems. Environments characterized by infrastructure disruption, uncertainty, rapidly changing network conditions, and operational risk are inherently difficult to reproduce through controlled experimentation. Conducting large-scale field evaluations under realistic disaster conditions is often constrained by logistical complexity, infrastructure availability, and limited access to representative emergency scenarios.

As a result, simulation provides a tractable, flexible, and scalable alternative, enabling researchers to systematically investigate network behavior under a broad range of synthetic conditions. These may include variable traffic loads, node mobility patterns, infrastructure failures, changing network topologies, resource constraints, and different protocol configurations [49]. Simulation environments also allow researchers to evaluate alternative architectures and operational strategies before considering more resource-intensive experimental validation.

Beyond practical feasibility, simulation supports methodological rigor by enabling controlled parameter isolation, repeatability, and systematic comparison across different scenarios. These characteristics are particularly valuable for comparative evaluation and sensitivity analysis, where the effects of individual network parameters or design choices must be examined independently. Consequently, the dominance of simulation-based validation reflects both the practical constraints of disaster-oriented experimentation and the analytical flexibility required to evaluate communication systems under diverse and highly dynamic conditions.

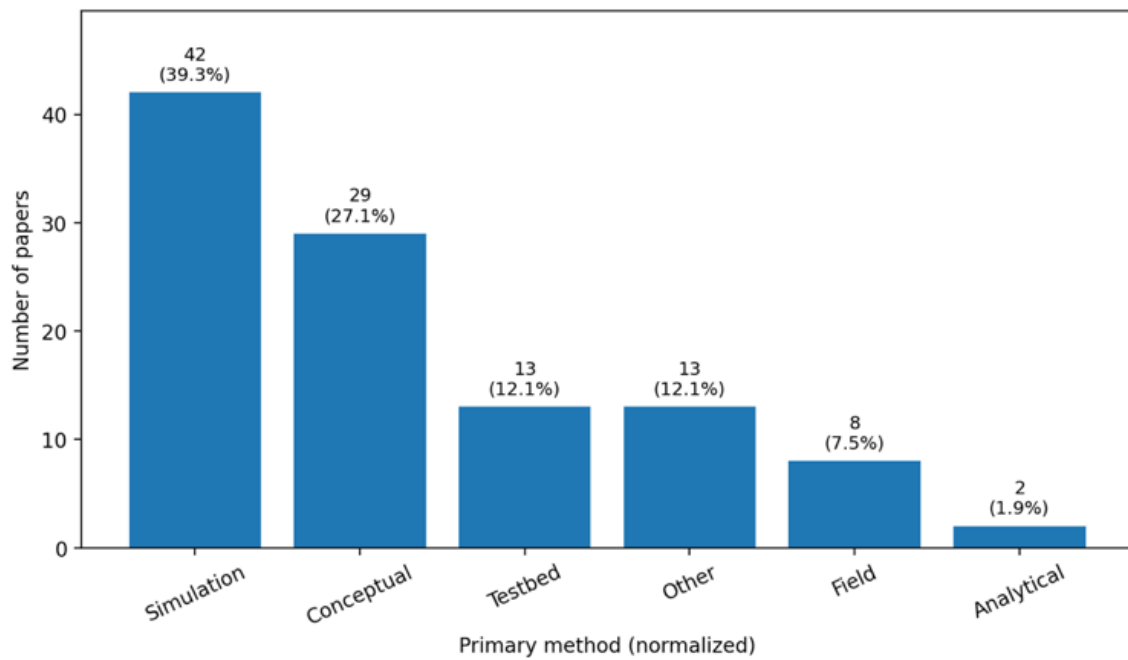


Figure 25 Distribution of Primary Evaluation Methods.

The second most prominent category comprises conceptual studies (29 studies, 27.1%), which focus on the formulation of frameworks, architectural models and system-level abstractions. The strong presence of this category indicates that the field remains actively engaged in defining its structural and operational paradigms. Rather than merely refining existing solutions, a substantial portion of the related literature is devoted to proposing new coordination models, resilience strategies and integration architectures often addressing emerging technologies such as UAV-assisted networking, edge-enabled orchestration, or hybrid satellite-terrestrial systems. This conceptual emphasis suggests that the domain is still undergoing a phase of architectural consolidation, where competing design logics and system configurations are being explored and refined [18], [31].

In contrast, validation through testbed experimentation and real-world deployment remains comparatively limited. Only 13 studies (12.1%) employ testbed-based methodologies, while 8 studies (7.5%) report field-level validation. This asymmetry reveals a clear stratification within the evaluation pipeline. While simulation and conceptual modeling facilitate rapid hypothesis generation and theoretical exploration, their translation into controlled experimental environments or operational contexts is far less frequent. The limited adoption of testbeds reflects both technical and logistical constraints, including the need for specialized infrastructure, interoperability challenges and reproducibility issues. Field validation, in turn, is constrained by even more demanding requirements, such as

coordination with institutional stakeholders, regulatory compliance and the unpredictability of real-world disaster conditions. As a result, the progression from abstract validation to empirically grounded verification remains incomplete.

Finally, the presence of the “Other” category (13 studies, 12.1%), alongside the marginal representation of strictly analytical approaches (2 studies, 1.9%), underscores the field's methodological diversity. These studies often employ hybridized or non-standard evaluation strategies that do not conform neatly to established categories. This heterogeneity is analytically significant: it indicates that the challenge is not solely the scarcity of empirical validation, but also the absence of a fully standardized evaluative paradigm. In effect, the related literature exhibits multiple coexisting methodological procedures, each with its own assumptions, validation criteria and scope of inference. This plurality complicates direct comparison across studies and further constrains the consolidation of generalizable findings.

4.2.2 Mean Score by Validation Dimension

Figure 26 presents the average scores across the four evaluation dimensions, revealing an uneven validation profile within the reviewed literature. The cross-disciplinary dimension achieves the highest mean score (3.64/5), indicating that many studies consider broader technical, organizational, and operational aspects of disaster communication systems. Simulation follows with a moderate mean score of 2.61/5, confirming its central role in assessing network performance under controlled disaster scenarios. In contrast, testbed (0.98/5) and field-based evaluation (0.67/5) remain substantially lower, indicating a limited transition from simulation toward experimental and real-world validation.

This distribution suggests that the literature demonstrates relatively strong conceptual and cross-disciplinary understanding, while empirical validation under realistic operational conditions remains less developed. The gap between simulation and testbed or field experimentation therefore represents an important limitation in assessing the practical maturity and operational readiness of proposed solutions. Researchers increasingly approach disaster communication as a complex socio-technical system, incorporating operational realities, coordination challenges, and institutional constraints alongside network performance [7]. However, this conceptual maturity does not necessarily provide evidence that proposed solutions will perform effectively under real-world conditions.

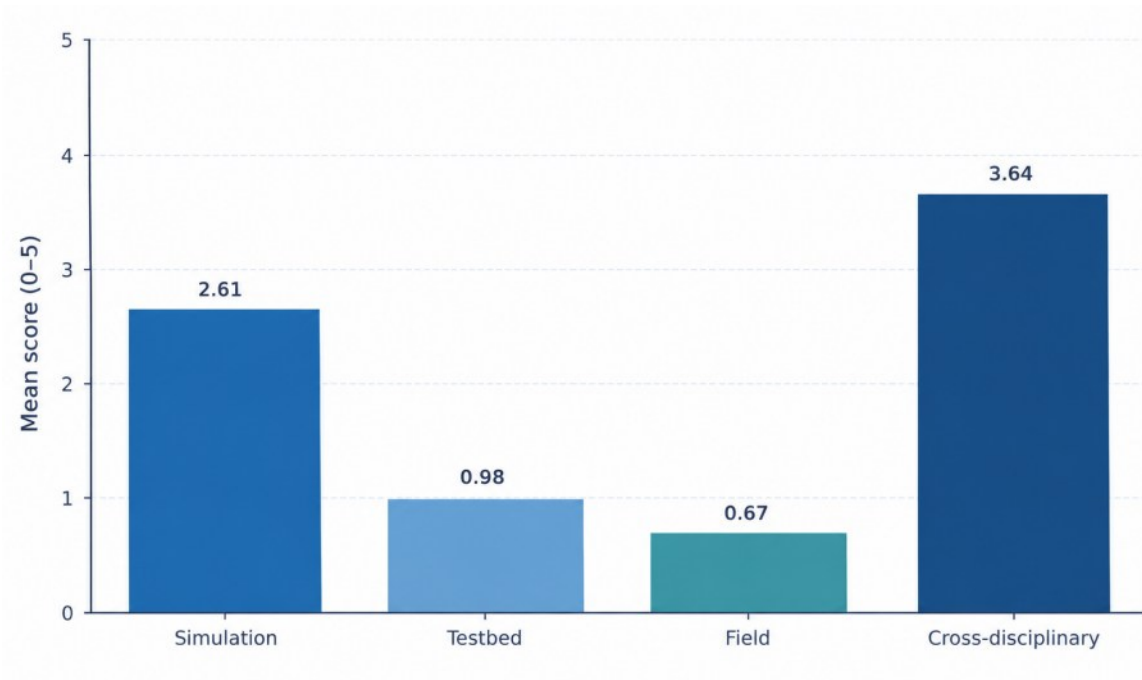


Figure 26 Mean Scores by Evaluation Dimension.

Simulation plays a central but non-uniform role in this landscape. While many studies use it as their primary validation method, its application varies considerably, ranging from detailed scenario-based evaluations to supporting evidence for largely conceptual proposals. It is therefore more accurate to consider simulation a dominant but flexible, rather than standardized, validation approach.

In contrast, testbed and field-based evaluations represent a key weakness in the literature. Their low scores indicate that real-world factors, such as infrastructure damage, human unpredictability, and inter-organizational coordination, remain insufficiently captured. Without exposure to these constraints, assessing the robustness and reliability of proposed solutions under realistic operational conditions remains difficult.

4.2.3 Validation Maturity Distribution

Figure 27 presents the distribution of validation maturity across the cleaned RQ1 dataset, offering a complementary perspective to the analysis of evaluation methods. While previous sections focus on how studies validate their solutions, this figure shifts the focus to how robust and complete that validation process is. By capturing the maturity level of each study, from weaker or partial validation to more structured and comprehensive approaches, the figure provides a clearer view of the overall reliability of the evidence produced in the field.

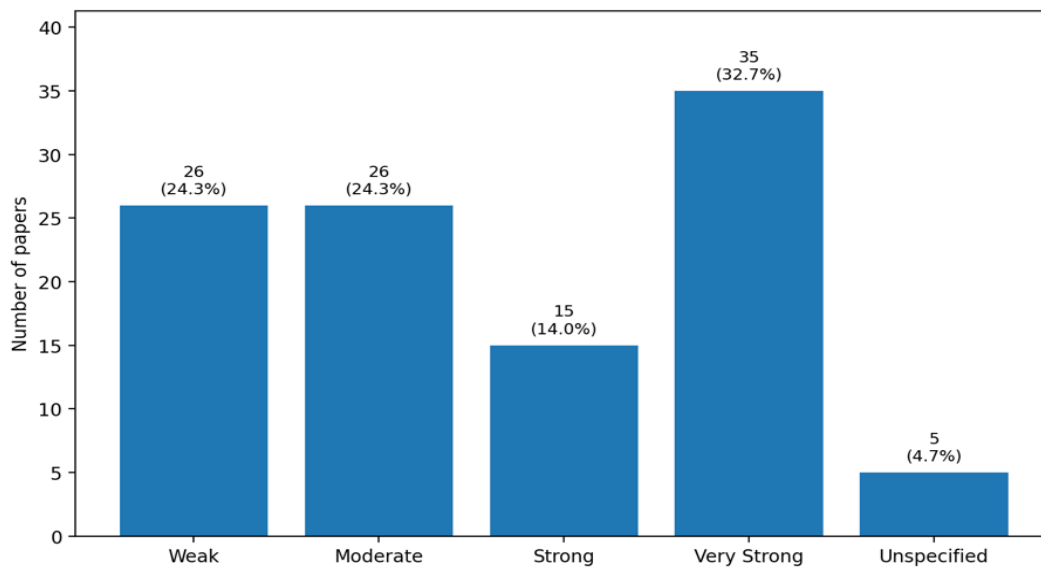


Figure 27 Validation Maturity Distribution.

More specifically, researchers tend to treat disaster communication as a complex socio-technical system. Their work often goes beyond pure network performance and includes operational conditions, coordination challenges and institutional constraints. This broader view certainly enriches the analysis and brings it closer to real-world complexity. At the same time, however, it mainly strengthens the conceptual side of the work, without always providing equally strong empirical support.

Simulation plays a central role in this context, but not in a uniform way. It is widely used, yet its depth varies from study to study. In some cases, simulations are carefully structured, with detailed scenarios and systematic evaluation processes. In others, they function more as supporting evidence for ideas that are primarily conceptual. For this reason, simulation should be seen as the main validation approach of the field, but not as a fully consistent or standardized one.

On the other hand, testbed and field-based evaluations clearly represent the weakest point. Their low scores indicate that many of the challenges present in real environments such as infrastructure disruption, unpredictable human behavior and coordination between multiple actors are not fully captured. This limitation is important, because without testing under such conditions, it is difficult to confidently assess how well these solutions would perform outside controlled or simulated environments.

4.2.4 Interaction Between Method and Generalizability

The relationship between the primary evaluation method and generalizability, as shown in Figure 28, provides important evidence for addressing RQ1. Simulation-based studies are predominantly associated with analytical generalizability, accounting for 24 of the 42 reviewed studies. This indicates that simulation remains the principal mechanism through which proposed architectures, protocols and communication strategies are evaluated across the literature. Such studies can provide internally consistent and methodologically controlled evidence regarding system behavior, performance trends and comparative effectiveness under predefined experimental conditions. However, their findings are not necessarily directly transferable to real-world disaster environments, where infrastructure degradation, mobility, interference, unpredictable traffic patterns and operational constraints may substantially affect system performance. The strong concentration of studies within this category therefore reveals a clear gap between analytical validation and operational generalizability. While simulation provides a valuable foundation for evaluating emerging communication technologies, broader testbed, field-based and operational validation is required to determine whether the reported performance improvements can be consistently reproduced under realistic emergency-response conditions.

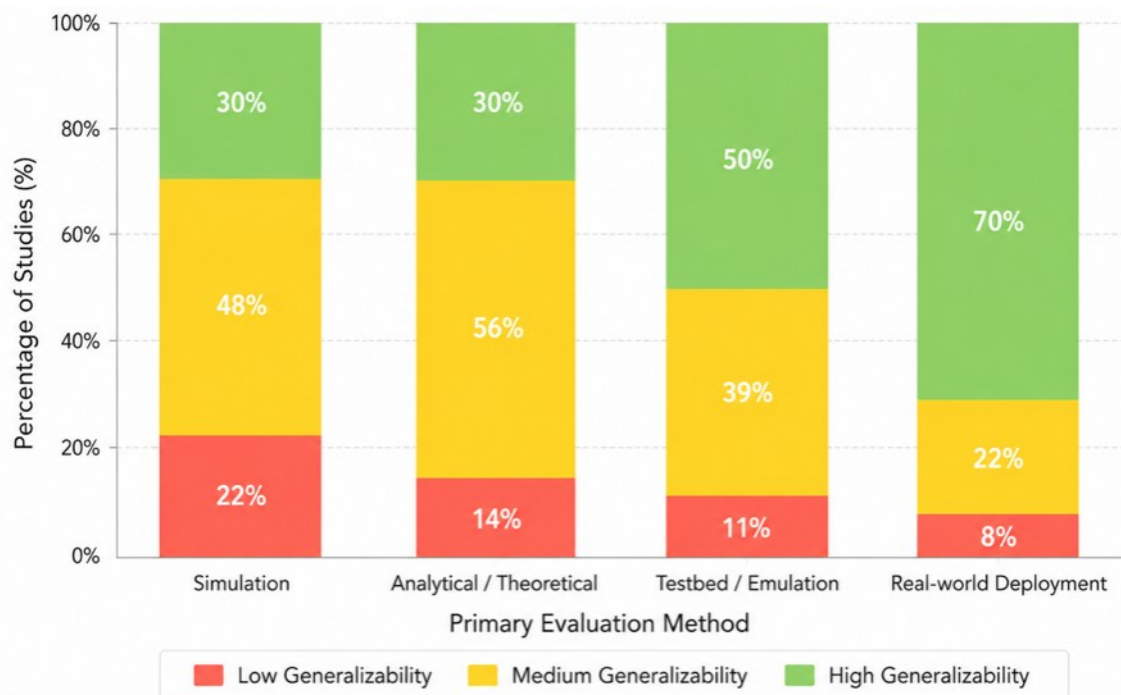


Figure 28 Primary Method vs Generalizability.

Conceptual studies are more strongly associated with institutional generalizability, with 20 of the 29 studies falling within this category. This indicates that conceptual research primarily examines how communication architectures, technologies, and operational models can be integrated into organizational structures, multi-agency coordination mechanisms, and governance frameworks. Such studies provide valuable insight into system-level requirements and institutional interoperability, but generally offer limited empirical evidence regarding technical feasibility and performance under realistic operational conditions.

Testbed-based studies exhibit a different pattern, with 11 of 13 associated with technical generalizability. This highlights their role in bridging theoretical development and practical implementation. Unlike simulation-based approaches, testbeds introduce physical constraints such as hardware limitations, processing delays, protocol interactions, and resource restrictions. They therefore provide stronger evidence of implementation feasibility and represent an important intermediate stage between simulation and full-scale field deployment, particularly for emerging 5G, 6G, and mission-critical communication technologies.

Figure 29 reinforces this pattern by showing that each evaluation methodology tends to strengthen the type of generalizability with which it is naturally aligned. Simulation primarily supports analytical generalizability, conceptual studies emphasize institutional applicability, and testbed approaches provide stronger evidence of technical generalizability. Overall, the literature places considerable emphasis on system-level understanding and architectural development, while fewer studies progress toward rigorous validation under realistic operational conditions. This imbalance highlights the need for stronger progression from conceptual and simulation-based research toward testbed experimentation, field validation, and real-world deployment.

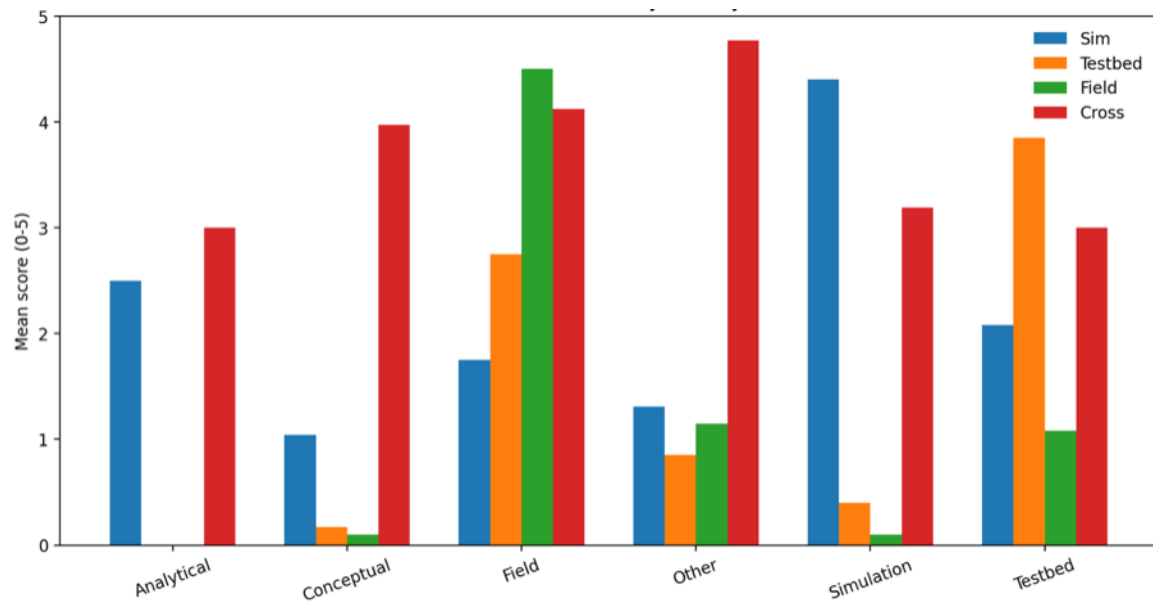


Figure 29 Mean Dimension Scores.

4.2.5 Interpretation for RQ1

The statistical findings provide a direct and structured answer to RQ1. Across the 107-study dataset, evaluation practices are heavily concentrated around simulation-based and conceptual approaches, which together account for more than two-thirds of the reviewed literature. In contrast, methodologies approximating real operational conditions namely testbed experimentation and field validation remain comparatively limited, with only 13 and 8 studies respectively. This asymmetry extends beyond a simple imbalance in methodological distribution, it fundamentally shapes both the nature of the evidence produced and the degree to which findings can be generalized across operational environments.

Simulation-based evaluation offers several clear advantages. It enables controlled experimentation, reproducibility and systematic comparison across multiple scenarios, which explains its dominant presence within the dataset (mean simulation score: 2.61/5). However, these advantages are closely tied to modeling assumptions that simplify real-world complexity, particularly regarding network behavior, infrastructure degradation, failure propagation and coordination dynamics. As a result, simulation-based methodologies primarily support analytical generalizability. They provide reliable insights within the boundaries of the modeled environment but remain limited in their ability to capture the

uncertainty, variability and operational unpredictability characteristic of real disaster conditions.

Conceptual studies contribute in a different yet complementary manner. Their strong representation reflects the broader effort within the field to structure complex communication problems, define architectural paradigms and integrate multiple analytical dimensions into unified system-level perspectives. This observation is further supported by the relatively high cross-disciplinary score observed across the dataset (3.64/5), indicating that many studies successfully connect technical design considerations with organizational, operational and policy-oriented dimensions. Nevertheless, in the absence of systematic empirical validation, these contributions largely remain within the domain of institutional or conceptual generalizability. In practical terms, they explain how systems are theoretically expected to operate, without fully demonstrating how such systems perform under realistic deployment conditions.

By comparison, testbed and field-oriented methodologies despite their comparatively limited representation play a disproportionately important role in strengthening the empirical foundation of the field. Testbed studies (mean score: 0.98/5) introduce implementation-level constraints such as hardware limitations, protocol interactions, synchronization overhead and timing behavior, thereby supporting stronger forms of technical generalizability. Field studies (mean score: 0.67/5), although relatively rare, constitute the only category capable of capturing the full operational complexity of real deployments, including infrastructure disruption, environmental uncertainty, human factors and multi-agency coordination dynamics. Their limited presence within the related literature therefore indicates that empirical generalizability remains the least mature dimension of current research.

Taken together, these findings reveal a broader structural imbalance in the way knowledge is currently produced and validated within disaster communication research. The field has developed substantial capabilities in simulation, conceptual modeling and analytical system design, yet the transition toward empirically grounded operational validation remains comparatively underdeveloped. This imbalance is further reflected in the overall methodological distribution and scoring profile:

- clear dominance of simulation-based and conceptual approaches (66.4% combined)

- consistently limited presence of testbed and field validation methodologies (below 20% combined)
- strong emphasis on cross-disciplinary framing without equivalent empirical depth

Collectively, this pattern suggests that the field has reached what may be described as a validation plateau. Although the related literature has clearly progressed beyond purely theoretical exploration and demonstrates significant methodological sophistication in terms of architectural design and analytical modeling, this maturity has not yet been systematically translated into large-scale operational validation. As a result, the field remains considerably stronger in generating analytical, conceptual and institutional insights than in producing empirically validated evidence under realistic disaster conditions.

For the purposes of this thesis, this observation constitutes the central interpretative axis of RQ1. Evaluation methodologies should not be viewed as neutral methodological preferences, rather, they directly determine the type, strength and scope of the generalizability that can ultimately be achieved. Simulation-oriented studies primarily support analytical claims, conceptual contributions reinforce institutional and architectural understanding, whereas only a relatively small subset of studies contributes to robust technical and empirical validation. As a result, the dominant methodological configuration of the field inherently constrains its capacity to produce fully generalizable and operationally validated communication solutions for real-world disaster environments.

4.3 Quantitative Analysis of Evaluation Methodologies

The quantitative examination of evaluation methodologies plays a central role in addressing RQ1, as it enables a structured and empirically grounded assessment of how current research validates communication solutions within man-made disaster environments. Based on a curated dataset of 107 distinct studies, this section examines not only the distribution of validation approaches but also their methodological characteristics and broader analytical implications. The analysis is organized around four principal dimensions simulation-based evaluation, testbed experimentation, field deployment and cross-disciplinary validation thereby supporting a systematic investigation of how different validation strategies influence the robustness, reliability and transferability of research outcomes [\[15\]](#), [\[20\]](#).

From a quantitative perspective, the results reveal a clear methodological imbalance across these dimensions. Simulation-oriented approaches constitute the dominant validation

mechanism throughout the related literature, reflecting their widespread adoption as scalable and comparatively accessible experimentation environments. In contrast, testbed-based validation appears substantially less frequent, while field-oriented evaluation remains relatively limited. At the same time, cross-disciplinary approaches are well represented, highlighting the growing tendency in contemporary research to integrate multiple technological and organizational domains, including AI, IoT infrastructures, edge computing, and policy-oriented coordination frameworks. Collectively, these findings indicate that although methodological diversity exists across the field, it remains unevenly distributed, with strong preference toward approaches emphasizing flexibility, abstraction and analytical tractability over empirical realism.

This distribution immediately reveals a broader structural asymmetry within the research landscape. While the conceptual and architectural sophistication of proposed communication solutions continues to increase, the corresponding depth of empirical validation does not keep pace. In practical terms, the field shows strong innovation at the design and modeling level, yet remains comparatively limited in operational verification and realistic deployment assessment. This imbalance establishes the foundation for a deeper investigation into the characteristics, strengths and methodological limitations associated with each evaluation paradigm.

Simulation-based validation represents the most prevalent methodological approach across the dataset, primarily due to its flexibility, scalability, reproducibility and cost-effectiveness. Simulation environments allow researchers to model complex communication scenarios under controlled conditions while evaluating performance metrics such as latency, throughput, packet-delivery ratio, network coverage and resource utilization. However, an important observation emerging from the analysis is that simulation-based validation should not be interpreted as a homogeneous methodological category. Instead, it constitutes a fragmented ecosystem encompassing multiple analytical and experimental paradigms.

This fragmentation is explicitly illustrated in Table 3, which summarizes representative simulation-oriented, analytical and data-driven evaluation environments. The table demonstrates that simulation-based validation spans several distinct subcategories, including standardized network simulators (e.g., OMNeT++), hybrid simulation environments integrating external cryptographic or optimization libraries, custom-built analytical and optimization models, formal mathematical formulations and dataset-driven

machine-learning evaluation frameworks. As a result, simulation-based validation within the related literature reflects not a single methodological tradition, but rather a broad spectrum of analytical practices operating at different levels of abstraction, realism and implementation complexity.

Study Type	Environment	Category	Metrics	Reproducibility
OMNeT++ Simulation [49]	Standard Simulator	Simulation	Delay/Throughput	High
NS2 + MIRACL[18]	Hybrid	Simulation	Execution Time	Low
ML UAV Optimization[50]	Custom Model	Custom	Fairness/Throughput	Low
Analytical Model[48]	Mathematical	Analytical	Latency/Blocking	Low
Dataset IDS[51]	Kitsune/5G- NIDD	Data-driven	Accuracy	Medium

Table 3 Simulation and Analytical Evaluation.

This methodological diversity introduces a fundamental challenge for the evaluation landscape. Although standardized simulation environments such as OMNeT++ provide relatively high levels of reproducibility, transparency and experimental consistency, a substantial portion of the related literature relies on custom-built or only partially specified simulation frameworks. These environments frequently exhibit limited reproducibility and reduced comparability across studies, making it difficult to establish consistent benchmarking conditions. At the same time, analytical models despite their mathematical rigor typically operate under highly simplified assumptions and therefore fail to capture broader system-level interactions and operational dynamics. Similarly, dataset-driven evaluation approaches, while effective for assessing specialized components such as intrusion-detection mechanisms or machine-learning classifiers, generally remain restricted to algorithm-level validation and do not adequately reflect full communication-system behavior under realistic disaster conditions.

From the perspective of RQ1, these observations carry important implications. Although simulation-based validation dominates the related literature, it does not necessarily produce uniformly generalizable findings. Instead, simulation-oriented studies often generate context-dependent results that remain strongly influenced by underlying assumptions, model configurations, traffic-generation strategies, environmental abstractions and dataset characteristics. As a result, the external validity of simulation-based research remains

inherently constrained, particularly when considering the heterogeneous, dynamic and unpredictable nature of real disaster environments.

In contrast, testbed-oriented and field-based validation approaches summarized in Table 4 provide a fundamentally different category of empirical evidence. These methodologies involve the deployment and assessment of communication systems within physically instantiated, semi-operational, or fully operational environments, ranging from embedded LoRa mesh infrastructures to large-scale 5G-enabled UAV architectures and integrated search-and-rescue coordination platforms. Unlike purely simulated environments, such approaches expose systems to real implementation constraints, environmental variability, hardware dependencies, timing uncertainties and operational coordination challenges that cannot be fully reproduced through abstract modeling alone.

System	Validation Type	Infrastructure	Generalizability	Complexity
LoRa Mesh	Testbed	Embedded Nodes	Technical	Low
SDN Multipath	Testbed (Hybrid)	ONOS, OVS, 5G	High	Medium-High
5G UAV Detection	Field	5G + UAV	Very High	High
X-IoCA SAR	Field	5G + MEC + Robotics	Very High	Very High

Table 4 Testbed and Field Validation.

Table 4 highlights three critical characteristics associated with empirical validation methodologies. First, these approaches achieve substantially higher levels of generalizability, particularly in field-deployment scenarios where real operational conditions are partially or fully represented. Second, they involve progressively increasing levels of system complexity, ranging from relatively contained testbed configurations, such as embedded-node deployments, to highly integrated environments combining 5G infrastructures, MEC, robotics, sensing platforms and human operators. Third, these methodologies require significant infrastructure availability, coordination effort and resource investment, directly affecting both their scalability and their frequency of adoption within the related literature.

These observations lead to an important structural insight: the limited prevalence of testbed-oriented and field-based studies is not incidental but rather reflects inherent constraints related to technical complexity, implementation cost and operational feasibility. Unlike

simulation-based approaches, which can be executed within controlled and scalable environments, empirical validation requires coordination across heterogeneous technological ecosystems, including communication infrastructures, computing platforms, sensing systems and, in many cases, human participants operating under realistic conditions. The multi-system nature of such environments substantially increases both implementation difficulty and operational overhead.

As a result, a fundamental trade-off emerges between validation realism and methodological feasibility. Simulation-based approaches provide scalability, flexibility and cost efficiency but remain constrained in terms of realism and external validity. Testbed-oriented methodologies offer improved implementation realism while still facing limitations related to scale, interoperability and environmental complexity. Field-based validation provides the strongest form of operational generalizability but remains exceptionally difficult to implement systematically in practice. This trade-off largely explains the observed dominance of simulation-oriented methodologies and the comparatively limited adoption of higher-realism validation approaches throughout the related literature.

Another important dimension emerging from the analysis concerns the prevalence of cross-disciplinary methodologies, which achieve the highest average score among all evaluation categories. This observation reflects the increasing integration of multiple technological and organizational domains within modern emergency communication systems. However, the analysis further reveals that this architectural and conceptual integration is not consistently accompanied by equivalent validation depth. Many studies propose sophisticated multi-domain architectures and orchestration frameworks while evaluating them through simplified, partially abstracted, or narrowly scoped validation environments. As a result, the practical generalizability of these integrated solutions often remains limited despite their conceptual sophistication.

Taken together, these findings suggest that the evaluation ecosystem within disaster communication research can be understood as a structured yet fundamentally imbalanced methodological landscape. Simulation-oriented methodologies dominate because of their practicality, scalability and accessibility, although they simultaneously suffer from fragmentation and limited standardization. In contrast, testbed and field-oriented approaches provide substantially higher levels of realism and operational generalizability but remain constrained by implementation complexity, infrastructure requirements and cost. Analytical

and data-driven methodologies contribute valuable theoretical and algorithmic insights, yet they generally remain restricted to partial, subsystem-level, or component-oriented validation.

From the perspective of RQ1, these observations lead to a clear evidence-based conclusion. The dominant evaluation methodologies within the field primarily simulation, analytical modeling and data-driven approaches enable controlled experimentation and scalable analytical exploration but impose important limitations on the generalizability of reported findings. Conversely, methodologies capable of providing stronger empirical evidence and higher operational realism, namely testbed and field-based validation approaches, remain significantly underutilized because of structural, technical and economic constraints.

4.4 Final Answer to RQ1

The analysis conducted in this study provides a clear and evidence-based answer to RQ1, addressing both the dominant evaluation methodologies used for validating communication solutions in man-made disaster scenarios and the extent to which these methodologies influence the generalizability of research findings.

First, regarding the dominant evaluation paradigms, the results demonstrate that simulation-based validation constitutes the prevailing methodological approach across the related literature. This dominance is primarily driven by the inherent advantages of simulation environments, including flexibility, scalability, cost efficiency, reproducibility and the ability to model complex communication scenarios under controlled conditions. Alongside simulation-oriented approaches, analytical modeling and data-driven methodologies particularly machine-learning-based evaluations and benchmark-dataset analyses are also widely employed, frequently serving as complementary mechanisms for assessing specific system components or isolated performance metrics. In contrast, testbed-oriented validation and field deployments remain significantly underrepresented despite their substantially greater potential for providing operationally grounded and empirically realistic evidence.

However, the findings extend beyond the simple identification of dominant methodologies and reveal a more fundamental structural issue within the evaluation landscape. Simulation-based validation should not be interpreted as a homogeneous or standardized methodological paradigm. Instead, it represents a fragmented ecosystem encompassing standardized simulation frameworks, custom-built computational environments, analytical abstractions, optimization-based models and dataset-driven evaluation pipelines. The

absence of methodological consistency across these approaches limits reproducibility, complicates cross-study comparability and reduces the cumulative integration of scientific knowledge. As a result, although simulation-based methodologies dominate the field quantitatively, their findings frequently remain highly context-dependent and difficult to generalize across heterogeneous disaster environments.

More importantly, the analysis demonstrates that the selection of evaluation methodology exerts a direct and decisive influence on the generalizability of research outcomes. Simulation-based and analytical methodologies, while highly effective for controlled experimentation, rapid prototyping and scalable analytical exploration, primarily support technical or analytical forms of generalizability. In other words, their conclusions generally remain valid within the assumptions, abstractions and constraints of the modeled environment. However, such methodologies often fail to capture the broader complexity, uncertainty, environmental variability and operational unpredictability associated with real-world disaster conditions.

By comparison, testbed-oriented and field-based validation methodologies provide substantially higher levels of empirical and institutional generalizability. By incorporating real hardware infrastructures, dynamic network conditions, physical deployment constraints, and, in some cases, human operators and inter-agency coordination processes, these approaches offer a considerably more realistic representation of operational system behavior. Nevertheless, their adoption remains limited because of high implementation complexity, multi-system integration requirements, infrastructure dependencies and substantial economic cost. These limitations directly constrain both scalability and methodological feasibility across large-scale research efforts.

Taken together, these findings reveal the existence of a fundamental structural trade-off between validation realism and practical feasibility. Simulation-oriented methodologies dominate because they remain scalable, accessible and comparatively cost-efficient, whereas high-realism validation approaches remain relatively scarce because they are operationally demanding and resource intensive. As a consequence, the related literature remains concentrated within intermediate levels of validation maturity, with only a limited number of studies progressing toward fully empirical and operationally realistic validation environments.

As a direct outcome of this imbalance, the analysis identifies a broader Generalizability Gap, defined as the discrepancy between the theoretically demonstrated performance of proposed communication solutions and their empirically validated behavior under realistic disaster conditions. This gap is driven primarily by two interconnected factors:

- (i) the fragmentation and limited standardization of simulation-based evaluation methodologies and
- (ii) the comparatively limited adoption of testbed-oriented and field-based validation approaches.

5. RQ2 Integration of Advanced Paradigms in Emergency Communication Systems

This chapter investigates how recent research integrates advanced technological paradigms into emergency communication systems, moving beyond isolated innovations toward cohesive and multi-layered communication architectures. Using a structured meta-analytical methodology, the study systematically examines a curated corpus of contemporary research through a multi-dimensional feature-extraction framework capturing paradigm type, integration depth, architectural role and operational maturity.

The analysis identifies five dominant paradigm categories: AI-native intelligent systems, resilient communication infrastructures, secure and trustworthy integration frameworks, cyber-physical mission-critical ecosystems and sustainable smart-city integration models. Quantitative findings reveal a clear transition toward multi-paradigm and system-of-systems architectures, with AI, MEC and NTN emerging as central technological enablers. Co-occurrence analysis further highlights recurring convergence patterns, including AI-MEC orchestration, UAV-NTN-enabled resilience, blockchain-secured unmanned-system coordination and IoT-digital twin cyber-physical integration.

The findings demonstrate that advanced paradigms are increasingly integrated across architectural, functional and operational dimensions, enabling adaptive, service-aware and resilient communication ecosystems. These integrated systems support real-time decision-making, maintain connectivity under degraded or infrastructure-disrupted conditions and facilitate coordinated sensing, orchestration and control within highly dynamic operational environments. At the same time, the analysis identifies important trade-offs associated with architectural complexity, cybersecurity, interoperability and resource management, emphasizing the need for balanced and operationally sustainable design strategies.

Overall, the chapter demonstrates that modern emergency communication systems are progressively evolving into intelligent and tightly integrated ecosystems unifying communication, computation, sensing and physical interaction within a common operational framework. In doing so, the analysis provides a comprehensive answer to the research question while simultaneously establishing a conceptual foundation for future system design, large-scale operational integration and emerging standardization efforts.

5.1 Methodological Framework

The present study adopts a structured meta-analytical framework to systematically investigate the integration of advanced technological paradigms within emergency communication systems. The dataset consists of a curated corpus of peer-reviewed studies collected and evaluated through an incremental analytical process. Each contribution was selected according to strict relevance criteria aligned with the research question, ensuring that it explicitly addresses the incorporation of at least one advanced technological paradigm within a communication architecture designed for mission-critical or disaster-related environments.

Unlike conventional survey-oriented approaches that primarily rely on descriptive aggregation, the dataset construction process follows a controlled inclusion strategy grounded in functional integration relevance. More specifically, studies were included only if they demonstrated the operational role of advanced paradigms such as AI, MEC, NTN, blockchain or cyber-physical components within an integrated communication-system architecture [25], [47], [52]. Purely theoretical works lacking system-level implications, as well as studies focusing exclusively on isolated protocol optimization without broader integration context, were excluded in order to preserve analytical consistency and architectural comparability across the dataset.

A defining characteristic of the dataset is its multi-domain heterogeneity, encompassing applications related to disaster response, public safety communications, search-and-rescue operations, smart-city infrastructures and military-grade communication systems [31]. This diversity enables a comprehensive examination of integration patterns across heterogeneous operational environments while maintaining a unified analytical perspective.

Importantly, the dataset also reflects the broader methodological limitations characterizing the field. Prior large-scale studies have demonstrated that validation practices in wireless communication research remain significantly imbalanced, with only a limited fraction of studies achieving complete validation pipelines and experimentally reproducible results. These limitations directly affect the interpretability and generalizability of reported findings. As a result, the present study deliberately shifts the analytical focus away from validation fidelity as the primary unit of assessment and instead emphasizes integration behavior and paradigm interaction as the central analytical perspective. This positioning enables the extraction of robust architectural and systemic insights even with heterogeneous and

partially non-reproducible validation methodologies, extending beyond traditional evaluation-centric analytical approaches.

To support systematic analysis, each study in the dataset was evaluated using a multi-dimensional feature-extraction framework specifically designed to capture the role, interaction and integration depth of advanced paradigms within communication systems. The framework is implemented through a structured data schema in which each study is encoded across a standardized set of analytical attributes.

At the core of the framework lies the identification of technological paradigms. Each study is annotated using a multi-label representation covering major technological domains, including AI and machine learning, ISAC, UAV, NTN, MEC, blockchain, IoT and cyber-physical systems (CPS), digital twins, robotics, security mechanisms, network slicing and SDN/NFV architectures [40], [53]. This approach enables the simultaneous capture of both dominant and supporting technological paradigms within each contribution.

In addition to paradigm identification, the framework quantifies the level of technological integration. This is achieved by examining the number and interaction of coexisting paradigms within each study and mapping them onto an integration scale distinguishing between single-paradigm solutions, multi-paradigm integrations and broader system-of-systems architectures. This dimension is particularly important for determining whether a contribution represents an isolated technological enhancement or participates in a coordinated and intelligent communication ecosystem.

The architectural role of each contribution is further characterized through mapping to specific system layers, including physical infrastructure, network mechanisms, system-level orchestration, application-layer functionality and cross-layer architectural designs. This classification supports identifying where integration occurs within the communication stack while also enabling analysis of inter-layer dependencies and orchestration behavior.

Operational maturity constitutes another major analytical dimension. Each study is categorized according to its validation level, ranging from conceptual proposals and simulation-based analyses to prototype implementations and real-world operational deployments. This distinction differentiates emerging conceptual approaches from practically validated communication architectures.

To capture the degree of intelligence and security embedded within each system, additional analytical indices are introduced. The AI integration index reflects the depth of embedded

intelligence, ranging from basic machine-learning assistance to fully autonomous and adaptive decision-making systems. Similarly, the security index quantifies the presence and sophistication of protection mechanisms, including intrusion-detection systems, cryptographic frameworks, trust-management architectures and blockchain-enabled security mechanisms. Finally, each study is annotated according to its target application domain, including disaster response, public safety operations, smart-city services, search-and-rescue coordination and military communication scenarios. This dimension enables the contextual interpretation of technological choices within distinct operational environments. Building upon these extracted features, the study introduces a formalized scoring framework designed to evaluate the relative contribution and architectural significance of each research work. Unlike traditional evaluation metrics primarily centered on performance outcomes, the proposed framework focuses on integration quality, systemic coordination and architectural convergence, thereby providing a more appropriate analytical basis for examining paradigm interaction within emergency communication systems. Each study is evaluated across five core dimensions:

- **Integration Depth (D_1):** Measures the degree to which identified paradigms are structurally embedded within the system, distinguishing between superficial inclusion and tightly coupled architectures.
- **System-Level Integration (D_2):** Assesses whether the contribution operates at component level or proposes a coordinated, end-to-end system architecture.
- **Operational Relevance (D_3):** Captures the applicability of the proposed solution to real-world emergency or mission-critical scenarios.
- **Validation Strength (D_4):** Reflects the robustness of the evaluation methodology, incorporating simulation fidelity, experimental validation and deployment realism.
- **Cross-Paradigm Synergy (D_5):** Quantifies the extent to which multiple paradigms interact to produce emergent system capabilities.

Each dimension is normalized on a bounded scale:

$$D_i \in [0,5], i = 1, ..$$

The aggregate score SS for each study is computed as a weighted combination:

$$S = \sum_{i=1}^5 w_i \cdot$$

Where w_i represents the relative importance of each dimension. In the absence of domain-specific bias, equal weighting is initially assumed:

$$w_i = 0.2,$$

However, the framework remains extensible and allows adaptive weighting in future analytical extensions, enabling emphasis on specific perspectives such as system-level orchestration, operational realism, or validation maturity.

An important refinement of the scoring methodology concerns the controlled influence of validation strength. Given the well-documented reproducibility limitations associated with experimental communication-system research where only a limited fraction of studies provide fully replicable results the contribution of D_4 is intentionally bounded to prevent disproportionate weighting of potentially non-reproducible experimental claims. This adjustment ensures that studies are evaluated primarily according to their architectural, systemic and functional contributions rather than solely on the perceived sophistication of their validation environments.

Based on the aggregate score, studies are categorized into three tiers:

- **Flagship Contributions ($S \geq 4.0$):** Represent fully integrated, high-impact architectures with strong cross-paradigm synergy.
- **Core Contributions ($2.5 \leq S < 4.0$):** Provide substantial advancements within specific integration dimensions.
- **Supporting Contributions ($S < 2.5$):** Offer conceptual, domain-specific, or incremental insights.

This classification enables a structured interpretation of the dataset while supporting both quantitative ranking and qualitative synthesis. This structured representation also enables statistical aggregation techniques to identify broader trends in paradigm integration. The analysis operates across multiple dimensions, including paradigm frequency, integration complexity, architectural distribution, operational maturity and domain-specific deployment characteristics. A central component of the analysis involves the identification of co-occurrence patterns, defined as the joint presence of multiple paradigms within the same study. These patterns are represented through a co-occurrence matrix in which each entry

captures the frequency with which two paradigms appear together. This representation enables the identification of dominant integration clusters and reveals recurring technological convergence patterns across the related literature.

In parallel, integration complexity is examined through analysis of the number of paradigms embedded within individual studies. This enables identification of broader systemic transitions, including the evolution from isolated technological solutions toward coordinated multi-paradigm ecosystems and system-of-systems architectures. Architectural distribution is evaluated by aggregating across system layers, identifying the dominant loci of integration within the communication stack. This analysis reveals whether integration primarily occurs at infrastructure level, within orchestration mechanisms, or at the application layer.

Operational maturity is incorporated as a secondary aggregation dimension, providing additional insight into the developmental trajectory of the field. However, consistent with the methodological positioning of the study, maturity is interpreted alongside integration characteristics rather than as an isolated indicator of contribution quality.

Collectively, these aggregation techniques support a comprehensive quantitative characterization of the dataset and establish the empirical foundation for the taxonomy structures and convergence patterns developed throughout the following sections.

Despite its structured design, the proposed methodology remains subject to several limitations. First, the classification and scoring processes involve a degree of expert judgment, particularly in the assignment of paradigm roles, integration depth and cross-paradigm synergy. Although predefined analytical criteria are employed to maintain consistency, some level of interpretative subjectivity remains unavoidable in qualitative meta-analysis.

Second, although extensive, the dataset is not exhaustive and remains constrained by the selected literature corpus analyzed within the study. As a result, emerging contributions or highly specialized domain-specific works may not be fully represented. This limitation is inherent to all large-scale meta-analytical approaches and is partially mitigated through the diversity and breadth of the selected dataset.

Third, the abstraction of complex communication-system architectures into discrete analytical categories and numerical scores necessarily introduces a degree of simplification.

While this abstraction is required for comparative analysis, it may not fully capture nuanced architectural distinctions, particularly within highly heterogeneous or experimental systems. Finally, the broader research landscape itself remains constrained by persistent issues related to validation realism and reproducibility. Experimental studies frequently rely on custom-built testbeds with limited reproducibility, while simulation-based approaches cannot fully capture the uncertainty and operational variability of real-world disaster conditions. These limitations affect the interpretability of validation outcomes and further reinforce the need for alternative analytical perspectives centered on integration behavior and systemic convergence rather than evaluation methodology alone.

5.2 Taxonomy of Advanced Paradigms

Building upon the methodological framework introduced in Section 5.1, this section develops a comprehensive taxonomy of the advanced paradigms integrated within emergency communication systems. Unlike conventional classifications that merely enumerate technological domains, the proposed taxonomy is derived directly from the structured scoring and feature-extraction process applied to the RQ2 dataset. As a result, the taxonomy reflects measurable patterns of paradigm presence, architectural integration, operational relevance and cross-paradigm synergy rather than subjective or purely descriptive categorization.

The dataset currently consists of 107 studies, of which 80 have been fully evaluated across the five core analytical dimensions, while 79 include complete maturity characterization. Although the dataset remains under incremental refinement, the size and diversity of the scored subset are sufficient to reveal statistically stable and analytically meaningful trends. The taxonomy presented in this section can therefore be considered both data-driven and broadly representative of the current research landscape.

The quantitative analysis demonstrates that paradigm integration is not uniformly distributed across the related literature. Instead, the field exhibits a clear hierarchical structure in which certain paradigms function as foundational architectural enablers, whereas others operate as complementary, domain-specific, or specialized integration components [25], [54]. This hierarchical organization reflects the broader evolution of emergency communication systems from isolated technological solutions toward coordinated and layered communication ecosystems.

The dominant technological family within the dataset is associated with 5G/6G infrastructures, PPDR systems and mission-critical communication architectures, appearing in approximately 57.9% of the analyzed studies. This finding confirms that next-generation mobile communication infrastructures now constitute the primary architectural backbone of modern emergency communication systems [17], [31], [54]. These technologies provide the foundational connectivity layer enabling URLLC, network slicing, service prioritization and adaptive support for mission-critical traffic management.

The second most prevalent category includes IoT, wireless sensor network (WSN) and sensing-oriented systems, appearing in approximately 36.4% of the dataset. These paradigms collectively form the data-acquisition and environmental-awareness layer of modern emergency communication architectures, enabling real-time monitoring, infrastructure assessment, distributed sensing and situational-awareness generation. Their strong presence reflects the increasing transition toward data-centric and context-aware operational decision-making processes.

AI and machine-learning paradigms appear in approximately 27.1% of the analyzed studies. This observation is particularly important because it reflects the ongoing transition from static communication infrastructures toward adaptive, intelligent and partially autonomous communication ecosystems. AI-driven approaches are increasingly employed for network optimization, anomaly detection, predictive analytics, autonomous orchestration and decision-support functions operating across multiple system layers [50], [55].

MEC and cloud-oriented paradigms appear in approximately 24.3% of the dataset. These technologies enable distributed computational capabilities closer to the operational environment, thereby reducing latency, improving responsiveness and supporting localized decision-making processes. Their role becomes especially critical in emergency scenarios where centralized infrastructure may be degraded, unavailable, or operationally unreliable. UAV-enabled and drone-assisted communication systems [23], [49], [57] appear in approximately 22.4% of the analyzed studies. These paradigms provide highly flexible and rapidly deployable communication platforms capable of restoring connectivity, extending network coverage and supporting temporary infrastructure deployment within disaster-affected environments. Their growing integration highlights the increasing importance of mobility, spatial adaptability and dynamic topology management within modern emergency communication architectures.

More specialized technological paradigms include NTN, satellite, and SAGIN architectures [58], [59], together with security-oriented mechanisms, each appearing in approximately 14.0% of the dataset. These technologies extend the capabilities of conventional terrestrial networks by providing alternative connectivity mechanisms in scenarios where existing communication infrastructure is damaged, overloaded, or unavailable. In particular, the integration of terrestrial, aerial, and satellite communication layers contributes to broader coverage and greater architectural flexibility, which are especially important in geographically dispersed or infrastructure-constrained disaster environments.

Blockchain-based trust frameworks account for approximately 8.4% of the studies. Although less frequently represented, these approaches address important requirements related to decentralized trust, secure information exchange, data integrity, and coordination among multiple entities operating within heterogeneous emergency-response ecosystems. Similarly, SDN/NFV architectures and network-slicing mechanisms appear in approximately 9.3% of the dataset. Their presence reflects growing interest in programmable and dynamically configurable network infrastructures capable of adapting communication resources and services according to changing operational requirements and mission-critical priorities.

Finally, digital twin, CPS, and robotics-oriented paradigms appear in approximately 6.5% of the corpus. These technologies introduce additional capabilities for system monitoring, modeling, automation, and interaction between physical and digital environments. Their integration may support improved situational awareness, coordinated decision-making, and more adaptive management of complex emergency operations.

Although these specialized paradigms remain comparatively less frequent than more established technologies, their role is strategically significant. Collectively, they contribute to enhancing network resilience, distributed trust, orchestration flexibility, system security, and coordinated operational control. Their presence also indicates a broader evolution of emergency communication research toward increasingly heterogeneous, programmable, and interconnected architectures capable of supporting highly dynamic and demanding disaster-response environments.

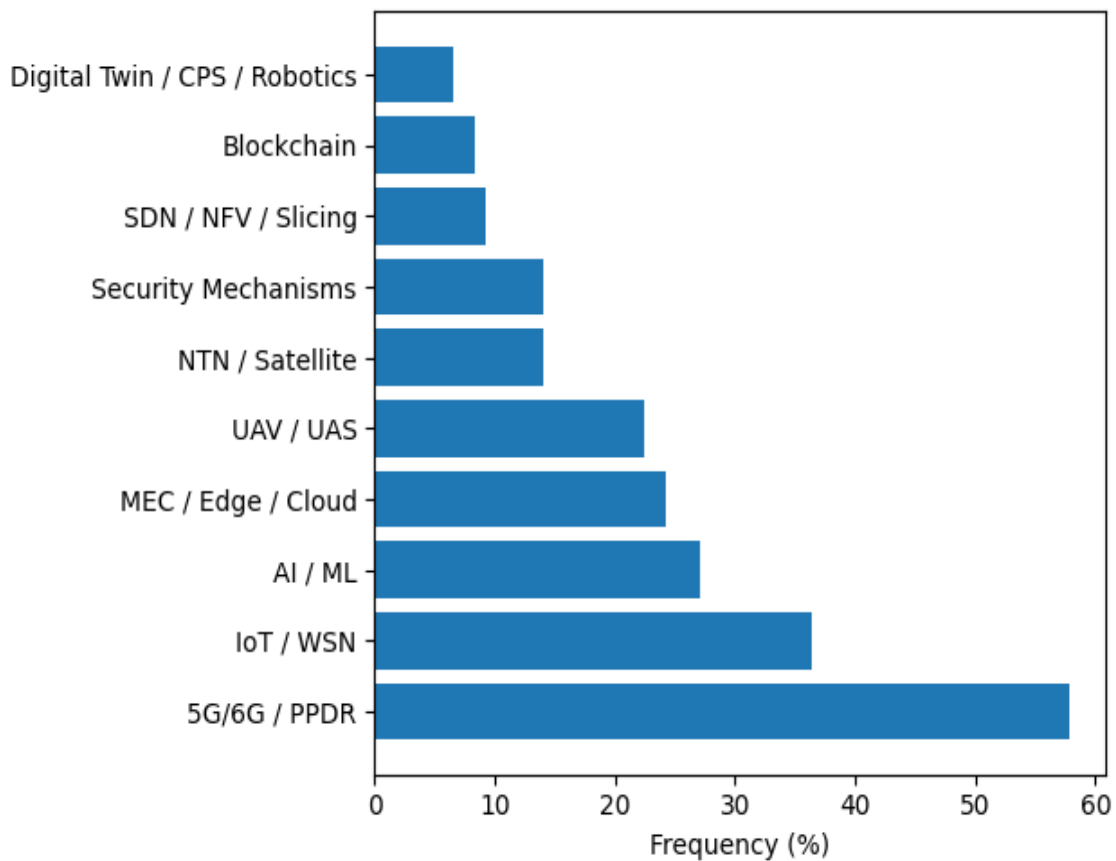


Figure 30 Frequency Distribution in RQ2 Dataset.

Figure 30 illustrates the frequency distribution of advanced paradigms across the RQ2 dataset, providing a quantitative overview of the contemporary technological landscape within emergency communication research. The figure clearly confirms the dominance of 5G/6G-oriented architectures, which significantly exceed all other paradigm categories in terms of frequency. This observation indicates that modern emergency communication systems are increasingly structured around next-generation connectivity infrastructures serving as the primary architectural backbone for paradigm integration. Rather than operating as isolated communication technologies, these infrastructures function as foundational integration platforms upon which additional intelligent, distributed and adaptive capabilities are deployed.

A second cluster of paradigms including IoT/WSN systems, AI/ML mechanisms, MEC and UAV-assisted communication architectures forms a dense intermediate tier with frequencies ranging approximately between 20% and 40% of the dataset. Collectively, this cluster represents the functional and operational core of integrated emergency communication ecosystems. Each paradigm contributes a distinct systemic capability: IoT and WSN

infrastructures provide distributed sensing and environmental awareness, AI/ML paradigms enable intelligent orchestration and predictive decision-making, MEC architectures support low-latency distributed computation, while UAV-enabled systems introduce mobility, spatial adaptability and rapidly deployable connectivity.

The lower-frequency paradigms including blockchain-based trust frameworks, SDN/NFV architectures and digital-twin-oriented systems form a more specialized integration layer primarily associated with enhancing security, programmability, virtualization, orchestration flexibility and simulation-driven operational awareness. Although these paradigms appear less frequently across the dataset, they are often associated with comparatively higher integration-complexity scores, suggesting that their architectural impact is disproportionately significant relative to their quantitative representation within the related literature.

Taken together, the figure demonstrates that modern emergency communication systems are no longer organized around a single dominant technological paradigm. Instead, they increasingly emerge as layered and interdependent ecosystems in which multiple paradigms interact to provide complementary operational capabilities. This transition reflects a broader shift from isolated communication infrastructures toward integrated, intelligent and system-of-systems architectures capable of supporting adaptive coordination, resilient connectivity and distributed operational decision-making under highly dynamic disaster conditions.

5.3 Functional Taxonomy of Advanced Paradigms

Building upon the statistical analysis and paradigm distribution presented in the previous sections, this subsection develops a functional taxonomy of advanced paradigms integrated within emergency communication systems. The objective is not to classify technologies according to their standalone characteristics, but rather to organize them based on their operational role within complex and interconnected communication architectures.

The taxonomy is derived directly from the RQ2 dataset and reflects observed patterns of technological integration, paradigm co-occurrence and system-level contribution. Consequently, it captures how paradigms operate within real architectural ecosystems rather than how they are described in isolation at conceptual level. This distinction is particularly important because modern emergency communication systems are increasingly shaped by interactions across multiple technological layers rather than by the isolated behavior of individual components.

A central observation emerging from the dataset is that high-maturity communication systems rarely depend on a single technological paradigm. Instead, advanced architectures increasingly integrate multiple complementary technologies to address the diverse operational requirements of disaster and mission-critical environments. These requirements include resilient and continuous connectivity, distributed computation, intelligent resource orchestration, environmental sensing, adaptive coordination, and security assurance. The combination of these capabilities enables communication systems to respond more effectively to rapidly changing conditions, infrastructure disruption, heterogeneous network resources, and fluctuating service demands.

This convergence-oriented design pattern reflects a broader transition from isolated and technology-specific communication infrastructures toward integrated system-of-systems communication ecosystems. Within these environments, individual technologies are no longer considered independent solutions but rather interconnected components that contribute different capabilities to the overall architecture. For example, communication, computing, sensing, and orchestration mechanisms may operate jointly to improve network adaptability, situational awareness, resource allocation, and service continuity. Consequently, technological convergence becomes an important architectural principle for supporting the complexity and dynamic nature of modern emergency-response operations. As a result, the proposed taxonomy is structured around five functional categories, each representing a distinct architectural and operational role within the broader communication ecosystem. This functional organization provides a systematic framework for examining how different technological paradigms contribute to specific communication requirements while also identifying their relationships within integrated architectures. Rather than functioning as mutually exclusive classes, these categories frequently interact and overlap, reflecting the inherently heterogeneous nature of modern emergency communication systems.

Collectively, the five categories illustrate how different technological capabilities can be combined to support adaptive, resilient, secure, and intelligent emergency communication environments. The taxonomy therefore captures not only the individual contribution of each technological paradigm but also the increasing importance of their functional integration within next-generation disaster communication architectures.



Figure 31 Functional Taxonomy of Paradigms. Source: Author's own analysis and functional taxonomy derived from the systematic review dataset (RQ2).

5.3.1 AI-Native Intelligent Communication Systems

The first functional category concerns AI-native intelligent communication systems. Within the current dataset, AI/ML-related paradigms appear in approximately 27.1% of the analyzed studies. Although this does not position AI as the most numerically dominant paradigm, its architectural influence extends far beyond simple frequency representation. AI emerges as one of the most transformative elements in the evolution of modern emergency communication systems because, unlike traditional communication technologies operating as isolated functional modules, it functions as a pervasive enabling layer embedded across multiple architectural components. Through this role, AI supports network optimization, predictive analytics, autonomous decision-making, adaptive resource management and intelligent orchestration, fundamentally redefining how emergency communication systems behave under dynamic and uncertain operational conditions [50], [60], [61].

The scored dataset strongly supports this interpretation. Studies integrating AI-related paradigms consistently achieve high scores within the innovation and cross-paradigm synergy dimension, with an average value of approximately 3.94/5 across the evaluated corpus. This observation is not incidental, rather, it reflects a defining characteristic of AI-

native architectures. AI is rarely deployed as an isolated subsystem. Instead, it is typically embedded within broader communication ecosystems and integrated alongside complementary paradigms such as MEC, UAV-assisted networking, IoT sensing infrastructures, network-slicing mechanisms and cloud-oriented orchestration frameworks. Within these architectures, AI effectively operates as the cognitive layer of the communication system. It interprets environmental and network conditions, predicts demand patterns, detects anomalies, dynamically allocates resources and supports mission-level decision-making processes under rapidly evolving operational constraints.

A particularly important conceptual distinction emerging from the dataset is the difference between algorithmic AI and architectural AI. Algorithmic AI refers to the application of machine-learning techniques for solving narrowly scoped operational tasks, including traffic prediction, signal classification, congestion estimation, or disaster-event detection. While operationally valuable, this form of AI does not fundamentally alter the architecture of the communication system itself. Architectural AI, by contrast, is deeply embedded in the system's control and orchestration logic. It directly influences how communication infrastructures react, adapt, coordinate and evolve in response to changing environmental and operational conditions. This distinction is especially important for addressing RQ2 because the chapter's analytical focus is system-level integration rather than isolated performance optimization. Through architectural AI, communication infrastructures evolve from static and preconfigured entities into adaptive, context-aware and partially autonomous communication ecosystems.

This capability becomes particularly critical within disaster response and mission-critical operational environments. Emergency communication systems function under conditions characterized by uncertainty, instability, infrastructure degradation and rapidly shifting operational priorities. Communication demand may fluctuate unpredictably, network infrastructure may be partially damaged or entirely unavailable and mission requirements may evolve in real time. Under such conditions, static communication models become operationally insufficient. AI-native systems address these limitations by introducing adaptive and self-organizing mechanisms, including predictive resource allocation, automated service prioritization, intelligent routing strategies, anomaly-detection frameworks and self-healing network behaviors capable of recovering from failures without continuous human intervention.

The integration of AI with complementary paradigms further amplifies its systemic impact. When integrated with MEC [62], [63], AI models can be deployed closer to the operational environment, thereby reducing latency and enabling real-time decision-making at the network edge an essential capability when centralized cloud infrastructure becomes inaccessible or unreliable. When integrated with UAV/UAS platforms [64]. AI enables trajectory optimization, relay positioning, adaptive coverage management and intelligent handover coordination. Within NTN environments. AI contributes to dynamic link selection, adaptive backhaul optimization and intelligent routing across heterogeneous communication layers. These integration patterns are explicitly illustrated in Figure 31, which presents the co-occurrence relationships between AI and other technological paradigms across the dataset [60].

The figure demonstrates that the strongest associations emerge between AI and 5G-oriented communication infrastructures, followed closely by AI integration with MEC and IoT ecosystems. This observation confirms that AI is primarily embedded within high-capacity communication environments and data-intensive sensing architectures. The comparatively strong co-occurrence between AI and UAV-enabled systems further highlights the role of AI in supporting mobility-aware, adaptive and topology-dynamic communication strategies. By contrast, the comparatively lower frequency of AI integration with security-oriented mechanisms suggests that, although AI possesses substantial potential within this domain, its convergence with trust-management and cybersecurity architectures remains comparatively less mature across the current research landscape.

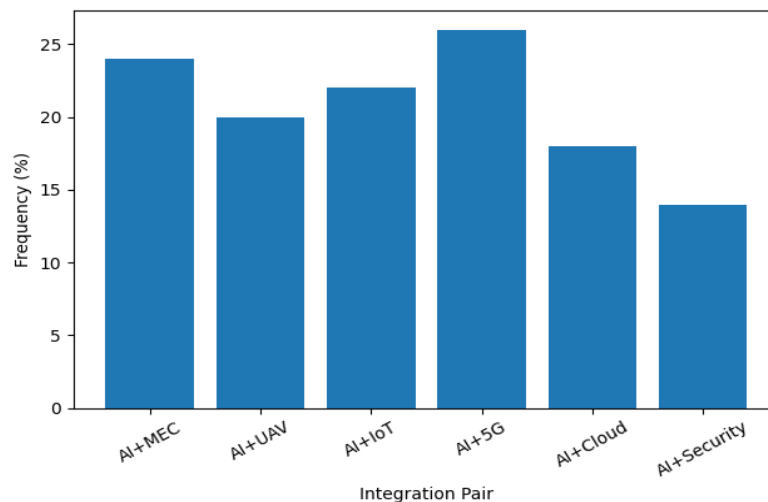


Figure 32 AI Co-occurrence Patterns in RQ2 Dataset.

The interpretation of Figure 32 reinforces a central insight emerging from the dataset: AI does not operate as an isolated technological component but rather as a coordination and orchestration mechanism spanning multiple layers of the communication architecture. Its strongest interactions occur with paradigms that either provide large-scale contextual data input, such as IoT and sensing infrastructures, or supply distributed computational support, such as MEC and cloud-oriented platforms. This integration behavior confirms that AI functions as a unifying architectural layer linking sensing, computation and communication into a coherent and adaptive operational ecosystem.

Consequently, AI-native communication systems should not be interpreted merely as communication platforms that incorporate machine-learning functionality. Such an interpretation would significantly underestimate their broader architectural significance. Their primary contribution lies in enabling the transition from manually configured and statically managed communication infrastructures toward adaptive, context-aware and partially autonomous emergency communication ecosystems. These systems are capable of continuously learning from environmental and operational conditions, anticipating evolving demands, dynamically reallocating resources and adapting communication behavior in response to changing mission requirements.

This transformation represents a fundamental shift in the design philosophy of emergency communication systems. Traditional communication architectures are primarily reactive, operating according to predefined configurations and static optimization policies. By contrast, AI-native architectures introduce proactive and intelligent operational behavior capable of functioning effectively under uncertainty, infrastructure degradation and rapidly changing environmental conditions. In this sense, AI no longer acts solely as an auxiliary optimization mechanism but increasingly becomes embedded within the core operational logic of the communication ecosystem itself.

As a result, AI-native systems are a foundational pillar of next-generation emergency communication design and play a central role in the broader paradigm-convergence landscape examined throughout this chapter. More broadly, their emergence reflects the ongoing transition from communication-centric infrastructures toward intelligent and self-adaptive operational ecosystems integrating connectivity, computation, sensing, orchestration and autonomous decision-making within a unified architectural framework.

5.3.2 Resilient Communication Infrastructures

The second functional category concerns resilient communication infrastructures. This category represents the most quantitatively dominant component of the proposed taxonomy, encompassing a broad spectrum of paradigms including 5G/6G architectures, PPDR communication systems, MEC, UAS, NTN, SDN, network slicing, multi-connectivity mechanisms and deployable communication infrastructures. Within the current dataset, 5G/6G and PPDR-oriented architectures appear in approximately 57.9% of the analyzed studies, confirming that next-generation mobile communication systems constitute the primary technological backbone of contemporary emergency communication research.

In this context, resilience extends far beyond conventional notions of redundancy [\[47\]](#), [\[48\]](#). Rather than representing a single technical capability, resilience should be understood as a systemic architectural property describing the ability of a communication ecosystem to maintain, restore, adapt, or dynamically reconfigure operational services under degraded, uncertain, or rapidly evolving conditions. Such conditions may include infrastructure destruction, network congestion, partial connectivity loss, environmental instability, or continuously changing mission requirements. Consequently, resilience emerges through the coordinated interaction of multiple architectural mechanisms, including adaptive resource allocation, service prioritization, distributed processing, flexible deployment strategies, alternative backhaul solutions, aerial relay infrastructures and programmable network orchestration.

A central component of this category involves the integration of mobile edge computing, edge-oriented architectures and cloud-based infrastructures, which collectively appear in approximately 24.3% of the dataset. Their importance derives from relocating computational and orchestration capabilities closer to the operational environment. In emergency scenarios, strict latency constraints and unstable connectivity may render centralized cloud processing insufficient. Edge-oriented paradigms address these limitations through localized data processing, real-time analytics, distributed intelligence and low-latency decision-making with reduced dependence on distant core-network infrastructure [\[56\]](#), [\[62\]](#). This enables communication systems to maintain operational continuity even when connectivity to centralized services becomes degraded or unavailable.

Closely associated with this capability is the integration of UAV/UAS-enabled and drone-assisted communication systems, appearing in approximately 22.4% of the studies analyzed.

These paradigms provide deployable and topology-adaptive communication nodes capable of rapidly extending or restoring connectivity in disaster-affected environments, particularly when terrestrial infrastructure is damaged or inaccessible. UAV-based platforms may operate as aerial base stations, relay nodes, distributed sensing units or temporary communication backbones [23], [49], [65]. Their effectiveness can be further enhanced through integration with 5G/6G, edge computing, AI and non-terrestrial communication architectures.

Non-terrestrial networking paradigms, including satellite communication systems and SAGIN architectures, appear in approximately 14.0% of the dataset. Although less frequent than terrestrial infrastructures, they remain strategically important. These paradigms extend connectivity to remote regions, maritime environments and large-scale disaster zones where terrestrial infrastructure may be compromised. They also provide alternative communication pathways during terrestrial-network failures, contributing to system resilience, continuity and survivability [58], [66].

Figure 33 illustrates the distribution and interaction of the principal technological components supporting resilient communication infrastructures across the analyzed dataset.

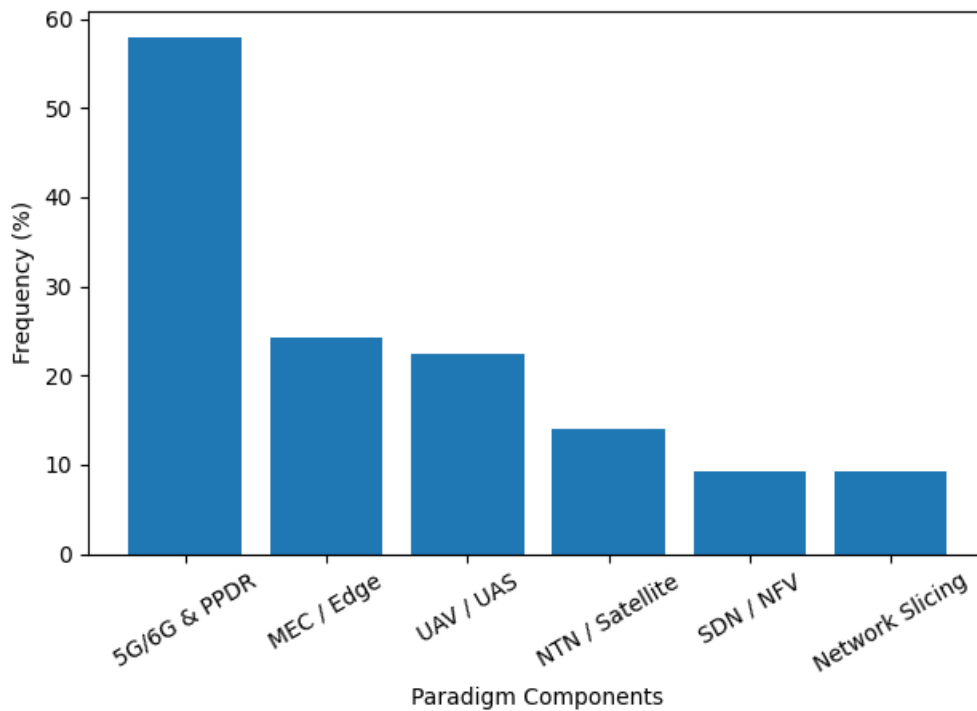


Figure 33 Resilient Communication Infrastructure Components in RQ2 Dataset.

The figure clearly illustrates the dominance of 5G/6G and PPDR-oriented architectures, which significantly exceed all other components in terms of frequency. This observation confirms that resilience in modern emergency communication systems is fundamentally anchored in advanced mobile communication infrastructures. These technologies form the primary connectivity substrate upon which adaptive and mission-critical communication capabilities are constructed. The second tier of components, including MEC/edge paradigms and UAV-enabled systems, forms a strong supporting layer that enhances deployment flexibility, distributed intelligence and operational adaptability. Their comparatively high frequency indicates that resilience is increasingly achieved through decentralization, mobility and dynamic orchestration rather than through static infrastructure redundancy alone.

Lower-frequency paradigms such as NTN, SDN/NFV architectures and network-slicing mechanisms occupy a more specialized yet strategically important role within the overall ecosystem. SDN and NFV introduce programmability, virtualization and centralized orchestration capabilities into the communication infrastructure, enabling rapid network reconfiguration, adaptive traffic management and more efficient resource utilization under dynamic operational conditions [\[34\]](#), [\[35\]](#), [\[36\]](#). Network slicing further supports the isolation and prioritization of mission-critical services, ensuring that essential communication flows remain operational even during severe congestion or partial infrastructure degradation [\[67\]](#). Although these paradigms appear less frequently across the dataset, their integration is typically associated with substantially higher levels of architectural sophistication and systemic coordination.

The relatively high average score associated with architectural and system-level integration approximately 3.96/5 further reinforces the interpretation of resilience as a systemic architectural property rather than a standalone technical mechanism. Across the related literature no longer focuses primarily on isolated backup links or conventional redundancy models. Instead, it increasingly proposes layered, heterogeneous and multi-domain communication ecosystems combining terrestrial, aerial, edge and satellite infrastructures into coordinated operational environments. This layered architectural approach enables multiple forms of redundancy, adaptability and service continuity, allowing communication systems to respond dynamically to a broad spectrum of failure scenarios and operational disruptions.

An important implication emerging from this observation is that resilience cannot be achieved through any single technological paradigm operating independently. Instead, resilient behavior emerges through the coordinated interaction of multiple complementary technologies, each contributing distinct operational capabilities. For example, 5G-oriented infrastructures provide high-capacity and low-latency connectivity, UAV platforms offer deployment flexibility and dynamic topology extension, edge-computing systems enable localized intelligence and low-latency processing, while satellite and NTN architectures ensure extended coverage and alternative communication pathways. The coordinated integration of these paradigms results in communication ecosystems that are not only robust, but also adaptive, scalable and operationally survivable under highly uncertain conditions. Within the broader taxonomy developed in this chapter, resilient communication infrastructures therefore constitute the foundational structural backbone upon which all other advanced paradigms depend. Without resilient communication capabilities, the functionality of higher-level paradigms becomes significantly constrained. AI cannot operate effectively without stable and continuous data flows, IoT ecosystems cannot reliably transmit sensing information, digital twins cannot maintain synchronization with the physical environment and trust-management or security mechanisms cannot adequately protect communication channels under degraded conditions. Resilience thus operates as the enabling substrate supporting the broader convergence of communication, computation, sensing, orchestration and autonomous coordination mechanisms.

In summary, the analysis demonstrates that resilience is progressively evolving from a supplementary system characteristic into a central design principle of next-generation emergency communication systems. The transition toward integrated and multi-layered infrastructures reflects both the increasing complexity of operational environments and the growing demand for communication ecosystems capable of maintaining functionality under uncertainty, infrastructure degradation and rapidly changing mission conditions. Consequently, resilient communication infrastructures occupy a central role in enabling the broader paradigm convergence patterns observed throughout the RQ2 dataset and represent one of the defining architectural foundations of future emergency communication ecosystems.

5.3.3 Secure and Trustworthy Integration Frameworks

The third functional category concerns secure and trustworthy integration frameworks. Security-oriented paradigms appear in approximately 14.0% of the analyzed dataset, while blockchain-based and trust-oriented frameworks account for approximately 8.4% of the studies. Although these frequencies remain lower than those associated with 5G/6G infrastructures, IoT ecosystems, AI, or UAV-enabled communication systems, their architectural significance should not be underestimated. Security and trust mechanisms rarely emerge as isolated dominant paradigms, instead, they become critically important within highly integrated communication ecosystems where multiple systems, organizations, autonomous agents and data flows interact under uncertain and potentially adversarial conditions.

Emergency communication systems should not be interpreted solely as technical networking infrastructures. They are operational ecosystems supporting mission-critical activities involving public safety agencies, emergency-response organizations, governmental authorities, critical infrastructure operators, military units and increasingly autonomous or semi-autonomous systems. Within such environments, communication availability alone is insufficient to guarantee operational effectiveness. Confidentiality, integrity, authentication, access control, trust management and coordination assurance become equally essential system requirements. A communication system that remains operationally available but lacks trustworthiness may become functionally unusable or even operationally dangerous in practice. Compromised communication channels, for example, may result in misinformation propagation, coordination failures, malicious interference, or unauthorized manipulation of rescue and response operations.

The proposed taxonomy distinguishes three progressive levels of security integration, each corresponding to increasing degrees of architectural maturity and systemic complexity. The first level consists of foundational security mechanisms, including encryption schemes, authentication protocols, identity management systems and access-control frameworks [68], [69]. These mechanisms form the baseline protection layer implemented across most communication infrastructures. Their primary role is to secure data transmission, prevent unauthorized access and maintain basic communication integrity. Although indispensable, these mechanisms are typically static in nature and generally lack the capacity to adapt

dynamically to evolving threats, changing operational conditions, or sophisticated adversarial behavior.

The second level introduces intelligent and adaptive security mechanisms incorporating AI and machine-learning techniques into cybersecurity processes. Systems within this category are capable of detecting anomalies, identifying potential intrusions, recognizing abnormal behavioral patterns and responding to emerging threats in near real time. AI-driven intrusion-detection systems, anomaly-recognition frameworks and adaptive threat-analysis mechanisms fall within this category. Their primary advantage lies in their ability to operate effectively under uncertainty and adapt to previously unseen attack patterns. This capability becomes particularly important in emergency communication environments, where operational conditions frequently deviate from predefined behavioral baselines and where static security models may prove insufficient [\[51\]](#).

The third level represents system-level trust architectures in which security is embedded directly into the operational logic and coordination structure of the communication ecosystem itself. This level includes blockchain-based solutions, distributed ledger technologies, zero-trust architectures, decentralized identity-management systems and distributed trust-coordination frameworks. At this stage, trust is no longer enforced exclusively through centralized control entities. Instead, trust relationships become distributed across the communication ecosystem, enabling multiple organizations and autonomous actors to coordinate securely without requiring complete reliance on a single trusted authority. Such architectures are particularly relevant in decentralized or multi-organizational emergency environments where operational collaboration must occur despite limited pre-existing trust relationships between participating entities [\[28\]](#), [\[42\]](#), [\[70\]](#).

Blockchain-oriented approaches are especially relevant within distributed emergency communication ecosystems, where multiple organizations, devices and autonomous platforms must exchange sensitive information without necessarily relying on a single centralized authority. These frameworks can support tamper-resistant event logging, decentralized authentication, secure information sharing, immutable coordination records and trusted interactions among heterogeneous entities, including UAV-enabled systems, IoT devices and distributed edge nodes. Such capabilities are particularly valuable in multi-agency environments, where maintaining data integrity, traceability and consistent access control becomes essential for reliable operational coordination.

In addition, smart-contract mechanisms enable automated policy enforcement, distributed coordination logic and self-executing operational agreements, thereby reducing dependence on manual administrative intervention. They may also facilitate predefined authorization rules and automated interactions among distributed communication and computing resources, supporting more transparent and auditable coordination across emergency-response infrastructures. When combined with edge computing and decentralized architectures, blockchain-based mechanisms can therefore contribute to establishing trusted information exchange across geographically distributed operational environments.

Despite these advantages, blockchain and distributed-trust paradigms remain comparatively limited within the current dataset. This suggests that, although the research community increasingly recognizes their potential for strengthening trust, security and decentralized coordination, their integration into large-scale emergency communication architectures remains at a relatively early stage of maturity. The gap between conceptual potential and operational adoption also indicates an area where further experimental validation and integration with emerging 5G/6G, MEC, IoT and UAV-based infrastructures may be required. Figure 34 illustrates the distribution of security and trust paradigms across the different levels of architectural integration identified throughout the dataset.

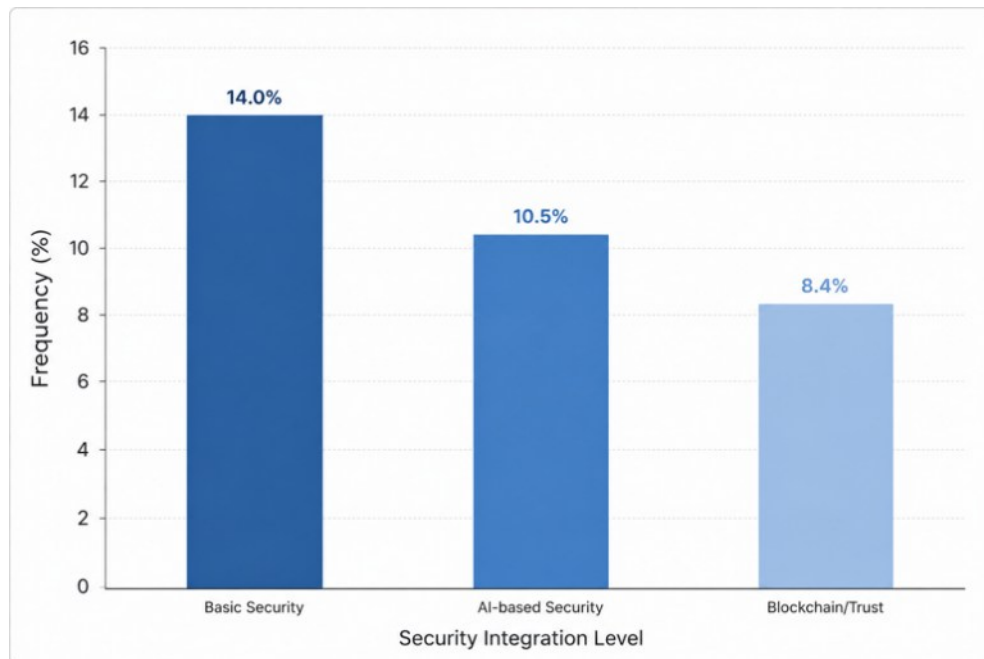


Figure 34 Security and Trust Paradigms in RQ2 Dataset.

The figure demonstrates that foundational security mechanisms remain the most frequently implemented category across the dataset, reflecting their essential role within communication-system architectures. AI-driven security mechanisms appear with moderate frequency, indicating a growing although not yet dominant adoption of adaptive and intelligent cybersecurity approaches. By contrast, blockchain-oriented and distributed trust frameworks exhibit the lowest frequency, confirming that they currently represent an emerging integration layer rather than a mature or widely adopted architectural standard.

This distribution reveals an important structural trend within the evolution of emergency communication systems. Security is progressively transitioning from static protection-oriented models toward adaptive, distributed and trust-centric architectural paradigms. Nevertheless, this transition remains incomplete. Most communication systems continue to operate primarily at the level of foundational or intermediate security integration, while fully decentralized trust architectures remain comparatively rare across the related literature.

This observation should be interpreted carefully. The relatively limited frequency of blockchain-based and advanced trust-management mechanisms does not imply reduced strategic importance. On the contrary, it reflects the significantly higher levels of architectural complexity, operational coordination and systemic maturity required for their successful integration. Distributed trust frameworks must operate reliably under highly dynamic and uncertain conditions while simultaneously supporting heterogeneous stakeholders, decentralized coordination processes, autonomous agents and resilience against sophisticated adversarial threats. These requirements make their implementation substantially more challenging than conventional security mechanisms based on static and centralized control models.

This category is also closely connected to the broader validation and reproducibility challenges discussed previously in Section 5.2. Security-related claims within communication-system research are often particularly difficult to validate rigorously, especially when experimental evaluation relies on custom-built testbeds, limited-scale deployments, or non-standardized validation methodologies. A system may propose sophisticated cybersecurity mechanisms or advanced trust architectures, yet their practical effectiveness ultimately depends on robust adversarial testing, realistic deployment conditions and reproducible evaluation procedures. In the absence of such validation,

security remains primarily a theoretical or conceptual property rather than a guaranteed operational capability.

Consequently, secure and trustworthy integration frameworks represent a strategically critical yet still evolving dimension of modern emergency communication ecosystems. As communication infrastructures become increasingly decentralized, autonomous, intelligent and interconnected, the importance of distributed trust management and adaptive security coordination is expected to grow substantially. Future research will likely focus on the integration of security and trust mechanisms across all architectural layers of the communication ecosystem, ranging from physical communication channels and network orchestration mechanisms to application-layer coordination and autonomous decision-making processes. In this context, resilience alone will no longer be sufficient, operational trustworthiness will become equally fundamental to system viability.

In summary, this category highlights one of the core architectural requirements of next-generation emergency communication systems. Connectivity, intelligence and adaptability alone are insufficient in the absence of trust. Secure and trustworthy integration frameworks provide the mechanisms necessary to ensure that communication ecosystems remain reliable, credible, resilient and operationally usable under highly dynamic, uncertain and potentially adversarial conditions.

5.3.4 Cyber-Physical Mission-Critical Ecosystems

The fourth functional category concerns cyber-physical mission-critical ecosystems. This category encompasses IoT infrastructures, WSN, distributed sensing systems, digital twins, CPS, robotics, hybrid sensor architectures and real-time situational-awareness platforms [71], [72]. Quantitatively, IoT, WSN and sensing-oriented paradigms appear in approximately 36.4% of the dataset analyzed, making them the second most prevalent technological family after 5G/6G and public safety communication architectures. This observation is particularly important because it demonstrates that modern emergency communication systems are no longer focused exclusively on connectivity. Instead, they are increasingly designed to observe, interpret, model and interact dynamically with the physical environment through continuous data acquisition and system-level feedback mechanisms.

IoT and sensing infrastructures constitute the observational and environmental-awareness layer of modern emergency communication ecosystems. These paradigms provide the

capability to continuously monitor environmental conditions, detect emerging hazards, assess infrastructure integrity, identify and locate victims, track mobility patterns, and generate real-time situational awareness across affected areas. Through distributed sensors, connected devices, wearable technologies, and other monitoring platforms, emergency communication systems can obtain information from locations that may otherwise remain inaccessible or insufficiently observed. Such capabilities are particularly critical in emergency and mission-critical environments, where operational conditions evolve rapidly and decision-making depends heavily on the availability of timely, reliable, and context-sensitive information.

The importance of IoT-based sensing becomes even more pronounced when conventional sources of information are disrupted or incomplete. During complex emergency scenarios, responders may need to operate with limited visibility regarding infrastructure damage, environmental hazards, population movement, or the availability of communication resources. Distributed sensing infrastructures can help reduce this information gap by continuously collecting and transmitting operational data from multiple points across the affected environment. This distributed observational capability contributes to a more comprehensive representation of evolving conditions and can support faster identification of operational priorities.

However, the operational value of sensing infrastructures does not emerge from data acquisition alone. Their significance materializes only when sensing capabilities are tightly integrated with communication networks, computational platforms, orchestration frameworks, and decision-support mechanisms. Large volumes of heterogeneous sensor data must be transported efficiently, processed within appropriate time constraints, and converted into information that can directly support emergency-response activities. Consequently, sensing infrastructures should be understood not as isolated technological components but as integral elements of a broader communication-computation continuum. A sensor network operating independently therefore does not constitute an advanced emergency communication ecosystem. Its functionality becomes operationally meaningful only when generated data flows are transmitted, processed, interpreted, and acted upon within a broader system architecture. In practice, this requires integration with edge-computing platforms for localized and low-latency processing, AI mechanisms for pattern recognition, anomaly detection, and predictive analytics, and command-and-control

infrastructures for operational coordination. Such integration can reduce the time between event detection and operational response, which is particularly important in rapidly evolving disaster environments.

Digital-twin environments provide an additional layer of integration by enabling sensing information to be incorporated into virtual representations of physical infrastructures and operational environments. Through this process, raw environmental observations can be contextualized and analyzed within a broader representation of the affected system. The combination of sensing, communication, computation, and intelligent analytics therefore establishes a continuous information flow from the physical environment toward decision-support and coordination mechanisms. Through this layered integration process, raw environmental data is progressively transformed into actionable operational intelligence, enabling more informed and adaptive decision-making under highly dynamic and time-critical conditions.

Digital twin, cyber-physical system, and robotics-oriented paradigms appear in approximately 6.5% of the analyzed dataset. Although quantitatively less frequent than other technological categories, these paradigms should not be interpreted as secondary in terms of strategic importance. On the contrary, they represent some of the most advanced forms of technological and architectural integration identified throughout the related literature. Their significance lies particularly in their ability to establish a direct relationship between communication infrastructures, computational intelligence, and the physical operational environment.

Digital twins enable the creation of continuously updated virtual representations of physical environments, infrastructures, assets, and operational processes. By incorporating real-time or near-real-time data generated by sensing infrastructures, these virtual models can evolve alongside the physical systems they represent. This synchronization enables emergency-response stakeholders to observe changing conditions, assess potential system states, and examine alternative operational scenarios within a digital environment. Consequently, digital twins can support predictive simulation, operational forecasting, scenario analysis, infrastructure assessment, and dynamic situational awareness.

Their role extends beyond visualization. When combined with AI, edge computing, and distributed sensing, digital twins can provide an analytical environment in which operational information is continuously interpreted and used to support planning and coordination. This

creates the potential for a feedback-oriented architecture in which information collected from the physical environment updates the digital representation, while insights generated within the virtual environment can subsequently inform actions in the physical domain. As a result, digital twins provide an interactive and continuously evolving representation of emergency conditions that can support both strategic planning and real-time mission coordination.

CPS further reinforce this connection by integrating computational processes with physical components and communication networks. Within emergency environments, this integration allows sensing, computation, communication, and physical action to operate as interconnected functions rather than independent technological layers. Such architectures are particularly relevant where emergency-response systems must continuously observe environmental changes, interpret incoming information, and coordinate appropriate operational responses.

Robotics and autonomous systems extend this cyber-physical integration directly into the physical domain by enabling communication ecosystems to interact with the operational environment itself. These systems can support mission-critical activities including search-and-rescue operations, hazardous-area inspection, infrastructure assessment, supply delivery, environmental exploration, and information collection in locations that may be inaccessible or dangerous for human responders. Their mobility and autonomous capabilities also allow communication and sensing functions to be dynamically repositioned according to evolving operational requirements.

When integrated with communication, sensing, edge-computing, and AI infrastructures, robotic platforms evolve from isolated operational tools into active agents within a broader cyber-physical ecosystem. They can simultaneously collect environmental information, communicate observations, receive updated mission objectives, and execute actions based on processed data or coordinated instructions.

This transition represents a significant architectural evolution from passive communication infrastructures, primarily designed to transport information, toward intelligent and environment-interactive operational ecosystems capable of sensing, interpreting, coordinating, and acting upon changing conditions. Figure 35 illustrates the distribution and integration patterns of cyber-physical paradigms across the analyzed dataset.

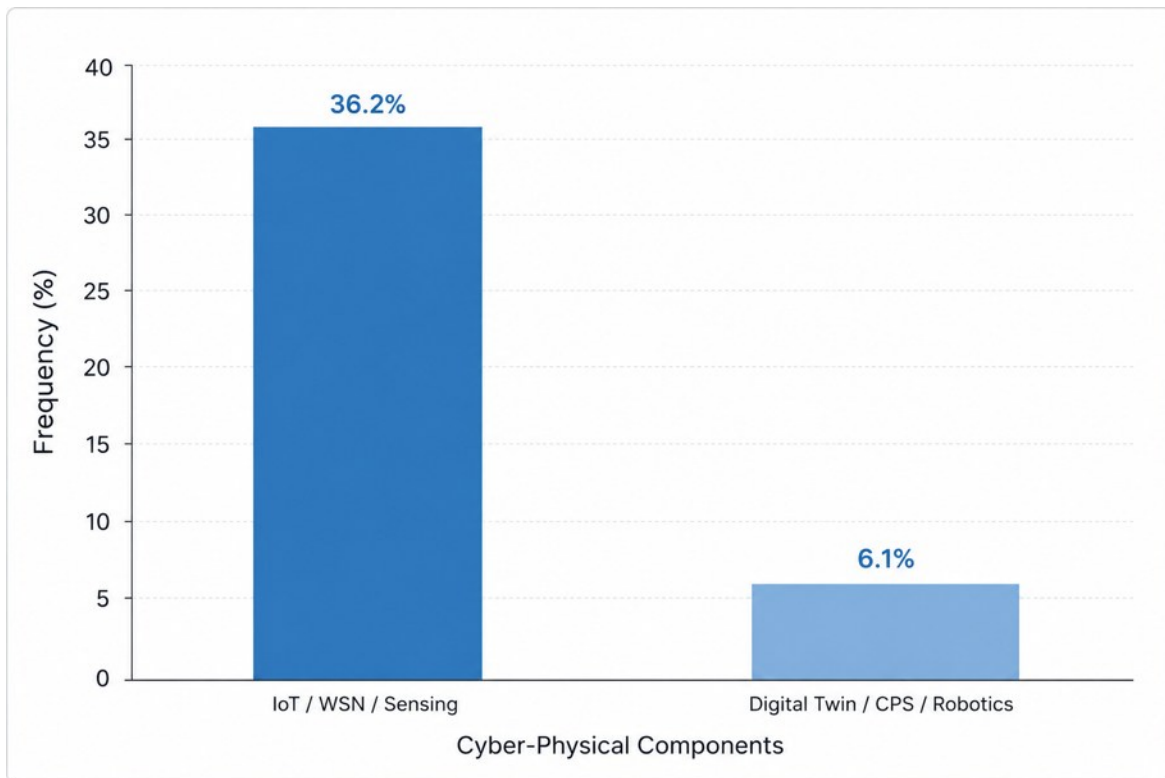


Figure 35 Cyber-Physical Paradigms in RQ2 Dataset.

The figure highlights a clear asymmetry between the high prevalence of IoT and sensing-oriented systems and the comparatively lower frequency of digital-twin and CPS-related paradigms. This distribution reflects the current stage of technological evolution and adoption within the field. Sensing infrastructures are widely implemented because they constitute the foundational layer of cyber-physical integration. They are comparatively mature, cost-efficient, scalable and directly applicable across a broad spectrum of emergency and mission-critical operational scenarios.

By contrast, digital-twin and cyber-physical-system paradigms require substantially more sophisticated integration across multiple architectural layers. Their effective deployment depends on the availability of reliable real-time data streams, distributed computational resources, accurate environmental modeling techniques, synchronization mechanisms and continuous interaction between physical and virtual system components. These requirements significantly increase implementation complexity and help explain their comparatively lower representation within the dataset. Nevertheless, their strategic and operational impact is considerably greater because they enable predictive, adaptive and proactive system behavior rather than purely reactive operational responses.

This observation supports a broader interpretation of the ongoing evolution of emergency communication systems. The field is progressively transitioning from simple data acquisition toward real-time data interpretation and ultimately toward autonomous or semi-autonomous data-driven operational action. Within this progression, IoT and sensing infrastructures provide raw environmental input, AI extracts operational meaning and predictive insight from collected data, while cyber-physical systems and digital twins enable decision execution and adaptive interaction within the physical environment itself. Collectively, this transition reflects a broader architectural shift from communication-centric infrastructures toward integrated ecosystems combining sensing, computation, communication, orchestration and control within a unified operational framework.

The importance of this category is further reinforced by the exceptionally high average score associated with operational relevance, which reaches approximately 4.56/5 across the evaluated dataset. This observation indicates that a substantial proportion of the analyzed studies are explicitly oriented toward realistic operational scenarios, including disaster response coordination, public safety operations, search-and-rescue missions, infrastructure monitoring and critical infrastructure management. The strong operational emphasis confirms that cyber-physical integration is not merely a conceptual or theoretical research direction, but rather an increasingly necessary architectural requirement for next-generation emergency communication systems.

Cyber-physical ecosystems therefore represent a fundamental transformation in the role and operational identity of communication systems. Traditional emergency communication networks were primarily designed to transmit information between human users and centralized command structures. In contrast, cyber-physical ecosystems integrate sensing, computation, communication, orchestration and control into a tightly coordinated operational environment. This integration enables communication systems not only to transmit information, but also to interpret environmental conditions, support autonomous or semi-autonomous decision-making, coordinate distributed actions and interact dynamically with the operational environment itself.

An important implication of this transformation is the emergence of environment-aware communication ecosystems. Modern communication systems no longer function solely as passive channels for information exchange. Instead, they increasingly operate as active participants within the operational process itself, continuously sensing environmental

conditions, adapting system behavior and coordinating distributed responses across multiple agents and infrastructures. This capability becomes especially important in highly dynamic and uncertain emergency environments where rapid adaptation, contextual awareness and coordinated multi-agent action are essential for effective operational response.

In summary, the cyber-physical category highlights the broader transition from network-centric communication infrastructures toward environment-aware, data-driven and action-oriented operational ecosystems. It demonstrates how advanced paradigms enable emergency communication systems to evolve beyond basic connectivity and toward integrated platforms capable of sensing, interpreting, predicting and interacting with the physical world in real time. Consequently, cyber-physical mission-critical ecosystems constitute one of the foundational pillars of the proposed taxonomy and occupy a central role in addressing the paradigm-integration challenges explored throughout RQ2.

5.4 Final Answer to RQ2

The recurring convergence patterns identified throughout the RQ2 dataset demonstrate that advanced paradigms are becoming increasingly interdependent within modern emergency communication architectures. AI depends on distributed computational infrastructures and continuous real-time data availability. UAV-assisted systems require adaptive communication management, resilient backhaul connectivity and distributed edge processing. Digital twin environments rely on synchronized sensing infrastructures and continuous environmental data streams. Blockchain-enabled trust mechanisms depend on interoperable communication protocols and distributed coordination frameworks. Collectively, these relationships reveal that contemporary emergency communication systems can no longer be understood as collections of isolated technological components. Instead, they are progressively evolving into integrated operational ecosystems in which functionality emerges through coordinated interaction across multiple architectural layers. This observation represents one of the most important conceptual findings of the chapter. Earlier generations of communication systems were generally organized around modular and relatively independent architectures. Communication, sensing, computation and control mechanisms were typically developed separately and optimized according to domain-specific objectives. Although such architectures could provide acceptable functionality under stable operational conditions, they often lacked the adaptability, coordination capability and operational awareness required within complex emergency environments.

The dataset clearly indicates that this architectural paradigm is gradually being replaced by convergence-oriented ecosystems. Within these environments, the boundaries separating communication infrastructures, computational resources, sensing platforms, orchestration mechanisms and operational control layers become increasingly fluid. Technologies no longer function as independent modules connected through static interfaces. Instead, they interact continuously through dynamic feedback loops that enable adaptive, coordinated and context-aware system behavior.

This growing interdependence introduces profound architectural implications. Emergency communication ecosystems can no longer be designed through isolated optimization strategies focused exclusively on individual technological subsystems. Improving the performance of a single component in isolation may produce limited operational benefit if coordination across the broader ecosystem remains weak. As a result, contemporary architectures increasingly prioritize interoperability, orchestration, synchronization and cross-layer integration as fundamental design principles rather than supplementary technical features.

The transition toward convergence also introduces substantially greater system complexity. Heterogeneous paradigms must exchange information continuously, maintain coordinated operational states and adapt dynamically to evolving environmental conditions. Communication ecosystems must therefore support not only connectivity, but also distributed coordination among computational infrastructures, sensing systems, autonomous agents, operational-control mechanisms and decision-support platforms.

Interoperability becomes particularly critical within this context. Emergency communication ecosystems frequently involve heterogeneous devices, communication protocols, sensing platforms, organizational actors and operational domains operating simultaneously within the same environment. UAV platforms may interact concurrently with terrestrial 5G infrastructures, satellite communication layers, edge-computing systems, IoT sensing environments and AI-enabled orchestration mechanisms. Without effective interoperability frameworks, the operational benefits of convergence cannot be fully realized.

Synchronization similarly emerges as a major architectural requirement. Distributed systems operating across multiple interconnected layers must maintain consistent situational awareness and coordinated operational states despite environmental instability and

communication uncertainty. Real-time synchronization becomes especially important within cyber-physical environments where sensing information, communication infrastructures, autonomous systems and operational actions remain tightly interconnected. The dataset further demonstrates that orchestration increasingly emerges as one of the defining capabilities of high-integration communication ecosystems. Traditional communication systems primarily focused on routing and resource allocation within relatively static infrastructures. By contrast, converged ecosystems require orchestration mechanisms capable of coordinating heterogeneous resources dynamically across multiple operational and architectural layers simultaneously.

This orchestration capability increasingly depends on AI and distributed edge-processing infrastructures. AI-enabled orchestration frameworks can analyze environmental conditions, evaluate operational priorities, allocate communication resources dynamically, optimize mobility patterns, coordinate autonomous agents and support adaptive decision-making processes in real time. Edge infrastructures provide the distributed computational substrate necessary to support these operations with low latency and reduced dependence on centralized cloud environments.

The architectural role of orchestration therefore extends well beyond conventional network management. It becomes the core mechanism through which the ecosystem maintains adaptive coordination, operational continuity and distributed intelligence under uncertain conditions. Communication systems progressively evolve into operational coordination ecosystems rather than passive transmission infrastructures.

Another important implication of convergence concerns the emergence of cross-layer adaptive behavior. In traditional communication architectures, communication, computation and sensing processes frequently operated independently with limited interaction across layers. In converged ecosystems, however, operational conditions detected within one layer may dynamically influence behavior across multiple interconnected layers simultaneously. Environmental changes detected through sensing infrastructures may trigger communication-resource reallocation, autonomous mobility adaptation, predictive computational analysis, or distributed operational coordination throughout the ecosystem.

The dataset strongly suggests that convergence additionally enables emergent operational capabilities that cannot be achieved through standalone technological paradigms operating

independently. This represents one of the most important conceptual insights of the chapter. The value of converged architectures lies not simply in combining multiple technologies, but in generating system-level operational behaviors that exceed the capabilities of individual paradigms functioning in isolation.

Among these emergent capabilities are adaptive resilience, predictive coordination, distributed autonomy and environment-aware operational control. Adaptive resilience enables communication ecosystems to reconfigure dynamically under degraded or uncertain conditions. Predictive coordination allows systems to anticipate operational changes rather than responding reactively after failures occur. Distributed autonomy supports decentralized operational decision-making among intelligent agents operating across heterogeneous environments. Environment-aware control enables communication ecosystems to adapt continuously according to physical, environmental and mission-specific conditions.

Collectively, these capabilities fundamentally transform the role of emergency communication infrastructures themselves. Networks are no longer designed solely to transport information between users, field units and command centers. Instead, they increasingly evolve into integrated cognitive ecosystems capable of perception, interpretation, coordination, prediction and adaptive operational response.

This transformation also changes how resilience itself is understood within emergency communication research. Traditional resilience models primarily emphasized redundancy and fault tolerance. Converged ecosystems introduce a broader interpretation in which resilience emerges through intelligent coordination, distributed adaptation, predictive orchestration and dynamic resource management across multiple interconnected architectural layers.

The dataset further indicates that high-scoring studies consistently prioritize multi-paradigm coordination rather than isolated technological optimization. This trend strongly suggests that the research community increasingly recognizes that future operational effectiveness will depend more heavily on integration quality, orchestration capability and ecosystem coordination than on the advancement of any single technological paradigm individually.

At the same time, convergence introduces important architectural and operational challenges. Increasing interdependence also increases vulnerability to cascading failures, synchronization instability, orchestration complexity, interoperability limitations and cross-layer security exposure. Managing heterogeneous infrastructures dynamically requires

sophisticated coordination frameworks, adaptive control mechanisms and robust architectural design principles. Security also becomes significantly more complex because disruptions or attacks targeting one subsystem may propagate rapidly across interconnected layers of the broader operational ecosystem.

Ultimately, the findings of this section reinforce one of the central arguments developed throughout this chapter: the future of emergency communication systems will not be determined primarily by the isolated advancement of individual paradigms such as AI, UAVs, IoT infrastructures, or blockchain frameworks. Instead, it will depend fundamentally on the ability to orchestrate these paradigms into coherent, adaptive, resilient and intelligent operational ecosystems capable of functioning effectively under uncertainty, infrastructural degradation and rapidly evolving mission conditions.

6. RQ3 Network Layer Perspectives in Crisis Communication Systems

Emergency communication systems are rapidly evolving into highly distributed and interconnected networking ecosystems designed to support mission-critical operations under extreme conditions. Natural disasters, large-scale infrastructure failures, cyberattacks, terrorist incidents, armed conflicts, industrial accidents and mass-casualty events increasingly expose the structural limitations of conventional communication infrastructures, particularly regarding resilience, interoperability, scalability, latency management, survivability and service continuity [10]. Traditional communication architectures were primarily designed for stable civilian environments characterized by predictable traffic patterns and relatively centralized infrastructures. However, emergency scenarios frequently involve destroyed communication facilities, overloaded cellular infrastructures, fragmented connectivity, unstable power supply, dynamic mobility conditions and rapidly changing operational requirements. Under such conditions, conventional communication systems often fail to maintain reliable coordination between first responders, emergency agencies, autonomous systems and affected civilian populations [31].

As a result, the research community has progressively shifted its attention toward the development of resilient and adaptive communication architectures capable of preserving operational continuity even under degraded or partially destroyed networking environments. Modern emergency communication systems increasingly emphasize distributed operation, autonomous adaptation, edge-native intelligence and dynamic orchestration mechanisms capable of responding to rapidly evolving disaster conditions. This transition reflects a broader architectural evolution from isolated communication infrastructures toward integrated cyber-physical operational ecosystems where communication, computation, sensing, orchestration and intelligent decision-making operate as tightly interconnected components [73]. Figure 37 illustrates the architectural transition from traditional centralized communication systems toward distributed and intelligent emergency communication ecosystems.

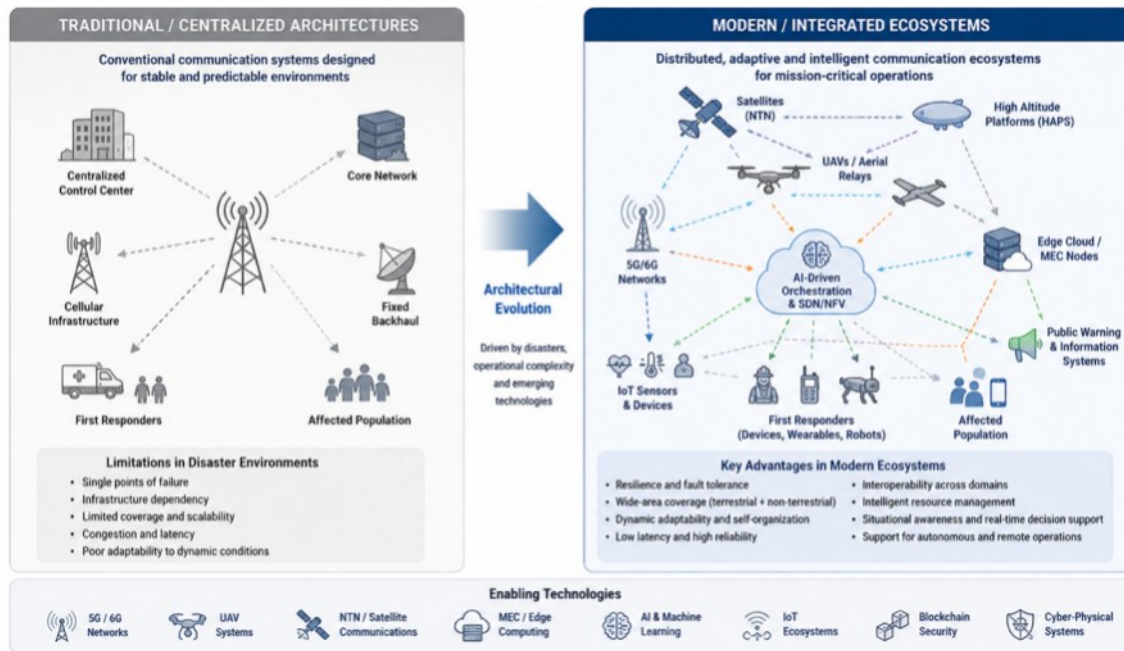


Figure 36 Evolution of Emergency Communication Architectures.

Within this context, the OSI model and broader network-layer perspectives provide a valuable analytical framework for understanding how different communication layers contribute to emergency communication resilience and operational effectiveness. Each networking layer addresses distinct but interdependent operational requirements that collectively determine the survivability and efficiency of crisis communication systems

At the physical layer, research primarily focuses on resilient spectrum utilization, robust wireless communication, satellite connectivity, anti-jamming mechanisms, energy-efficient transceivers and communication reliability under hostile or infrastructure-deficient environments. Physical-layer resilience becomes especially critical during disasters where terrestrial infrastructures may be partially destroyed or unavailable. For this reason, recent research has focused heavily on NTN, low-earth-orbit satellite systems, high-altitude platform systems and adaptive radio communication mechanisms capable of extending communication coverage beyond conventional terrestrial limitations [40].

Among all networking layers, the data-link and network layers attract considerable research attention due to their direct role in maintaining communication continuity in highly dynamic and fragmented environments. Major research themes include MANETs, vehicular ad hoc networks (VANETs), UAV-assisted communication, topology-aware routing, multi-hop networking, mobility management, aerial base stations and disaster-area coverage optimization. These layers are particularly important in post-disaster environments where

traditional communication infrastructures may become unavailable and rapidly deployable networking mechanisms are required to restore operational connectivity. UAV-assisted networking has emerged as one of the dominant architectural directions because unmanned aerial systems can simultaneously function as communication relays, temporary base stations, sensing platforms and edge-computing nodes [\[49\]](#).

The transport layer addresses another critical dimension of emergency communication systems by focusing on latency-sensitive communication, congestion management, QoS continuity, handover optimization and session survivability. Mission-critical emergency operations require reliable real-time communication between command centers, first responders, autonomous systems and field personnel. Consequently, transport-layer mechanisms increasingly investigate adaptive QoS management, seamless terrestrial-satellite handover, delay-sensitive communication protocols and service continuity under unstable network conditions. However, despite its operational importance, transport-layer adaptation remains comparatively underexplored when compared with network-layer and orchestration-focused research [\[18\]](#), [\[74\]](#).

At the application layer, research focuses on intelligent emergency coordination systems, situational-awareness platforms, disaster-management applications, public-warning infrastructures, real-time monitoring systems and citizen-centric communication services. Modern emergency applications increasingly integrate AI, IoT sensing, cloud analytics and real-time decision-support mechanisms capable of improving situational awareness and accelerating emergency response coordination. However, application-layer effectiveness increasingly depends on lower-layer communication resilience, edge-computing support and orchestration efficiency [\[7\]](#). Figure 37 summarizes the primary operational roles and technological components associated with each networking layer in emergency communication environments.

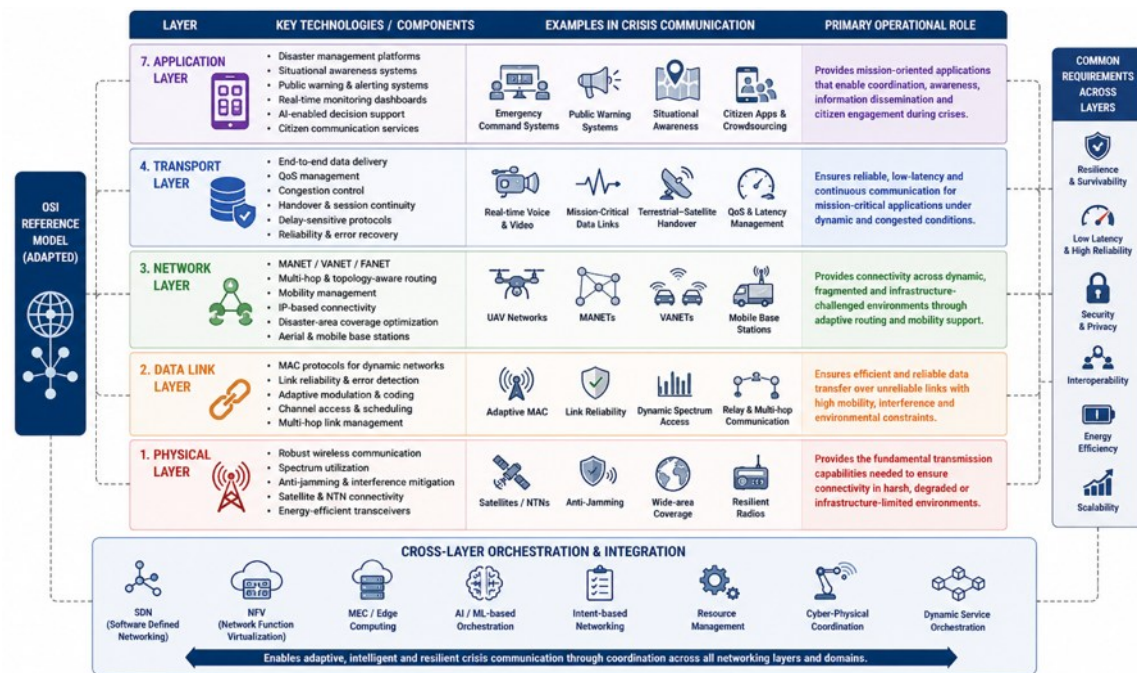


Figure 37 Network Layer Perspectives in Crisis Communication Systems.

Beyond isolated networking layers, one of the strongest trends identified in contemporary crisis communication research is the emergence of cross-layer orchestration architectures. These architectures integrate multiple communication domains through SDN, NFV, MEC, AI-driven orchestration, virtualization, distributed edge computing, cyber-physical coordination and adaptive service management. The rapid convergence of 5G/6G networking, UAV-assisted communication, edge intelligence, CPS, blockchain, IoT ecosystems and NTNs has fundamentally transformed the architectural priorities of emergency communication systems. Instead of focusing exclusively on isolated protocol optimization, modern research increasingly investigates integrated orchestration ecosystems capable of dynamically coordinating heterogeneous computational, communication and sensing resources across multiple networking layers [18].

This architectural transformation reflects the growing complexity of modern disaster response. Future emergency communication systems must support low latency, reliability, interoperability, scalability, fault tolerance, cyber resilience and autonomous adaptation. These requirements increasingly depend on distributed intelligence, efficient orchestration and cross-layer resilience. Figure 38 illustrates how SDN, NFV, MEC, AI orchestration, UAVs, IoT and NTNs collectively support adaptive crisis communication ecosystems.

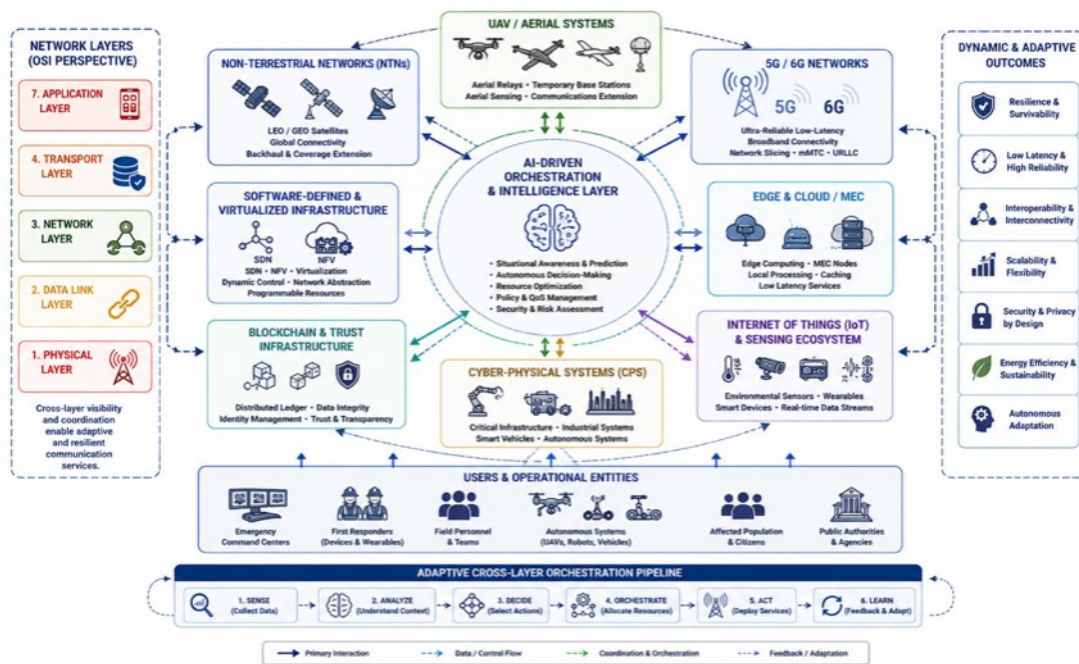


Figure 38 Cross-Layer Orchestration Ecosystem.

This chapter investigates the following research question: “Which network layers receive the most research attention for crisis communication and where do significant gaps remain?” To address this question, a structured analytical framework was developed and applied to the collected dataset. Each article was systematically evaluated according to:

- dominant network-layer focus,
- cross-layer integration maturity,
- operational relevance to emergency communications,
- QoS and resilience contribution,
- security contribution,
- AI and automation integration,
- and validation maturity.

The objective of the analysis is not only to identify which networking layers dominate current research activity, but also to reveal broader technological and architectural trends shaping the evolution of next-generation emergency communication systems. Particular emphasis is placed on identifying recurring architectural transitions, validation weaknesses, underexplored networking domains and future research opportunities.

The findings demonstrate that modern emergency communication research increasingly prioritizes cross-layer orchestration ecosystems combining networking, edge computing, virtualization, UAV infrastructures, AI-native resource management and distributed

intelligent coordination. At the same time, several important research gaps remain unresolved. These include limited real-world deployment validation, insufficient autonomous orchestration capabilities, fragmented cybersecurity integration, underdeveloped transport-layer adaptation mechanisms and limited operational evidence regarding large-scale heterogeneous emergency communication deployments. Consequently, although modern emergency communication research demonstrates significant architectural sophistication, the transition from experimental frameworks toward fully operational resilient communication ecosystems remains an ongoing challenge for both academia and industry.

6.1 Methodological Framework for RQ3 Evaluation

The purpose of the RQ3 evaluation framework is to provide a systematic and operationally oriented methodology for analyzing how contemporary emergency communication research distributes attention across the networking stack and associated architectural domains. Unlike conventional networking surveys, which frequently concentrate on isolated protocol optimization, throughput enhancement, spectral efficiency, or communication performance under stable conditions, the proposed framework evaluates communication architectures through the perspective of real-world crisis operations. Consequently, the analysis extends beyond purely technical networking performance and examines how communication systems contribute to operational continuity, resiliency, survivability, interoperability and adaptive coordination during mission-critical emergency scenarios [\[13\]](#).

The framework was specifically designed to capture the growing architectural complexity of next-generation emergency communication systems. Modern disaster response environments involve highly heterogeneous ecosystems where communication infrastructures interact dynamically with edge computing, UAV platforms, cyber-physical systems, IoT sensing infrastructures, AI, virtualization frameworks, satellite systems and distributed orchestration mechanisms. As a result, evaluating emergency communication research exclusively at the protocol level is no longer sufficient for understanding the operational maturity of contemporary architectures [\[18\]](#).

The first objective of the framework is to identify the dominant network layer emphasized by each study. This classification process is particularly important because many modern architectures simultaneously involve multiple communication layers. However, despite this convergence, most studies still exhibit a dominant architectural focus. Some papers

primarily investigate physical-layer resilience and spectrum survivability, while others emphasize routing optimization, QoS continuity, edge orchestration, or intelligent disaster-management applications. Identifying the dominant layer enables the quantitative mapping of research attention across the networking stack and reveals which domains receive the greatest architectural investment from the research community.

The second objective is to measure the depth of technical contribution associated with the target layer. Not all networking studies contribute equally to architectural innovation. Some articles merely adapt existing communication mechanisms to emergency environments, while others introduce fundamentally new orchestration paradigms, distributed coordination models, or resilient communication architectures. The framework therefore differentiates between minor protocol adaptation, moderate optimization, strong technical contribution, architectural innovation and novel networking paradigms. This distinction is essential for identifying which technological directions genuinely advance the state of the art.

A central component of the framework involves evaluating operational relevance to emergency and mission-critical communications. Many networking studies investigate advanced communication technologies without directly addressing disaster response conditions or mission-critical operational constraints. Consequently, the framework distinguishes generic networking research from architectures explicitly designed for:

- emergency response,
- disaster recovery,
- search-and-rescue operations,
- public safety communication,
- battlefield coordination,
- or infrastructure-deficient environments.

This operational perspective is particularly important because communication systems deployed during disasters must satisfy far stricter requirements than conventional civilian communication infrastructures. Mission-critical environments require uninterrupted service continuity, rapid deployment, survivability under infrastructure damage, mobility support, real-time situational awareness and interoperability between multiple agencies and heterogeneous technologies [\[10\]](#).

Another major analytical dimension concerns cross-layer integration. One of the strongest architectural trends in modern emergency communication research is the transition from

isolated networking mechanisms toward integrated orchestration ecosystems. Traditional communication architectures frequently optimized individual protocol layers independently. In contrast, contemporary emergency communication systems recent integrate networking, edge computing, virtualization, AI-driven orchestration, distributed sensing, UAV-assisted communication and cyber-physical coordination into unified operational frameworks. The framework therefore evaluates the degree to which studies support adaptive interaction and coordinated functionality across multiple networking layers. The framework also assesses contributions to QoS, resilience, survivability and fault tolerance [47]. These dimensions represent foundational operational requirements for emergency communication systems operating under hostile or degraded conditions. During disasters, communication infrastructures frequently experience:

- congestion,
- physical destruction,
- intermittent connectivity,
- power instability,
- mobility disruptions,
- and cascading service failures.

Consequently, modern emergency communication research recent prioritizes architectures capable of maintaining low latency, reliable communication continuity, dynamic rerouting, adaptive resource allocation and resilient service orchestration even under severe operational stress [15]. Evaluating these resiliency characteristics enables the framework to identify which architectures contribute most effectively to operational survivability. The cybersecurity and trust-management integration constitute another critical analytical dimension. As emergency communication systems evolve toward distributed and highly interconnected ecosystems, the attack surface expands significantly. Modern crisis communication architectures currently involve:

- IoT infrastructures,
- CPS,
- UAV swarms,
- edge-computing nodes,
- cloud services,
- VFN,

- and distributed orchestration mechanisms.

These environments introduce substantial vulnerabilities related to spoofing, denial-of-service attacks, malicious data manipulation, unauthorized access, communication interception and infrastructure compromise [67]. Consequently, the framework evaluates the degree to which studies integrate:

- authentication,
- encryption,
- trust management,
- blockchain-based security,
- anti-jamming mechanisms,
- and cyber-resilience strategies.

The framework further measures AI-driven automation and orchestration maturity. AI recent appears as a core enabling technology within emergency communication research. AI mechanisms are progressively applied to:

- resource allocation,
- intelligent routing,
- congestion mitigation,
- predictive failure analysis,
- anomaly detection,
- autonomous UAV coordination,
- and adaptive network orchestration [50].

However, the maturity of AI integration varies significantly across the related literature. Some studies incorporate only limited optimization mechanisms, while others investigate fully adaptive orchestration ecosystems capable of autonomous decision-making under rapidly changing disaster conditions. Measuring AI integration therefore helps to identify emerging intelligent networking paradigms.

Another important component of the framework concerns validation realism and deployment maturity. A recurring limitation within emergency communication research is the dominance of simulation-oriented evaluation. Many architectures demonstrate strong theoretical performance but lack realistic operational validation [46]. Consequently, the framework differentiates between:

- conceptual proposals,

- analytical models,
- simulations,
- laboratory testbeds,
- pilot deployments,
- and real operational implementations.

This distinction is essential because emergency communication systems operate under highly unpredictable and hostile conditions that are difficult to reproduce through controlled simulations alone. Finally, the framework aims to identify recurring architectural and operational research gaps. The purpose of the analysis is not merely classificatory, but also exploratory. By systematically evaluating the dataset, the framework reveals underdeveloped networking domains, recurring weaknesses and future research opportunities. In particular, the analysis enables the identification of gaps involving:

- autonomous orchestration,
- transport-layer adaptation,
- operational scalability,
- integrated cyber resilience,
- interoperability,
- and real-world deployment maturity.

Figure 39 summarizes the primary analytical dimensions used to evaluate architectural maturity, operational relevance, resiliency, orchestration complexity and deployment realism within the RQ3 dataset.

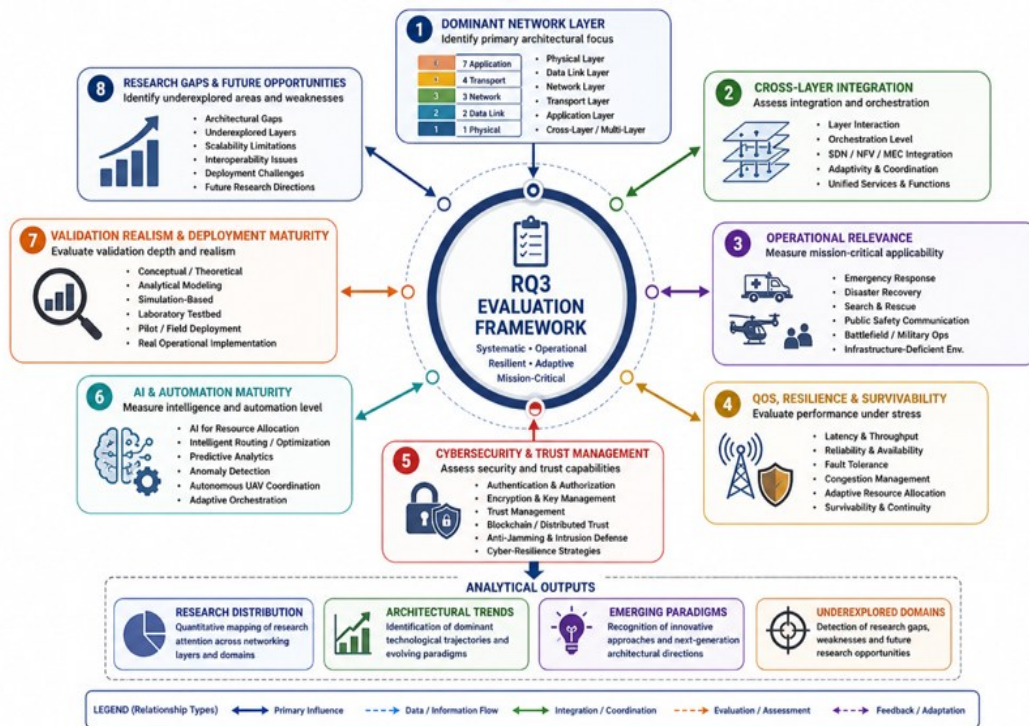


Figure 39 Multidimensional RQ3 Evaluation Framework.

Overall, the framework combines communication-network analysis, systems engineering, emergency management, cyber resilience and distributed orchestration perspectives into a unified analytical methodology. This multidimensional approach enables the identification of both dominant technological trajectories and insufficiently explored research domains, thereby providing a comprehensive understanding of how modern emergency communication systems are evolving toward intelligent, resilient and highly orchestrated cyber-physical ecosystems [25], [47].

6.1.1 Network Layer Classification

Each article included in the dataset was assigned one dominant primary network layer according to its architectural emphasis and operational focus. Although contemporary emergency communication systems increasingly integrate multiple networking domains, most studies still concentrate their main technical contribution within a specific architectural layer. This classification was therefore necessary to systematically evaluate how research attention is distributed across the communication stack and to identify broader technological trends shaping the evolution of next-generation crisis communication systems. It also provides a common analytical basis for comparing heterogeneous approaches that may differ substantially in their underlying technologies, deployment scenarios and operational

objectives. The analysis indicates that the networking stack is no longer investigated as a collection of isolated communication mechanisms. Instead, the current literature increasingly reflects the complexity of modern emergency environments, where communication infrastructures must simultaneously support mobility, resilience, interoperability, distributed coordination, low-latency communication and adaptive orchestration under highly unstable conditions [13]. Consequently, individual network layers are becoming increasingly interconnected through mechanisms such as software-defined control, edge intelligence, dynamic resource allocation and AI-assisted orchestration. This evolution suggests a gradual transition from conventional layer-specific optimization toward more integrated architectures capable of coordinating communication, computing and sensing resources across multiple levels of the network.

Nevertheless, despite this architectural convergence, clear research concentrations remain visible across different networking domains. Certain studies continue to emphasize specific layer-level mechanisms, while a growing proportion adopts cross-layer approaches that coordinate functions across the communication stack. This distribution provides an important indication of how research priorities are shifting from isolated protocol improvements toward more holistic, adaptive and intelligent networking architectures. Figure 40 illustrates the relative concentration of research activity across the networking stack, highlighting the increasing prominence of cross-layer orchestration architectures within the analyzed literature.

NETWORK LAYER	1. PHYSICAL LAYER	2. DATA LINK / NETWORK LAYER	3. TRANSPORT LAYER	4. APPLICATION LAYER	5. CROSS-LAYER ARCHITECTURES
RELATIVE RESEARCH ATTENTION	 Moderate	 Very High	 Low	 Moderate – High	 Dominant
APPROXIMATE DISTRIBUTION	~18%	~32%	~10%	~20%	~20%
PRIMARY RESEARCH FOCUS	Communication survivability under harsh or degraded conditions	Connectivity, routing, mobility and distributed networking in dynamic environments	Reliable data delivery, QoS and session continuity under instability	Situational awareness, coordination, and decision support applications	Integrated orchestration across multiple layers and domains toward unified ecosystems
EXAMPLES OF KEY TECHNOLOGIES & APPROACHES	 NTN / Satellite Communication  Anti-Jamming & Spectrum Resilience  Energy-Efficient Transceivers	 UAV-Assisted Networks  MANET / VANET Topologies  Adaptive Routing & Multi-hop Networking	 QoS & Latency Management  Handover & Session Continuity  Congestion Control & Reliability	 AI-Driven Analytics & Decision Support  Emergency Coordination Platforms  Public Warning & Alert Systems	 SDN / NFV / MEC Integration  AI-Driven Orchestration & Automation  UAV, IoT, CPS & NTN Convergence
OPERATIONAL ROLE IN CRISIS COMMUNICATION	Provides the fundamental communication capabilities required in hostile or infrastructure-limited environments.	Ensures connectivity and communication continuity among mobile and distributed emergency assets.	Guarantees reliable and timely data delivery for mission-critical applications.	Enables awareness, decision-making, and coordination among responders and affected populations.	Coordinates all resources and functions across layers for adaptive, resilient and intelligent operations.

Figure 40 Distribution of Research Attention Across Network Layers.

Studies assigned to the physical-layer category primarily focused on communication survivability under degraded or hostile conditions. Most studies within this category focused primarily on maintaining reliable communication connectivity when conventional terrestrial infrastructures become unavailable or severely degraded. Research attention focused heavily on resilient wireless communication mechanisms designed to support emergency operations under adverse environmental and infrastructural conditions.

A major trend identified within this category was the increasing importance of non-terrestrial communication infrastructures. A growing number of studies explored satellite-assisted communication and extended wireless coverage mechanisms capable of supporting communication continuity during large-scale disasters or geographically isolated operations [75]. The Physical-layer research also demonstrated a strong emphasis on communication robustness and survivability rather than purely maximizing communication performance. Consequently, operational reliability, energy efficiency and communication persistence under unstable conditions emerged as central priorities.

The Data Link and Network layer category represented one of the strongest concentrations of research activity throughout the dataset. This reflects the operational importance of maintaining connectivity and communication continuity in highly dynamic disaster environments characterized by mobility, fragmentation and infrastructure instability. The dominant architectural themes included topology-aware networking, adaptive routing, distributed communication coordination, mobility management and rapidly deployable communication infrastructures [76].

One of the strongest trends within this category was the extensive investigation of UAV-assisted communication systems. Unmanned aerial systems increasingly appear as central operational components capable of functioning simultaneously as communication relays, temporary base stations, sensing platforms and distributed communication extenders. The related literature demonstrated substantial research interest in optimizing aerial-network deployment, maintaining communication coverage over damaged areas and supporting dynamic multi-hop connectivity between mobile emergency units [23]. Another major focus involved communication continuity in highly mobile and decentralized operational environments. Researchers increasingly examined architectures capable of maintaining resilient connectivity despite changing topologies, intermittent links, infrastructure destruction and rapidly evolving operational conditions. As a result, the Data Link and

Network layer literature strongly emphasized distributed adaptability and infrastructure independence.

The transport-layer category received comparatively lower attention within the dataset, despite its operational importance for emergency communication systems. Studies assigned to this category primarily concentrated on maintaining communication continuity and service reliability under unstable network conditions. The dominant research themes involved congestion handling, delay-sensitive communication, continuity of service sessions, QoS preservation and seamless transitions between heterogeneous communication infrastructures. The transport-layer research frequently addressed the challenge of maintaining uninterrupted communication during infrastructure transitions, particularly between terrestrial and non-terrestrial communication domains. Recent work has increasingly examined adaptive mechanisms capable of preserving communication continuity during handover operations under emergency conditions [\[43\]](#), [\[74\]](#). These mechanisms are especially important for mission-critical applications requiring uninterrupted situational awareness and command coordination. However, the analysis revealed that transport-layer adaptation remains relatively underdeveloped compared with orchestration-oriented and network-layer research. Many transport-focused studies remain narrowly scoped and primarily optimization-oriented, without fully integrating intelligent orchestration, cybersecurity mechanisms or autonomous adaptive coordination. This observation is particularly important because future emergency communication systems will rely heavily on intelligent QoS management and adaptive latency-aware communication continuity.

At the application layer, research primarily focused on operational coordination, situational awareness, emergency response management and disaster-support services. Unlike lower-layer studies focusing on communication continuity itself, application-oriented research investigated how communication infrastructures support decision-making, emergency coordination, resource allocation and operational awareness during crisis conditions. The dataset demonstrated increasing integration between application-layer systems and intelligent computational infrastructures. Many studies combined real-time monitoring, distributed sensing, AI-based analytics, cloud processing and emergency coordination services into unified operational platforms [\[71\]](#). Application-layer architectures increasingly support:

- situational-awareness generation,
- real-time decision support,
- emergency alert dissemination,
- disaster response coordination,
- and intelligent operational management.

However, the analysis also demonstrated that current application-layer systems are becoming progressively dependent on lower-layer resiliency and orchestration mechanisms. Their operational effectiveness increasingly depends on reliable edge computing, distributed networking, low-latency communication and resilient infrastructure coordination. The strongest architectural trend identified throughout the dataset was the dominance of cross-layer architectures. Studies assigned to this category integrated multiple networking domains simultaneously and increasingly approached emergency communication systems as unified orchestration ecosystems rather than isolated protocol layers.

Cross-layer architectures frequently combined:

- SDN,
- NFV,
- MEC,
- edge computing,
- AI-driven orchestration,
- UAV-assisted communication,
- CPS,
- network slicing,
- and distributed intelligent infrastructures [\[18\]](#), [\[35\]](#).

The rapid growth of this category demonstrates a fundamental transformation in emergency communication research priorities. Rather than optimizing individual communication mechanisms independently, researchers increasingly investigate coordinated ecosystems capable of dynamically integrating communication, computation, sensing, virtualization and intelligent resource management. This shift reflects the growing recognition that disaster communication environments cannot be effectively managed through isolated protocol-level improvements, particularly when network conditions, infrastructure availability and operational demands change rapidly during emergency scenarios.

Distributed orchestration and adaptive coordination are therefore emerging as foundational architectural requirements for next-generation crisis communication systems. The integration of MEC, SDN and NFV provides greater flexibility in the placement, configuration and management of network functions, while enabling distributed computational capabilities and dynamic service deployment under unstable operational conditions. These technologies also facilitate adaptive resource allocation and rapid network reconfiguration when conventional infrastructure becomes congested, degraded or partially unavailable.

At the same time, AI-driven orchestration increasingly supports intelligent resource allocation, adaptive communication management and predictive resilience mechanisms. By continuously analyzing network conditions, traffic patterns and operational requirements, AI-assisted mechanisms can contribute to more dynamic coordination of communication and computing resources. This capability becomes particularly relevant in complex disaster environments, where network behavior must adapt to changing user mobility, connectivity constraints and mission-critical service priorities.

Another important observation is that cross-layer architectures frequently integrate cyber-physical coordination mechanisms involving UAVs, IoT infrastructures, edge computing and distributed sensing environments. These technologies extend the communication architecture beyond conventional networking functions by incorporating real-time sensing, localized processing and autonomous operational capabilities. Consequently, emergency communication systems are progressively evolving into interconnected cyber-physical ecosystems in which networking, sensing, computation, orchestration and intelligent decision-making operate as closely coordinated components. This convergence indicates a broader transition from layer-specific network optimization toward adaptive architectures capable of managing heterogeneous resources across multiple technological domains. Figure 41 demonstrates this architectural shift from isolated protocol-layer optimization toward integrated cross-layer coordination and intelligent orchestration ecosystems.

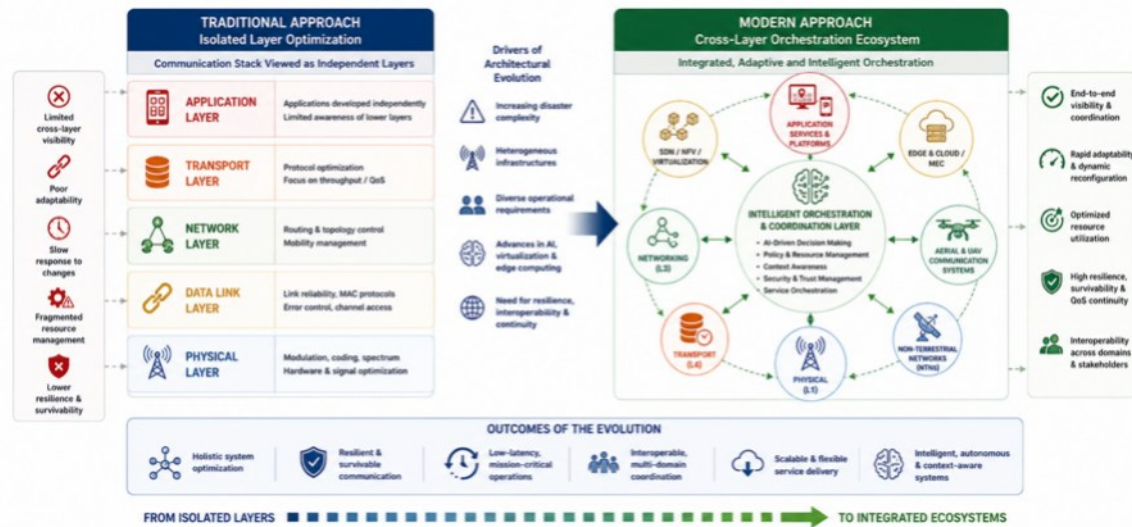


Figure 41 Evolution from Isolated Networking Layers to Cross-Layer Orchestration Ecosystems.

The classification process ultimately enabled quantitative comparison between isolated-layer studies and orchestration-oriented architectures. More importantly, it revealed a broader systemic transition occurring within emergency communication research. The related literature increasingly demonstrates that future crisis communication systems cannot rely on isolated networking mechanisms alone. Instead, they require highly adaptive, resilient, intelligent and distributed orchestration ecosystems capable of maintaining operational continuity under extreme and highly unpredictable conditions [47].

6.1.2 Evaluation Dimensions

Each article in the dataset was evaluated using seven numerical dimensions intended to measure architectural maturity, operational relevance, technical depth, resiliency contribution and deployment realism within emergency communication research. The purpose of this multidimensional scoring process was to transform highly heterogeneous literature into a structured comparative analytical framework capable of revealing broader technological trends and recurring weaknesses across the networking ecosystem.

The evaluation process was intentionally designed to avoid superficial categorization and instead provide a balanced assessment of both technical sophistication and operational applicability. Current emergency communication systems operate under highly unstable and mission-critical conditions where communication infrastructures must maintain continuity despite infrastructure destruction, congestion, mobility disruptions, cyber threats and rapidly evolving operational requirements. As a result, the scoring framework emphasized

not only networking innovation, but also resiliency, interoperability, adaptive orchestration, security integration and deployment maturity.

The first analytical dimension evaluated the depth of technical contribution associated with the dominant network layer. This metric was particularly important because the reviewed studies demonstrated substantial variation in architectural maturity. Some studies simply adapted existing communication technologies to emergency environments without introducing substantial innovation, while others proposed entirely new orchestration mechanisms, distributed communication paradigms, or resilient networking ecosystems. Lower scores were assigned to studies that merely referenced emergency communication scenarios without significantly modifying the underlying networking mechanisms. Moderate scores corresponded to optimization-oriented studies introducing improvements in routing, communication continuity, or resource allocation. Higher scores were reserved for studies presenting architectural innovation, distributed orchestration frameworks, integrated edge-native ecosystems, or novel communication paradigms capable of fundamentally extending the operational capabilities of emergency communication systems. This dimension therefore enabled the distinction between incremental optimization and genuine architectural advancement. It also revealed that the most mature studies increasingly focus on orchestration complexity and distributed resiliency rather than isolated protocol enhancement. The second analytical dimension evaluated operational relevance to emergency and mission-critical communications. This metric distinguished generic networking research from architectures explicitly designed for disaster response environments and mission-critical operational conditions. This distinction was essential because many advanced networking studies investigate sophisticated communication technologies without directly addressing the operational realities of crisis management. Studies receiving high operational relevance scores demonstrated an explicit focus on disaster response, public safety communications, search-and-rescue operations, emergency coordination or communication continuity under degraded infrastructure conditions. These architectures typically addressed operational constraints such as rapid deployment, mobility support, infrastructure fragmentation, communication survivability, low-latency coordination and multi-agency interoperability. In contrast, studies focusing primarily on generic smart-city communication, commercial networking optimization, or conventional wireless communication without explicit emergency applicability received lower scores.

This evaluation dimension therefore ensured that the analysis remained centered on crisis communication systems rather than broader communication technologies lacking direct operational relevance.

The third dimension measured the degree of cross-layer integration. One of the strongest findings throughout the dataset was the progressive transition from isolated protocol-layer optimization toward highly integrated orchestration ecosystems. As a result, evaluating the extent of interaction between networking layers became essential for understanding architectural maturity. Lower scores were assigned to studies focusing exclusively on isolated communication mechanisms without broader orchestration capabilities. Intermediate scores corresponded to partially coordinated architectures integrating limited communication and computational functionalities. The highest scores were assigned to architectures demonstrating adaptive orchestration across multiple networking domains simultaneously.

The strongest cross-layer studies integrated SDN, NFV, MEC, edge computing, AI-driven orchestration, UAV-assisted networking, distributed sensing, virtualization and cyber-physical coordination. This dimension therefore captured the increasing architectural convergence characterizing modern emergency communication research. Another major analytical dimension evaluated contributions related to QoS, resiliency, survivability and fault tolerance. Emergency communication systems frequently operate under conditions involving infrastructure damage, unstable connectivity, overloaded communication channels, mobility disruptions, and cascading service failures. As a result, resiliency-oriented communication mechanisms increasingly represent foundational operational requirements. Studies receiving high scores within this category typically focused on latency reduction, adaptive congestion handling, communication survivability, fault-tolerant orchestration, dynamic rerouting, resilient service continuity, and distributed backup communication infrastructures.

Particular emphasis was placed on architectures capable of preserving operational continuity under degraded or partially destroyed network conditions. This dimension revealed that resiliency engineering has become one of the dominant priorities within next-generation emergency communication research. Cybersecurity and trust-management integration constituted another important analytical dimension. The current emergency communication ecosystems increasingly involve distributed and heterogeneous infrastructures including

UAVs, IoT devices, CPS, virtualized services, edge-computing nodes, satellite communication and distributed orchestration mechanisms.

This convergence significantly expands the attack surface and introduces vulnerabilities related to spoofing, unauthorized access, denial-of-service attacks, communication interception, malicious data manipulation and infrastructure compromise. The framework therefore evaluated the degree to which studies integrated authentication mechanisms, encryption, trust management, anti-jamming strategies, secure routing, blockchain-based security and broader cyber-resilience mechanisms. The analysis demonstrated that although cybersecurity appears increasingly important across the related literature, many architectures still treat security as a partially integrated subsystem rather than a foundational architectural component.

The sixth analytical dimension evaluated AI-driven automation and orchestration maturity. AI increasingly appears as a core enabling technology within emergency communication systems. AI-based mechanisms are progressively applied to intelligent routing, adaptive orchestration, predictive resiliency, congestion mitigation, anomaly detection, autonomous resource allocation and distributed communication management. However, the degree of AI integration varies substantially across the related literature. Some studies apply relatively simple optimization techniques, while others investigate fully adaptive orchestration ecosystems capable of autonomous decision-making under rapidly changing operational conditions. This dimension therefore enabled the identification of emerging intelligent networking paradigms and highlighted the growing transition toward AI-native emergency communication systems. The final analytical dimension evaluated validation strength and deployment maturity. This dimension was especially important because a recurring weakness throughout the dataset involved the dominance of simulation-based evaluation. Many architectures demonstrate strong theoretical or analytical performance but lack realistic operational validation. Lower validation scores were assigned to conceptual or purely analytical studies. Intermediate scores corresponded to simulation-based evaluation and laboratory emulation environments. Higher scores were reserved for pilot deployments, operational exercises, field experimentation and real-world implementations. This distinction is particularly important because emergency communication systems operate under highly unpredictable and hostile conditions that cannot be fully reproduced in controlled simulation environments. Finally, the overall layer maturity score was computed

as the average of all numerical dimensions. This aggregated metric enabled direct comparison between studies with different architectural focuses while preserving analytical consistency across the dataset. More importantly, it provided a structured mechanism for identifying broader technological trajectories, operational limitations, validation weaknesses and underexplored networking domains shaping the future evolution of resilient emergency communication ecosystems.

6.2 Quantitative Distribution of Research Attention Across Network Layers

The analysis of the dataset indicates that recent research activity is increasingly concentrated on cross-layer orchestration architectures rather than isolated networking layers. This shift reflects the growing operational and architectural complexity of modern emergency communication systems, where communication infrastructures no longer function as independent technical entities. Instead, they operate as highly interconnected ecosystems combining networking, computation, sensing, virtualization and intelligent coordination mechanisms. Such architectures are designed to respond dynamically to changing network conditions, infrastructure failures and evolving operational requirements, making cross-layer interaction increasingly important for maintaining reliable mission-critical services. A significant portion of the related literature therefore focuses on architectures that integrate multiple technological domains simultaneously [\[18\]](#), [\[49\]](#). In particular, cross-layer studies frequently combine MEC, SDN, NFV, UAV-assisted communication, AI-driven orchestration, edge computing, CPS, network slicing and distributed edge intelligence within unified operational frameworks. Rather than functioning independently, these technologies increasingly rely on continuous information exchange and adaptive coordination across several networking layers. MEC brings computational capabilities closer to operational environments, while SDN and NFV provide programmable mechanisms for dynamic network configuration and service deployment. In parallel, AI-assisted orchestration can support adaptive resource allocation and network optimization, while UAVs and distributed sensing infrastructures extend connectivity and situational awareness across affected areas. The coordinated interaction of these technologies provides a more flexible architectural foundation for maintaining operational continuity under highly dynamic and infrastructure-degraded emergency conditions.

The second strongest concentration of research activity appears within the Data Link and Network layer domain. Studies in this category primarily investigate mechanisms designed to preserve connectivity, routing stability and communication continuity in environments characterized by mobility, fragmented infrastructure and unstable network conditions [23], [50]. The related literature demonstrates particularly strong interest in UAV-assisted networking, MANETs, aerial base stations, topology-aware routing, mobility-aware communication and resilient wireless architectures capable of adapting to rapidly changing disaster-response scenarios. The prominence of this domain therefore reflects the fundamental importance of maintaining basic connectivity as a prerequisite for higher-level emergency communication services.

By comparison, transport-layer research receives considerably less attention despite its critical role in mission-critical communication environments. Existing studies mainly focus on maintaining QoS, minimizing end-to-end latency, supporting seamless handover between heterogeneous communication infrastructures, managing congestion and preserving service continuity during infrastructure instability [77]. These functions become particularly important when emergency networks simultaneously carry heterogeneous traffic, including voice, telemetry, sensor information and real-time multimedia services with different performance requirements. This imbalance suggests that current research places greater emphasis on architectural integration and connectivity restoration than on transport-level optimization under dynamic disaster conditions. Overall, the distribution across networking layers indicates a broader evolution from conventional layer-specific communication mechanisms toward integrated, adaptive and increasingly intelligent architectures. Cross-layer orchestration appears to represent the most mature direction of this transition, while network-level resilience remains a strong technical priority and transport-layer adaptation presents comparatively greater opportunities for further investigation. Figure 42 illustrates this distribution of research activity across networking layers while highlighting differences in architectural maturity and operational focus throughout the RQ3 dataset.

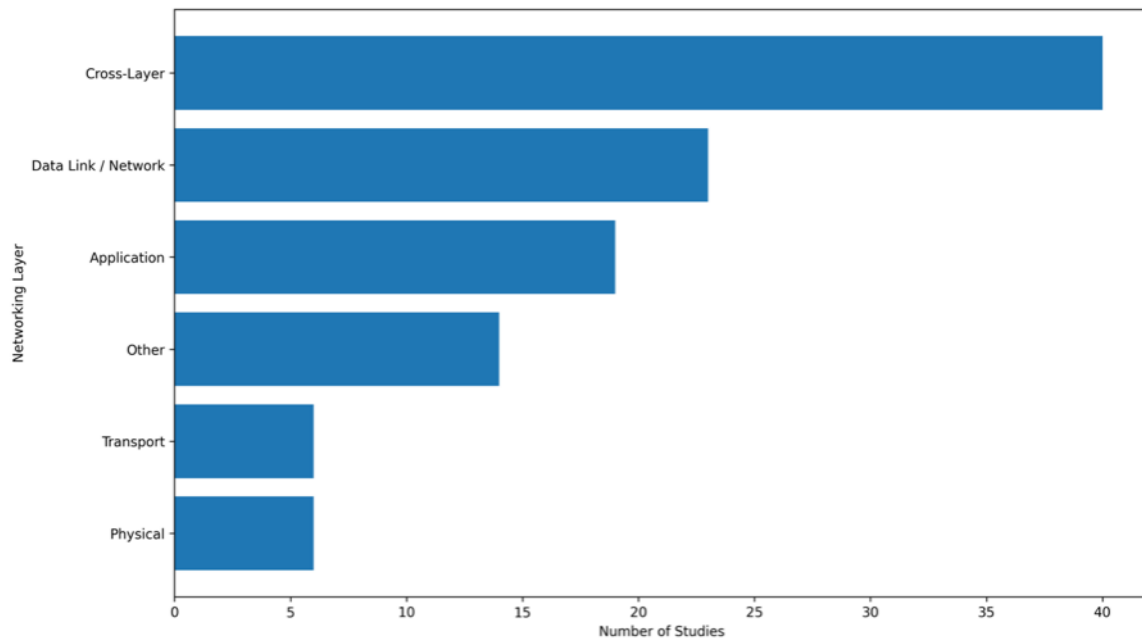


Figure 42 Quantitative Distribution of Research Attention Across Network Layers.

Physical-layer research also appears less dominant throughout the dataset and is often incorporated into broader architectural frameworks rather than investigated as an independent research domain. Most physical-layer contributions focus on communication survivability, resilient wireless transmission, spectrum reliability and satellite-assisted communication under degraded operational conditions [48].

At the application layer, research activity is primarily associated with disaster-management platforms, public-warning infrastructures, situational-awareness systems and intelligent emergency coordination applications. However, the analysis demonstrates that many application-oriented systems increasingly depend on lower-layer resiliency mechanisms, edge-computing support and cross-layer orchestration capabilities in order to achieve reliable real-time operation during crisis scenarios.

Overall, the dataset reveals a clear architectural transition within emergency communication research. Contemporary studies increasingly move away from isolated protocol optimization and instead prioritize integrated orchestration ecosystems capable of dynamically coordinating communication, computation, sensing and intelligent resource management across highly heterogeneous operational environments.

6.2.1 Dominance of Cross-Layer Architectures

Cross-layer architectures receive the highest concentration of research attention because modern emergency communication systems are required to satisfy multiple operational

demands simultaneously. Unlike conventional networking environments, disaster response scenarios involve highly unstable and heterogeneous conditions where communication infrastructures must support ultra-low latency, reliability, scalability, survivability, interoperability, mobility management and cybersecurity under continuous operational stress. This observation is consistently reflected across the reviewed literature, where integrated cross-layer orchestration emerges as the dominant architectural paradigm for mission-critical emergency communications [20], [22], [23].

As a result, recent research increasingly focuses on integrated orchestration ecosystems that combine communication, computation, sensing, virtualization and intelligent resource coordination within unified architectural frameworks. Many studies investigated architectures integrating SDN for centralized orchestration, NFV for flexible service deployment, MEC for low-latency processing, UAV-assisted communication for dynamic coverage extension, AI-driven resource management and distributed sensing infrastructures capable of supporting adaptive disaster response operations [73].

MEC-enabled resilient network slicing architectures further extend this convergence by integrating NFV, SDN, multi-connectivity mechanisms, orchestration frameworks, backup-service continuity strategies and latency-aware resource management into adaptive communication ecosystems capable of dynamically responding to changing disaster conditions.

Overall, the related literature demonstrates that emergency communication research is progressively shifting away from isolated networking optimization and toward orchestration-centric architectural models. Increasing attention is now placed on orchestration complexity, adaptive service management, intelligent edge coordination, distributed resiliency engineering and autonomous resource allocation across heterogeneous operational environments. Cross-layer architectures therefore represent far more than a temporary technological trend. They reflect a broader systemic transformation in the design philosophy of emergency communication systems, where resiliency, intelligence, distributed coordination and operational adaptability increasingly emerge as tightly interconnected architectural requirements.

6.2.2 Data Link and Network Layer Attention

The Data Link and Network layer domain remains one of the most extensively investigated isolated networking categories within the dataset. This strong research concentration reflects

the critical operational role of maintaining communication continuity in highly dynamic and infrastructure-deficient disaster environments. Unlike conventional civilian networking scenarios, emergency communication systems frequently operate under conditions involving damaged infrastructure, fragmented connectivity, unstable mobility patterns and rapidly changing operational requirements [19], [21], [23], [69].

The dominant research themes within this category include UAV-assisted communication, topology-aware networking, aerial base stations, ad hoc communication architectures, mobility-aware routing and resilient wireless coverage mechanisms. A significant portion of the related literature focuses on rapidly deployable networking infrastructures capable of restoring communication services following large-scale disasters or infrastructure failures [42].

Post-disaster environments often experience severe communication disruption caused by destroyed base stations, fragmented terrestrial connectivity, overloaded communication channels and unstable wireless coverage. As a result, UAV-assisted networking has emerged as one of the most prominent research directions within the Data Link and Network layer domain. Many studies investigate the use of unmanned aerial systems as temporary communication relays, aerial base stations, mobile edge nodes, or wireless coverage extenders capable of supporting emergency coordination during critical operational periods. Several studies in the dataset place particular emphasis on aerial communication coverage optimization, UAV trajectory planning, ergodic-capacity analysis, topology-aware deployment strategies, multi-hop communication and adaptive routing mechanisms designed to preserve connectivity under unstable networking conditions. Collectively, these approaches aim to rapidly restore communication continuity and improve operational coordination during disaster response operations. Beyond UAV-assisted networking, several studies also investigate satellite-ground integrated communication architectures to ensure service continuity in geographically isolated or infrastructure-denied environments, further strengthening the resilience of network-layer emergency communications [21], [44]. Despite the high level of research activity, however, several important limitations remain visible throughout the related literature. A large portion of network-layer studies continue to rely heavily on simulation-based evaluation, analytical modeling and theoretical optimization frameworks. In contrast, realistic operational deployments and large-scale field validation remain comparatively limited. The analysis also reveals that many network-layer

architectures still lack advanced orchestration capabilities, autonomous adaptation mechanisms, integrated cybersecurity frameworks and support for large-scale heterogeneous interoperability across multiple communication domains. Consequently, although Data Link and Network layer research remains operationally essential, the related literature increasingly demonstrates a gradual transition toward broader cross-layer orchestration ecosystems capable of integrating communication, computation, sensing and intelligent coordination within unified operational architectures.

6.2.3 Transport-Layer Research Attention

Transport-layer research receives considerably less attention within the dataset when compared with cross-layer orchestration and network-layer communication studies, despite its operational importance for mission-critical emergency communications. Although comparatively few studies explicitly focus on the transport layer, those that do primarily investigate QoS continuity, congestion management, delay-sensitive communications, seamless handover mechanisms and session survivability across heterogeneous communication infrastructures [20], [21], [73].

The dominant research themes within this category include QoS continuity, congestion management, delay-sensitive communication, seamless handover mechanisms and session survivability across heterogeneous communication infrastructures. Many studies focus specifically on maintaining stable communication performance under highly unstable networking conditions where communication links may frequently degrade or become temporarily unavailable [20], [21], [42].

Satellite-ground handover architectures represent one of the most characteristic examples identified within the dataset. These systems aim to preserve communication continuity between terrestrial 5G infrastructures, GEO satellite systems and NTN emergency communication environments. The primary objective of these architectures is to minimize communication interruption, reduce blocking probability, limit latency degradation and maintain QoS consistency during transitions between heterogeneous networking domains. Transport-layer optimization becomes especially critical in operational scenarios involving command-and-control services, emergency response coordination, mission-critical voice communication and real-time situational awareness. In such environments, even short communication interruptions or latency spikes may significantly affect operational effectiveness and decision-making efficiency [73].

Despite its operational significance, however, the analysis reveals several important limitations across the existing transport-layer literature. Many studies remain narrowly scoped, heavily simulation-oriented and insufficiently integrated with broader orchestration ecosystems or AI-driven adaptive management frameworks. In many cases, transport-layer optimization is treated as an isolated communication problem rather than as part of a larger intelligent coordination architecture.

The analysis further demonstrates that transport-layer research rarely incorporates autonomous adaptation mechanisms, integrated cybersecurity frameworks, distributed intelligent coordination, or AI-native resource management capabilities. This observation represents one of the most important research gaps identified throughout the dataset. Future emergency communication systems will increasingly depend on autonomous QoS adaptation, dynamic traffic prioritization, intelligent congestion management and predictive latency-aware orchestration capable of operating under highly unpredictable and degraded operational conditions. Overall, although transport-layer research remains comparatively underdeveloped, its importance is expected to increase significantly as next-generation emergency communication ecosystems evolve toward fully adaptive and AI-driven orchestration environments.

6.2.4 Application-Layer Research Attention

Application-layer research within the dataset primarily focuses on disaster-management intelligence, public warning infrastructures, emergency coordination platforms, citizen-awareness applications, and situational-awareness systems designed to support operational decision-making during crisis events. Unlike the lower networking layers, which primarily concentrate on communication continuity, routing efficiency, and connectivity preservation, application-layer architectures emphasize transforming information into operational knowledge that supports emergency coordination, response management, and real-time situational awareness [\[22\]](#), [\[73\]](#).

A significant portion of the reviewed literature investigates the integration of AI, edge intelligence, Big Data analytics, IoT sensing infrastructures, cloud- and edge-based processing, and predictive disaster-management frameworks into unified emergency-response platforms. Rather than functioning solely as communication endpoints, these systems increasingly transform raw communication and sensor data into actionable

operational intelligence capable of supporting faster, more accurate, and context-aware decision-making during highly dynamic emergency scenarios [73].

Application-layer architectures are particularly important because they directly support several mission-critical operational functions, including emergency coordination, resource allocation, disaster monitoring, situational-awareness generation, decision support, and public information dissemination. Numerous studies further investigate intelligent dashboards, AI-assisted coordination platforms, and integrated command-and-control environments capable of aggregating heterogeneous communication, sensing, and operational data streams in real time to improve emergency response effectiveness.

At the same time, the analysis demonstrates that modern application-layer systems are becoming progressively dependent on lower-layer networking and orchestration mechanisms. In practice, disaster-management applications cannot operate effectively without resilient wireless connectivity, low-latency communications, edge-computing support, QoS continuity, and distributed orchestration capabilities capable of maintaining reliable system performance under degraded operational conditions. This growing dependency highlights that application-layer intelligence is no longer developed independently but increasingly relies on tightly integrated communication and computing infrastructures.

Consequently, application-layer research is progressively converging toward broader cross-layer architectural ecosystems in which communication, computation, sensing, AI-driven intelligence, and orchestration operate as tightly interconnected components rather than as isolated functional entities. This finding is also consistent with the advanced paradigms identified in RQ2, where AI-native networking, edge intelligence, SDN/NFV orchestration, and cyber-physical integration collectively redefine the architecture of next-generation emergency communication systems. Overall, the findings reinforce the broader architectural transition identified throughout the dataset, namely the shift from isolated networking mechanisms toward integrated, intelligent, adaptive, and highly resilient emergency communication ecosystems capable of supporting mission-critical operations under highly dynamic disaster conditions.

6.3 Final Answer to RQ3

The analysis conducted throughout Chapter 6 demonstrates that contemporary emergency communication research is increasingly dominated by cross-layer orchestration

architectures rather than isolated networking-layer optimization. This transition reflects the growing operational complexity of modern disaster response environments, where communication systems must simultaneously support ultra-low latency, reliability, scalability, interoperability, survivability, mobility management, cybersecurity, distributed sensing and autonomous coordination under highly unstable operational conditions.

Among all networking domains, cross-layer architectures receive the highest level of research attention. The related literature consistently demonstrates a strong convergence between SDN, NFV, MEC, UAV-assisted communication, AI-driven orchestration, edge computing, CPS, network slicing and distributed intelligent infrastructures. Rather than operating independently, these technologies increasingly function as tightly integrated orchestration ecosystems capable of dynamically coordinating communication, computation, sensing, virtualization and intelligent resource management across heterogeneous disaster environments.

The second strongest concentration of research activity appears within the Data Link and Network layer domain. Research in this category focuses heavily on maintaining communication continuity under infrastructure-deficient conditions through UAV-assisted networking, aerial base stations, ad hoc communication architectures, topology-aware routing, multi-hop networking and mobility-aware communication mechanisms. The dataset demonstrates that UAV-assisted networking has emerged as one of the dominant architectural directions because unmanned aerial systems can rapidly restore communication coverage and support emergency coordination when terrestrial infrastructures become unavailable.

Application-layer research also receives substantial attention, particularly in relation to disaster-management intelligence, situational-awareness systems, emergency coordination platforms, public-warning infrastructures and AI-assisted operational decision support. However, the analysis reveals that modern application-layer ecosystems increasingly depend on resilient lower-layer infrastructures, edge-computing support, distributed orchestration and low-latency communication mechanisms in order to operate effectively under crisis conditions.

In contrast, transport-layer research remains comparatively underexplored despite its operational importance for mission-critical communication environments. Existing studies primarily investigate QoS continuity, congestion management, delay-sensitive

communication, seamless handover and session survivability across heterogeneous terrestrial and non-terrestrial infrastructures. Nevertheless, most transport-layer contributions remain narrowly scoped, heavily simulation-oriented and insufficiently integrated with broader orchestration ecosystems, AI-driven adaptive management, cybersecurity mechanisms, or autonomous coordination capabilities.

Physical-layer research receives relatively lower attention and is frequently incorporated within broader orchestration-oriented architectures rather than investigated independently. Most physical-layer studies focus on communication survivability, resilient wireless transmission, spectrum reliability, anti-jamming resilience and satellite-assisted communication under degraded operational conditions.

Another major limitation concerns the incomplete integration of cybersecurity and trust-management mechanisms. Although security increasingly appears within modern emergency communication architectures, many studies still treat cybersecurity as an auxiliary subsystem rather than as a foundational architectural component integrated across all networking layers. Similar limitations appear in relation to autonomous orchestration and AI-native coordination. While AI-assisted optimization is becoming increasingly common, fully autonomous adaptive orchestration ecosystems capable of predictive resiliency management and distributed intelligent coordination remain relatively immature.

The findings therefore demonstrate that emergency communication research is undergoing a broader systemic transformation from isolated protocol-centric networking approaches toward highly adaptive, intelligent and distributed orchestration ecosystems. Future crisis communication systems will increasingly depend on the seamless convergence of networking, edge intelligence, distributed sensing, AI-driven orchestration, cyber resilience and autonomous operational coordination across heterogeneous terrestrial and non-terrestrial infrastructures. However, despite the substantial architectural sophistication demonstrated throughout the related literature, the transition from experimental frameworks toward fully operational resilient emergency communication ecosystems remains an ongoing challenge for both academia and industry.

7. Conclusions and Future Research Directions

This dissertation investigated the evolving role of advanced communication technologies in man-made disaster environments, focusing on the transition from conventional public safety communication systems toward intelligent, distributed and highly adaptive mission-critical ecosystems. The study systematically analyzed how modern emergency communication architectures integrate 5G, emerging 6G paradigms, MEC, AI-native networking, UAV-assisted communication, NTN, CPS and cross-layer orchestration mechanisms in order to address the increasing operational complexity of disaster response environments.

The findings demonstrate that contemporary emergency communication systems are undergoing a profound architectural transformation. Traditional communication infrastructures based primarily on isolated radio systems and static networking architectures are progressively evolving into integrated cyber-physical ecosystems combining communication, sensing, computation, orchestration and intelligent decision-support mechanisms within unified operational environments. This transformation is driven by the growing operational demands associated with modern disasters, where communication systems must simultaneously support ultra-low latency, interoperability, scalability, survivability, distributed situational awareness, autonomous coordination and resilient service continuity under highly unstable operational conditions.

The overall analysis further demonstrates that future disaster communication ecosystems will increasingly depend on the convergence of distributed intelligence, AI-driven orchestration, edge computing, UAV-enabled networking, IoT sensing infrastructures and non-terrestrial communication systems operating within highly heterogeneous and dynamically coordinated environments. Rather than functioning as isolated communication technologies, modern emergency communication systems increasingly operate as intelligent operational ecosystems capable of adaptive coordination and autonomous resilience management.

7.1 Conclusions Related to RQ1

The analysis presented in Chapter 4 revealed that simulation-based evaluation remains the dominant validation methodology across the majority of contemporary emergency communication studies. Most research contributions rely primarily on analytical models, synthetic traffic generation, network simulators and controlled emulation environments in

order to evaluate routing protocols, QoS management mechanisms, orchestration strategies, UAV-assisted communication architectures, AI-driven optimization frameworks and resilient networking approaches for disaster response operations.

This strong dependence on simulation-oriented evaluation is largely understandable. Emergency communication systems are designed to operate under highly complex and unpredictable conditions that are extremely difficult to reproduce in real-world environments. Large-scale disasters often involve damaged infrastructures, unstable communication links, mobility disruptions, overloaded networks, environmental interference and rapidly evolving operational conditions. Conducting realistic field experiments under such circumstances is not only financially demanding, but in many cases operationally dangerous or practically infeasible. Consequently, simulation environments provide researchers with a controlled and cost-effective mechanism for investigating system behavior under a wide range of hypothetical disaster scenarios.

Simulation-based methodologies also offer several important scientific advantages. They allow repeatable experimentation, precise parameter control, scalability analysis and comparative evaluation across different architectural approaches. Researchers can therefore examine how communication systems behave under varying levels of congestion, infrastructure failure, mobility conditions, or communication interference without the logistical complexity associated with large operational deployments. This methodological flexibility has significantly accelerated innovation within the field of emergency communications and has enabled the rapid exploration of advanced technologies such as AI-native networking, UAV-assisted relays, edge orchestration, network slicing and distributed cyber-physical coordination.

However, despite these advantages, the analysis also demonstrated that simulation-oriented validation introduces important limitations regarding the generalizability and operational realism of research findings. Many proposed architectures demonstrate strong theoretical or simulated performance but remain insufficiently validated under realistic disaster response conditions. In practice, emergency environments are influenced by a wide range of unpredictable operational variables that are difficult to model accurately within controlled simulation environments.

Several important operational dimensions remain comparatively underexplored throughout the related literature. These include the effects of infrastructure degradation under real

disaster conditions, the influence of unpredictable human behavior during crisis situations, the complexity of multi-agency interoperability, unstable communication availability, cyber-physical coordination failures, environmental interference and the scalability challenges associated with large heterogeneous emergency-response deployments. In real-world operations, communication systems must often function across fragmented infrastructures involving police forces, firefighters, healthcare providers, military units, civil protection agencies and critical infrastructure operators operating simultaneously under extreme time pressure and incomplete situational awareness. Such operational complexity is rarely reproduced comprehensively within simulation-based evaluation frameworks.

The findings therefore reveal a substantial gap between theoretical architectural sophistication and practical deployment maturity. Although modern emergency communication research demonstrates a high degree of technological innovation, many proposed solutions remain experimentally immature when evaluated from the perspective of real-world disaster response applicability. In many cases, architectures that appear highly efficient within controlled simulation environments may encounter significant operational limitations when exposed to infrastructure instability, unpredictable mobility patterns, human decision-making constraints, or large-scale interoperability requirements during actual emergencies.

For this reason, future research must progressively move beyond purely simulation-oriented evaluation and prioritize more operationally realistic validation approaches. Greater emphasis should be placed on large-scale pilot deployments, field experimentation, interoperability exercises and real-world emergency-response validation environments capable of testing communication architectures under realistic operational stress. Hybrid evaluation ecosystems combining digital twins, AI-driven simulation, edge-based emulation and operational field testing may provide a more balanced and realistic validation methodology for next-generation emergency communication systems.

At the same time, future evaluation frameworks should adopt a more multidisciplinary perspective integrating technical, organizational, operational and human-centric dimensions simultaneously. Emergency communication systems do not operate purely as networking infrastructures, they function within highly complex socio-technical ecosystems involving human decision-making, institutional coordination, operational doctrine and dynamic crisis management processes. Consequently, improving the realism and generalizability of future

emergency communication research will require closer integration between communication engineering, AI, cyber-physical systems, disaster management and operational field practice.

7.2 Conclusions Related to RQ2

The findings presented in Chapter 5 demonstrate that contemporary emergency communication research is increasingly shaped by deep technological convergence rather than isolated technological innovation. Modern emergency communication architectures no longer approach networking, sensing, computation, orchestration and operational coordination as independent technical domains. Instead, recent research increasingly integrates multiple advanced technologies into unified and highly interconnected operational ecosystems capable of supporting complex disaster response environments.

This transition reflects the growing realization that modern crises require far more than conventional communication connectivity alone. Large-scale emergencies involve rapidly changing operational conditions, fragmented infrastructures, unstable communication availability, dynamic mobility patterns and the simultaneous coordination of multiple heterogeneous actors. As a result, communication systems are progressively evolving into intelligent cyber-physical ecosystems where communication, computation, sensing, analytics and decision-making mechanisms operate together in a coordinated manner.

One of the strongest technological trends identified throughout the dataset is the emergence of AI-native networking and intelligent orchestration architectures. AI increasingly functions as a central enabling mechanism within modern emergency communication systems rather than as an auxiliary optimization tool. Across the related literature, AI-driven architectures support adaptive resource allocation, predictive congestion management, autonomous routing optimization, intelligent QoS enforcement, distributed resiliency engineering, edge orchestration, anomaly detection and predictive situational awareness generation.

The growing integration between AI and MEC represents one of the most important architectural developments identified in the analysis. By combining AI-based analytics with edge-computing infrastructures located near the disaster area, modern emergency communication systems can process operational data locally and support distributed real-time decision-making without relying exclusively on centralized cloud infrastructures. This convergence significantly improves operational responsiveness, reduces communication

latency, enhances service continuity under degraded networking conditions and enables partial operational autonomy even when communication links to centralized infrastructures become unstable or unavailable.

Another major architectural trend involves the rapid expansion of UAV-assisted communication ecosystems and the integration of NTN. The analysis demonstrated that unmanned aerial systems increasingly function as multifunctional operational platforms capable of supporting communication, sensing, coordination and infrastructure recovery simultaneously. Modern UAV-based architectures are no longer limited to simple communication relays. Instead, UAVs increasingly operate as aerial base stations, temporary communication extenders, airborne sensing platforms, mobile edge-computing nodes, distributed telemetry collectors and adaptive infrastructure-recovery mechanisms during disaster response operations.

At the same time, NTN and SAGIN architectures significantly improve communication survivability by integrating terrestrial, aerial and satellite communication infrastructures within unified operational environments. These architectures are especially important during large-scale disasters where terrestrial communication infrastructures may become partially destroyed or completely unavailable. By extending communication coverage beyond conventional terrestrial limitations, NTN-enabled systems improve communication continuity, operational coordination and disaster-area connectivity under highly degraded conditions.

The research also demonstrated growing interest in blockchain-enabled trust mechanisms and secure distributed coordination frameworks. As emergency communication ecosystems become increasingly distributed and heterogeneous, the need for trusted coordination and secure information exchange becomes substantially more important. Blockchain-based architectures increasingly support decentralized authentication, distributed access control, trusted operational logging, secure information sharing and resilient coordination among heterogeneous stakeholders operating across multiple communication domains.

This trend is particularly important because future disaster response ecosystems will likely involve highly decentralized operational environments integrating public authorities, emergency responders, critical infrastructure operators, autonomous systems, UAV swarms, IoT infrastructures and distributed edge-computing platforms simultaneously. Under such conditions, centralized trust management mechanisms may become operationally

insufficient or vulnerable to disruption. Blockchain-enabled coordination frameworks therefore represent an important step toward resilient and distributed trust management within future emergency communication ecosystems.

Furthermore, the convergence of ISAC, digital twins, CPS, IoT-enabled sensing infrastructures and intelligent situational-awareness platforms collectively indicates that future emergency communication systems are evolving toward fully integrated cyber-physical operational environments. These emerging ecosystems increasingly combine communication, distributed intelligence, sensing, autonomous coordination, predictive analytics and operational awareness within unified adaptive infrastructures capable of continuously responding to rapidly changing disaster conditions.

Overall, the findings of Chapter 5 demonstrate that the future of emergency communications will not depend solely on faster networking infrastructures or isolated protocol optimization. Instead, next-generation disaster response ecosystems will increasingly rely on the deep integration of AI, edge computing, UAV-assisted networking, distributed sensing, blockchain-enabled trust management and intelligent orchestration mechanisms operating together within highly adaptive and resilient cyber-physical environments.

7.3 Conclusions Related to RQ3

The analysis conducted in Chapter 6 demonstrated that cross-layer orchestration architectures currently receive the highest concentration of research attention within contemporary emergency communication literature. This finding reflects a broader architectural transition occurring across the field of crisis communications. Researchers increasingly recognize that isolated protocol optimization is no longer sufficient for addressing the operational complexity of modern disaster environments, where communication systems must function under conditions of infrastructure instability, mobility disruptions, heterogeneous networking environments and rapidly changing operational requirements.

Traditional communication architectures typically focused on improving the performance of individual networking layers independently. However, modern emergency communication ecosystems require continuous interaction between communication, computation, sensing, orchestration and intelligent resource management mechanisms. As a result, recent research increasingly prioritizes integrated orchestration environments

capable of dynamically coordinating heterogeneous infrastructures and distributed operational resources under highly unstable conditions.

The findings revealed particularly strong research interest in technologies associated with cross-layer orchestration and distributed intelligent coordination. Modern emergency communication systems increasingly prioritize SDN and NFV orchestration mechanisms, MEC-enabled distributed intelligence, AI-native networking architectures, UAV-assisted communication ecosystems, IoT integration, CPS coordination, edge-cloud convergence and interoperability between terrestrial and non-terrestrial communication infrastructures.

These technologies are rarely investigated as isolated architectural components. Instead, the related literature increasingly approaches them as tightly interconnected operational ecosystems where communication infrastructures, edge computing, sensing platforms, virtualization frameworks and AI-driven coordination mechanisms operate together in order to preserve communication continuity and operational effectiveness during crisis situations. The Data Link and Network layers also receive extensive research attention throughout the dataset. This strong concentration reflects the operational importance of maintaining resilient connectivity under disaster conditions where conventional terrestrial infrastructures may become degraded, fragmented, or completely unavailable. In particular, a substantial portion of the related literature focuses on UAV-assisted networking, topology-aware routing, resilient wireless coverage mechanisms, multi-hop communication architectures, ad hoc networking environments and infrastructure-independent communication systems capable of rapidly restoring operational connectivity during emergency-response operations.

UAV-assisted networking emerged as one of the most dominant architectural directions within this category. Modern unmanned aerial systems increasingly function not only as communication relays, but also as aerial base stations, mobile edge-computing platforms, distributed sensing nodes and adaptive communication extenders capable of supporting dynamic disaster response coordination under highly unstable operational conditions.

In contrast, transport-layer research remains comparatively underdeveloped despite its critical importance for mission-critical communication environments. Existing transport-layer studies primarily focus on QoS continuity, congestion management, latency-sensitive communication, seamless handover mechanisms and session survivability across heterogeneous communication infrastructures. These functions are particularly important

for command-and-control systems, real-time situational awareness, mission-critical voice communication and emergency coordination services where communication interruptions or latency degradation may significantly affect operational effectiveness.

Nevertheless, the analysis demonstrated that transport-layer adaptation remains relatively isolated from the broader architectural evolution occurring across emergency communication research. Most transport-layer studies remain heavily optimization-oriented and rarely integrate AI-native orchestration, autonomous coordination mechanisms, predictive resiliency management, distributed operational intelligence, or integrated cybersecurity ecosystems. As a result, transport-layer research currently represents one of the most important underexplored domains within next-generation emergency communication architectures.

A similar observation applies to application-layer systems. Although modern application-layer architectures increasingly support advanced situational-awareness generation, intelligent coordination services, disaster-management platforms and AI-assisted decision-support systems, their operational effectiveness remains highly dependent on lower-layer communication resilience and orchestration mechanisms. In practice, application-layer intelligence cannot function effectively without reliable wireless connectivity, resilient edge processing, low-latency communication and adaptive infrastructure coordination operating beneath the application environment.

Another critical limitation identified throughout the related literature concerns operational validation maturity. Although many proposed architectures demonstrate substantial technological sophistication, large-scale field validation and real-world operational deployment remain comparatively limited. Most studies continue to rely heavily on simulation-based evaluation, analytical modeling, or controlled laboratory experimentation. Consequently, several important operational dimensions remain insufficiently validated, including large-scale interoperability, multi-agency coordination, infrastructure degradation, communication instability, human behavioral uncertainty and operational scalability under realistic disaster conditions.

The findings therefore reveal a substantial gap between architectural innovation and deployment maturity. While contemporary emergency communication research demonstrates significant progress toward intelligent, distributed and highly adaptive communication ecosystems, many proposed solutions remain insufficiently validated for

real-world operational deployment. Future research must therefore place greater emphasis on operational realism, interdisciplinary validation methodologies, autonomous orchestration capabilities, integrated cyber resilience and large-scale deployment experimentation capable of bridging the gap between theoretical architectural sophistication and practical disaster response applicability.

7.4 Conclusions Related to Stakeholder Communication Needs

The analysis showed that modern disaster communication systems must address a wide range of heterogeneous operational requirements across multiple stakeholder groups operating under crisis conditions. Unlike conventional communication infrastructures designed primarily for stable civilian environments, emergency communication ecosystems must support the coordinated interaction of public authorities, first responders, citizens, healthcare services, military units and critical infrastructure operators, all of whom possess different operational priorities, communication requirements and decision-making responsibilities during disaster response operations.

As a result, contemporary emergency communication architectures are increasingly evolving into integrated, multi-domain coordination ecosystems that support differentiated operational functions across highly dynamic and unstable environments. Rather than operating as isolated telecommunications systems, modern emergency communication platforms increasingly function as interconnected operational infrastructures combining communication, sensing, distributed intelligence, orchestration and real-time situational awareness within unified crisis-management environments.

For public authorities and governmental coordination centers, communication systems primarily emphasize strategic situational awareness, large-scale operational coordination, inter-agency interoperability, predictive analytics, distributed command-and-control and real-time operational visibility. During large-scale emergencies, governmental agencies must continuously coordinate multiple organizations simultaneously, including emergency responders, healthcare services, transportation authorities, civil protection organizations, military units and infrastructure operators. Under such conditions, communication systems must support not only reliable information exchange, but also adaptive operational management and rapid decision-making under uncertainty.

The analysis demonstrated that AI-driven orchestration mechanisms, digital twins, edge analytics and integrated situational-awareness platforms increasingly support these strategic

operational functions. By aggregating information from distributed sensing infrastructures, communication networks, UAV platforms, IoT ecosystems and operational telemetry systems, modern disaster-management platforms significantly improve the ability of public authorities to monitor evolving crisis conditions, allocate resources dynamically and coordinate large-scale emergency-response operations in real time.

For first responders, the operational priorities are substantially different and far more time-critical. Mission-critical communication environments require URLLC, resilient mobile connectivity, uninterrupted voice and video communication, autonomous coordination and continuous situational awareness even under degraded infrastructure conditions. Firefighters, police units, medical teams, military personnel and search-and-rescue operators frequently operate in highly unstable environments where communication interruptions may directly affect operational effectiveness and human safety.

The findings revealed that technologies such as 5G PPDR architectures, network slicing, MEC-enabled edge processing, UAV-assisted relays and NTN-based communication infrastructures increasingly support these operational requirements. These technologies improve communication survivability, support distributed field coordination, reduce latency and enable more resilient communication continuity in environments where conventional terrestrial infrastructures may become damaged or unavailable.

The analysis also demonstrated the growing importance of communication technologies for affected civilian populations. For citizens, modern emergency communication systems increasingly support public-warning dissemination, emergency alerting, real-time information access, evacuation coordination and crisis-awareness services. During disasters, civilians require immediate access to reliable and continuously updated information regarding evacuation routes, infrastructure disruptions, healthcare availability, environmental hazards and emergency-response instructions.

Application-layer systems integrating IoT sensing infrastructures, AI-based analytics, cloud-edge coordination and public safety communication platforms increasingly improve communication transparency and situational awareness for affected populations. In many cases, modern emergency communication architectures also support bidirectional communication, allowing citizens not only to receive alerts, but also to transmit emergency information, situational updates and distress signals to operational coordination centers.

For infrastructure operators, communication systems focus primarily on maintaining operational continuity and protecting critical infrastructures under crisis conditions. Energy grids, transportation systems, industrial facilities, healthcare infrastructures, telecommunications networks and water-distribution systems increasingly depend on resilient communication ecosystems capable of supporting continuous monitoring, predictive maintenance, distributed sensing, cyber resilience and adaptive infrastructure management during emergencies.

The integration of CPS, IoT ecosystems, distributed telemetry, AI-based anomaly detection and edge-enabled monitoring architectures significantly improves the resilience and adaptive management capabilities of critical infrastructures. These technologies allow infrastructure operators to identify failures rapidly, isolate damaged system components, optimize recovery procedures and maintain partial operational continuity even under degraded conditions.

Overall, the findings demonstrate that modern emergency communication ecosystems are progressively evolving beyond traditional telecommunications infrastructures toward integrated multi-stakeholder operational environments. Future disaster response systems will increasingly depend on the ability to coordinate heterogeneous communication, sensing, computational and decision-support mechanisms simultaneously while addressing the distinct operational requirements of governmental authorities, first responders, citizens and critical infrastructure operators within highly dynamic and uncertain crisis environments.

7.5 Final Remarks

Overall, this dissertation demonstrates that emergency communication research is undergoing a rapid and fundamental architectural transformation toward highly integrated, intelligent and orchestration-centric operational ecosystems. Modern emergency communication systems are no longer designed solely as networking infrastructures responsible for transmitting information between isolated communication nodes. Instead, they are progressively evolving into complex cyber-physical ecosystems that combine communication, sensing, distributed computation, AI, autonomous coordination and real-time operational awareness within unified and adaptive disaster response environments.

The findings of this dissertation reveal that the future of disaster response communication will not depend exclusively on faster wireless connectivity or isolated protocol optimization.

While advances in communication performance remain important, future resilient emergency ecosystems will increasingly rely on the seamless integration of cross-layer orchestration, AI-native networking, edge intelligence, cyber-physical coordination, autonomous operational management and adaptive multi-domain resiliency mechanisms capable of operating under highly dynamic and degraded conditions.

One of the most important conclusions emerging from the analysis is that communication infrastructures are becoming deeply interconnected with distributed intelligence and operational decision-making processes. Technologies such as MEC, AI-driven orchestration, UAV-assisted communication, non-terrestrial networking, IoT sensing ecosystems, digital twins and cyber-physical coordination frameworks are progressively transforming emergency communication systems from reactive infrastructures into predictive and partially autonomous operational environments. These architectures increasingly support real-time situational awareness, adaptive resource allocation, intelligent congestion management, distributed sensing, predictive failure analysis and resilient coordination across heterogeneous operational domains.

At the same time, the dissertation demonstrates that substantial challenges remain unresolved despite the significant technological progress achieved in recent years. One of the most persistent limitations identified throughout the related literature concerns operational validation maturity. A large portion of contemporary emergency communication research continues to rely heavily on simulations, analytical models and controlled experimental environments, while realistic field deployments and large-scale operational validation remain comparatively limited. As a result, the practical applicability and scalability of many proposed architectures under real disaster conditions remain insufficiently verified.

Additional challenges involve the integration of cybersecurity and trust-management mechanisms across increasingly distributed and heterogeneous operational ecosystems. As emergency communication architectures evolve toward AI-native and highly interconnected infrastructures, the attack surface expands significantly, introducing vulnerabilities related to unauthorized access, malicious data manipulation, denial-of-service attacks, communication interception and infrastructure compromise. The findings demonstrated that cybersecurity remains insufficiently integrated into many proposed architectures and is

often treated as an auxiliary subsystem rather than as a foundational architectural requirement.

The analysis also revealed important limitations regarding autonomous resiliency management, large-scale interoperability, transport-layer intelligence and real-world deployment scalability. Although modern communication systems increasingly incorporate intelligent orchestration and distributed coordination mechanisms, fully autonomous disaster response ecosystems capable of predictive adaptation and self-organizing operational coordination remain relatively immature. Similarly, interoperability between heterogeneous communication domains, agencies, infrastructures and operational stakeholders continues to represent a major technical and organizational challenge.

Consequently, the evolution toward fully operational AI-native 6G disaster ecosystems remains an ongoing multidisciplinary challenge that extends far beyond conventional communication engineering alone. Future disaster response architectures will require the close integration of networking technologies, AI, cyber-physical systems, operational doctrine, public safety policy, distributed sensing, resilient infrastructure engineering and human-centric crisis management methodologies within unified operational frameworks.

Ultimately, this dissertation demonstrates that the future of emergency communications lies in the development of intelligent, resilient, adaptive and deeply interconnected operational ecosystems capable of continuously coordinating communication, sensing, computation and decision-making processes under highly uncertain and rapidly evolving disaster conditions. The transition toward such ecosystems represents not only a technological evolution, but also a broader transformation in the philosophy of crisis management itself, where communication infrastructures increasingly function as the cognitive and operational backbone of future disaster response environments.

References

- [1] Mehmet Ulema, *Fundamentals of public safety networks and critical communications systems : technologies, deployment, and management*. Piscataway, IEEE Press, Hoboken, New Jersey, 2019.
- [2] M. Kordi and M. Ertz, “Deciphering technological advancements for efficient disaster management and community resilience” *Technology in Society*, vol. 84, p. 103057, Mar. 2026, doi: <https://doi.org/10.1016/j.techsoc.2025.103057>.
- [3] S. Rani *et al*, “A new generation cyber-physical system: A comprehensive review from security perspective,” *Computers & Security*, vol. 148, p. 104095, Jan. 2025, doi: <https://doi.org/10.1016/j.cose.2024.104095>.
- [4] Abdulrahman Yarali, *Public Safety Networks from LTE To 5G*. Hoboken, NJ: John Wiley & Sons, 2019.
- [5] D. Fischer-Preßler *et al*, “Digital transformation in disaster management: A literature review” *The Journal of Strategic Information Systems*, vol. 33, no. 4, p. 101865, Oct. 2024, doi: <https://doi.org/10.1016/j.jsis.2024.101865>.
- [6] N. H. Mahmood *et al*, *Wireless Networks and Industrial IoT*. University of the West of Scotland, 2020.
- [7] S. Majumdar *et al*, “First Responder Communication Systems: A Technical Analysis of Interoperability and Situational Awareness Optimization” *2022 IEEE 12th Annual Computing and Communication Workshop and Conference*, pp. 00331–00339, Jan. 2025, doi: <https://doi.org/10.1109/ccwc62904.2025.10903555>.
- [8] Q. Wang *et al*, “An Overview of Emergency Communication Networks” *Remote Sensing*, vol. 15, no. 6, pp. 1595–1595, Mar. 2023, doi: <https://doi.org/10.3390/rs15061595>.
- [9] F. Neto *et al*, “A Survey on Security Approaches on PPDR Systems Toward 5G and Beyond” *IEEE Access*, vol. 10, pp. 117118–117140, 2022, doi: <https://doi.org/10.1109/access.2022.3217223>.
- [10] Salwa Saafi, *et al*, “Enabling Next-Generation Public Safety Operations with Mission-Critical Networks and Wearable Applications,” *Sensors*, vol. 21, no. 17, pp. 5790–5790, Aug. 2021, doi: <https://doi.org/10.3390/s21175790>.
- [11] B. Kożuch and K. Sienkiewicz-Małyjurek, “Building collaborative trust in public safety networks” *Safety Science*, vol. 152, p. 105785, Aug. 2022, doi: <https://doi.org/10.1016/j.ssci.2022.105785>.

- [12] K. Saini *et al*, “Disaster emergency response framework for smart buildings” *Future Generation Computer Systems*, vol. 131, pp. 106–120, Jun. 2022, doi: <https://doi.org/10.1016/j.future.2022.01.015>.
- [13] K. Ali *et al.*, “Review and Implementation of Resilient Public Safety Networks: 5G, IoT, and Emerging Technologies” *IEEE Network*, vol. 35, no. 2, pp. 18–25, Mar. 2021, doi: <https://doi.org/10.1109/mnet.011.2000418>.
- [14] F. Franchi *et al*, “A Survey of Cloud-Enabled GIS Solutions Toward Edge Computing: Challenges and Perspectives,” *IEEE open journal of the Communications Society*, vol. 5, pp. 312–331, Jan. 2024, doi: <https://doi.org/10.1109/ojcoms.2023.3344198>.
- [15] M. Matraccia *et al*, “Post-Disaster Communications: Enabling Technologies, Architectures, and Open Challenges,” *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1177–1205, 2022, doi: <https://doi.org/10.1109/ojcoms.2022.3192040>.
- [16] Sayaka Hinata *et al*, “Communicating with the public in emergencies: A systematic review of communication approaches in emergency response” *International Journal of Disaster Risk Reduction*, vol. 111, pp. 104719–104719, Aug. 2024, doi: <https://doi.org/10.1016/j.ijdr.2024.104719>.
- [17] F. Rastoceanu *et al*, “Mission-Critical Services in 4G/5G and Beyond: Standardization, Key Challenges, and Future Perspectives” *Sensors*, vol. 25, no. 16, pp. 5156–5156, Aug. 2025, doi: <https://doi.org/10.3390/s25165156>.
- [18] P. K. Thiruvassagam *et al*, “Resilient and Latency-Aware Orchestration of Network Slices Using Multi-Connectivity in MEC-Enabled 5G Networks” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2502–2514, Sep. 2021, doi: <https://doi.org/10.1109/tnsm.2021.3091053>.
- [19] J. Bravo-Arrabal *et al*, “The Internet of Cooperative Agents Architecture for Robots, Hybrid Sensor Networks, and MEC Centers in Complex Environments: A Search and Rescue Case Study” *Sensors (Basel)*, vol. 21, no. 23, pp. 7843–7843, Nov. 2021, doi: <https://doi.org/10.3390/s21237843>.
- [20] M. M. Alsayyed *et al*, “A Review of Applicable Technologies, Routing Protocols, Requirements, and Architecture for Disaster Area Networks” *IEEE Access*, pp. 1–1, Jan. 2025, doi: <https://doi.org/10.1109/access.2025.3570733>.
- [21] D. K. R. and S. Chavhan, “Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts” *Sustainable Energy Technologies and Assessments*, vol. 54, p. 102666, Dec. 2022, doi: <https://doi.org/10.1016/j.seta.2022.102666>.

- [22] Y. Zhou and X. Chen, "Edge Intelligence: Edge Computing for 5G and the Internet of Things" *Future Internet*, vol. 17, no. 3, p. 101, Feb. 2025, doi: <https://doi.org/10.3390/fi17030101>.
- [23] M. Matracia, *et al*, "On the Topological Aspects of UAV-Assisted Post-Disaster Wireless Communication Networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 59–64, Nov. 2021, doi: <https://doi.org/10.1109/mcom.121.2100166>.
- [24] S. P. Dash *et al*, "Introduction to integrated sensing and communications for the next generation of wireless connectivity" *Elsevier eBooks*, pp. 1–32, Jan. 2025, doi: <https://doi.org/10.1016/b978-0-44-322143-9.00007-2>.
- [25] P. Loganathan *et al*, "Towards 6G technologies: Insight into architecture, communication, AI applications and use cases" *Advances in Computers*, pp. 561–583, 2025, doi: <https://doi.org/10.1016/bs.adcom.2025.03.018>.
- [26] H. Shin *et al.*, "The future service scenarios of 6G telecommunications technology" *Telecommunications Policy*, vol. 48, no. 2, pp. 102678–102678, Mar. 2024, doi: <https://doi.org/10.1016/j.telpol.2023.102678>.
- [27] S. Zyoud and A. H. Zyoud, "Advancing sustainable cities and communities with internet of things: Global insights, trends, and research priorities for SDG 11" *Results in Engineering*, vol. 26, p. 104917, Jun. 2025, doi: <https://doi.org/10.1016/j.rineng.2025.104917>.
- [28] S. Kumar Jagatheesaperumal *et al*, "Blockchain-Based Security Architecture for Uncrewed Aerial Systems in B5G/6G Services and Beyond: A Comprehensive Approach" *IEEE Open Journal of the Communications Society*, vol. 6, pp. 1042–1069, 2025, doi: <https://doi.org/10.1109/ojcoms.2025.3528220>.
- [29] C.-X. Wang *et al.*, "On the Road to 6G: Visions, Requirements, Key Technologies and Testbeds" *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1–1, 2023, doi: <https://doi.org/10.1109/comst.2023.3249835>.
- [30] D. R. Bolla *et al*, "5G-Enabled Disaster Management: Enhancing Emergency Response and Recovery," pp. 1–5, Apr. 2025, doi: <https://doi.org/10.1109/amathe65477.2025.11080754>.
- [31] E. Di Fina *et al*, "Emerging Technologies for Crisis: Challenges for Applying 5G to Public Protection and Disaster Relief Scenarios" *2024 IEEE Future Networks World Forum*, pp. 141–146, Oct. 2024, doi: <https://doi.org/10.1109/fnwf63303.2024.11028785>.
- [32] V. Sharma, "5G-Enabled Mission-Critical Networks Design and Performance Analysis" *International Journal on Science and Technology*, vol. 14, no. 4, Oct. 2023, doi: <https://doi.org/10.71097/ijst.v14.i4.7998>.

- [33] M. T. Raza *et al*, “Highly Available Service Access Through Proactive Events Execution in LTE NFV” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2531–2544, Sep. 2021, doi: <https://doi.org/10.1109/tnsm.2021.3103160>.
- [34] K. Nguyen *et al*, “Empowering 5G Mobile Devices With Network Softwarization” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2492–2501, Sep. 2021, doi: <https://doi.org/10.1109/tnsm.2021.3094871>.
- [35] B. Tola *et al*, “Model-Driven Availability Assessment of the NFV-MANO with Software Rejuvenation,” *IEEE Transactions on Network and Service Management*, pp. 1–1, 2021, doi: <https://doi.org/10.1109/tnsm.2021.3090208>.
- [36] Y. Wu *et al*, “Reliability-Aware VNF Placement Using a Probability-Based Approach,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2478–2491, Sep. 2021, doi: <https://doi.org/10.1109/tnsm.2021.3093199>.
- [37] M. Mahbub *et al*, “A holistic survey of UAV-assisted wireless communications in the transition from 5G to 6G: State-of-the-art intertwined innovations, challenges, and opportunities” *Journal of Network and Computer Applications*, vol. 237, p. 104131, Jan. 2025, doi: <https://doi.org/10.1016/j.jnca.2025.104131>.
- [38] P. P. Ray, “A review on 6G for space-air-ground integrated network: Key enablers, open challenges, and future direction” *Journal of King Saud University - Computer and Information Sciences*, Aug. 2021, doi: <https://doi.org/10.1016/j.jksuci.2021.08.014>.
- [39] S. Sharif *et al*, “Space-aerial-ground-sea integrated networks: Resource optimization and challenges in 6G,” *Journal of Network and Computer Applications*, vol. 215, pp. 103647–103647, Jun. 2023, doi: <https://doi.org/10.1016/j.jnca.2023.103647>.
- [40] P. He *et al*, “Non-terrestrial Network Technologies: Applications and Future Prospects,” *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6275–6299, Mar. 2025, doi: <https://doi.org/10.1109/jiot.2024.3522912>.
- [41] Y. Lin *et al*, “Satellite-MEC Integration for 6G Internet of Things: Minimal Structures, Advances, and Prospects,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 3886–3903, 2024, doi: <https://doi.org/10.1109/ojcoms.2024.3418860>.
- [42] E. A. Vijai *et al*, “Trust-aware energy-efficient and secure routing in MANETs using explicit feature interaction graph neural networks,” *Knowledge-Based Systems*, vol. 331, p. 114572, Jan. 2026, doi: <https://doi.org/10.1016/j.knosys.2025.114572>.

- [43] R. Castelhana *et al*, “Service-Aware Multipath for Heterogeneous Networks with Non-Terrestrial Technologies” *NOMS 2025-2025 IEEE Network Operations and Management Symposium*, pp. 1–7, May 2025, doi: <https://doi.org/10.1109/noms57970.2025.11073681>.
- [44] M. Matraccia, *et al*, “Unleashing the Potential of Aerial RISs in Post-Disaster Scenarios,” *IEEE Internet of Things Magazine*, vol. 7, no. 6, pp. 88–93, Nov. 2024, doi: <https://doi.org/10.1109/iotm.001.2300258>.
- [45] E. Demircioglu, “Field Deployment and Performance Evaluation of an NR-V2X C-ITS Test Corridor Over a 5G SA Private Network,” *Electronics*, vol. 15, no. 12, p. 2668, Jun. 2026, doi: <https://doi.org/10.3390/electronics15122668>.
- [46] W. Elleuch, *et al*, “Evaluation of 5G Relay-Empowered and Device-to-Device Communications for Rescue Mission” *IEEE Access*, vol. 13, pp. 104614–104629, 2025, doi: <https://doi.org/10.1109/access.2025.3579872>.
- [47] L. Khaloopour *et al*, “Resilience-by-Design in 6G Networks: Literature Review and Novel Enabling Concepts” *IEEE Access*, pp. 1–1, Jan. 2024, doi: <https://doi.org/10.1109/access.2024.3480275>.
- [48] Z. Xiao *et al*, “Resilience Enhancement and Evaluation Methods for Space-Air-Ground Integrated Network” *Space: Science & Technology*, Jan. 2025, doi: <https://doi.org/10.34133/space.0182>.
- [49] Z. Kaleem *et al*, “UAV-Empowered Disaster-Resilient Edge Architecture for Delay-Sensitive Communication” *IEEE Network*, vol. 33, no. 6, pp. 124–132, Nov. 2019, doi: <https://doi.org/10.1109/mnet.2019.1800431>.
- [50] J. Wu *et al*, “Joint Power and Coverage Control of Massive UAVs in Post-Disaster Emergency Networks: An Aggregative Game-Theoretic Learning Approach,” *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 4, pp. 3782–3799, Apr. 2024, doi: <https://doi.org/10.1109/tNSE.2024.3385797>.
- [51] H. Dahmani and M. Al-Hubaishi, “Intelligent Detection System for SMF-AMF Stream Multiplexing Attacks in 5G-Enabled Smart Cities” *2025 5th International Conference on Pervasive Computing and Social Networking*, pp. 330–337, May 2025, doi: <https://doi.org/10.1109/icpcsn65854.2025.11035191>.
- [52] A. Jahid *et al*, “The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap” *Journal of Network and Computer Applications*, vol. 217, p. 103677, Aug. 2023, doi: <https://doi.org/10.1016/j.jnca.2023.103677>.

- [53] S. Zeb *et al* “Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey” *Journal of Network and Computer Applications*, vol. 200, p. 103309, Apr. 2022, doi: <https://doi.org/10.1016/j.jnca.2021.103309>.
- [54] V. Charpentier *et al*, “From 5G to 6G: Empowering vertical industries with next-gen technologies and trial facilities” *Computer Communications*, vol. 241, p. 108218, Sep. 2025, doi: <https://doi.org/10.1016/j.comcom.2025.108218>.
- [55] H. Raghukumar *et al.*, “Smart Communities, Smart Responders -Artificial Intelligence for Internet of Things Competition: A Case Study in Organizing a Public Safety Innovation Challenge” *2024 IEEE World Forum on Public Safety Technology*, pp. 114–119, May 2024, doi: <https://doi.org/10.1109/wfpst58552.2024.00039>.
- [56] F. Franchi *et al*, “A Cloud-Edge Architecture to Support Post-Earthquake Reconstruction in Central Italy,” *IEEE Access*, vol. 12, pp. 91823–91831, 2024, doi: <https://doi.org/10.1109/access.2024.3420695>.
- [57] Y. Drif *et al*, “Towards 6G-UAV Disaster-Resilient Networks,” *2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–6, Sep. 2024, doi: <https://doi.org/10.1109/pimrc59610.2024.10817298>.
- [58] W. Feng *et al*, “Structured Satellite-UAV-Terrestrial Networks for 6G Internet of Things,” *IEEE Network*, pp. 1–1, Jan. 2024, doi: <https://doi.org/10.1109/mnet.2024.3380052>.
- [59] S. Yu *et al*, “EC-SAGINs: Edge-Computing-Enhanced Space–Air–Ground-Integrated Networks for Internet of Vehicles,” *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5742–5754, Apr. 2022, doi: <https://doi.org/10.1109/jiot.2021.3052542>.
- [60] R. Giuliano and E. Innocenti, “Machine Learning Techniques for Non-Terrestrial Networks” *Electronics*, vol. 12, no. 3, pp. 652–652, Jan. 2023, doi: <https://doi.org/10.3390/electronics12030652>.
- [61] T. Chaymae *et al*, “Machine Learning and 5G Edge Computing for Intelligent Traffic Management” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, 2025, doi: <https://doi.org/10.14569/ijacsa.2025.0160644>.
- [62] M. Raesi-Varzaneh *et al*, “Resource Scheduling in Edge Computing: Architecture, Taxonomy, Open Issues and Future Research Directions” *IEEE Access*, vol. 11, pp. 25329–25350, 2023, doi: <https://doi.org/10.1109/ACCESS.2023.3256522>.
- [63] S. Chandra *et al*, “Intelligent resource management in 5G/6G network by adopting edge intelligence for higher education systems” *e-Prime - Advances in Electrical Engineering Electronics*

and *Energy*, vol. 8, pp. 100517–100517, Mar. 2024, doi: <https://doi.org/10.1016/j.prime.2024.100517>.

[64] S. Hashima *et al*, “Next-Gen UAV-Satellite Communications: AI Innovations and Future Prospects,” *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 1990–2021, 2025, doi: <https://doi.org/10.1109/ojvt.2025.3587028>.

[65] F. Z. Rabahi and A. A. Saadi, “IoT-Enhanced Hybrid 5G-UAV Networks for Post-Catastrophe Assessment,” *2024 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, pp. 1–6, Nov. 2024, doi: <https://doi.org/10.1109/gcaiot63427.2024.10833581>.

[66] A. Ahmed *et al*, “Integrated Terrestrial-Wired and LEO Satellite With Offline Bidirectional Cooperation for 6G IoT Networks,” *IEEE internet of things journal*, pp. 1–1, Jan. 2024, doi: <https://doi.org/10.1109/jiot.2023.3349144>.

[67] Z. Milicevic and Z. Bojkovic, “Contemporary Network Slicing Security” *WSEAS TRANSACTIONS ON COMMUNICATIONS*, vol. 24, pp. 7–10, Apr. 2025, doi: <https://doi.org/10.37394/23204.2025.24.2>.

[68] I. Darman *et al*, “Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications” *IEEE Access*, vol. 10, pp. 92774–92787, 2022, doi: <https://doi.org/10.1109/access.2022.3198642>.

[69] Dr. G. Nanthakumar *et al*, “Improved User Authenticated Key Management Scheme for 6G based Industrial Applications” *International Journal of Advanced Research in Science, Communication and Technology*, pp. 110–121, May 2023, doi: <https://doi.org/10.48175/ijarsct-9667>.

[70] Sudeep Tanwar *et al*, “Blockchain-assisted industrial automation beyond 5G networks,” vol. 169, pp. 108209–108209, Jul. 2022, doi: <https://doi.org/10.1016/j.cie.2022.108209>.

[71] M. Peng *et al*, “Learning-Based IoT Data Aggregation for Disaster Scenarios,” *IEEE Access*, vol. 8, pp. 128490–128497, 2020, doi: <https://doi.org/10.1109/access.2020.3008289>.

[72] T. Alam, “Cloud-Based IoT Applications and Their Roles in Smart Cities,” *Smart Cities*, vol. 4, no. 3, pp. 1196–1219, Sep. 2021, doi: <https://doi.org/10.3390/smartcities4030064>.

[73] E. Grigoriou *et al*, “Towards the RESPOND-A initiative: Next-generation equipment tools and mission-critical strategies for First Responders,” pp. 1–5, Aug. 2022, doi: <https://doi.org/10.1109/coins54846.2022.9854967>.

[74] J. Bai *et al*, “Satellite-ground Network Handover Method Based on QoS Mapping Mechanism in Emergency Communication Network,” *2022 IEEE 5th Advanced Information Management*,

Communicates, Electronic and Automation Control Conference (IMCEC), pp. 481–485, Dec. 2022, doi: <https://doi.org/10.1109/imcec55388.2022.10020028>.

[75] F. Parzysz *et al*, “Use cases for 6G NTN combining sustainability and performance,” *Non-Terrestrial Networks*, pp. 165–178, 2026, doi: <https://doi.org/10.1016/b978-0-443-26526-6.00014-1>.

[76] Shambhavi Prasanna *et al*, “A Survey on Routing Protocols for Disaster Management,” *SN Computer Science/SN computer science*, vol. 5, no. 2, Jan. 2024, doi: <https://doi.org/10.1007/s42979-023-02509-2>.

[77] N. N. Sirhan and M. Martinez-Ramon, “QoS-based Packet Scheduling Algorithms for Heterogeneous LTE-Advanced Networks: Concepts and a Literature Survey,” *International Journal of Wireless & Mobile Networks*, vol. 14, no. 4, pp. 1–18, Aug. 2022, doi: <https://doi.org/10.5121/ijwmn.2022.14401>.

[78] M. Kumar *et al*, “Investigating Action Recognition Approaches for Accident Detection in Smart City Transport Systems,” *2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE)*, pp. 265–269, Jul. 2025, doi: <https://doi.org/10.1109/mrie66930.2025.11156524>.

[79] Y. Ye *et al.*, “QoI-Aware Mobile Crowdsensing for Metaverse by Multi-Agent Deep Reinforcement Learning,” *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 3, pp. 783–798, Mar. 2024, doi: <https://doi.org/10.1109/jsac.2023.3345395>.

[80] L. Tello-Oquendo *et al*, “Enabling LEO Satellite Vertical Handover for Massive 6G IoT Random Access,” *ICC 2024 - IEEE International Conference on Communications*, pp. 4293–4298, Jun. 2024, doi: <https://doi.org/10.1109/icc51166.2024.10623063>.

[81] M. K. Shehzad *et al*, “RNN-Based Twin Channel Predictors for CSI Acquisition in UAV-Assisted 5G+ Networks,” *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Dec. 2021, doi: <https://doi.org/10.1109/globecom46510.2021.9685990>.

[82] M. Ashraf *et al*, “Low Complexity Algorithms for Mission Completion Time Minimization in UAV-Based Emergency Response,” *IEEE Transactions on Intelligent Vehicles*, pp. 1–16, 2024, doi: <https://doi.org/10.1109/tiv.2024.3405475>.

[83] M. Xu *et al*, “Trustworthy Precipitation Prediction via Communication-Efficient Lightweight Trend Perception Network,” *IEEE Internet of Things Journal*, pp. 1–1, 2025, doi: <https://doi.org/10.1109/jiot.2025.3581429>.

- [84] A. Agrawal and A. K. Pal, “Adaptive Hybrid Genetic-Ant Colony Optimization for Dynamic Self-Healing and Network Performance Optimization in 5G/6G Networks,” *Procedia Computer Science*, vol. 252, pp. 404–413, Feb. 2025, doi: <https://doi.org/10.1016/j.procs.2024.12.041>.
- [85] H.-S. Jang and J. Yeo, “Current status analysis of 5G mobile communication services industry using business model canvas in South Korea,” *Asia Pacific Management Review*, Nov. 2024, doi: <https://doi.org/10.1016/j.apmr.2024.11.002>.
- [86] Azita Laily Yusof *et al*, “Handover management for UAV communication in 5G networks: A systematic literature review,” *Engineering Science and Technology an International Journal*, vol. 71, pp. 102198–102198, Sep. 2025, doi: <https://doi.org/10.1016/j.jestch.2025.102198>.
- [87] C. C. Lessi *et al*, “5G and Beyond 5G Technologies Enabling Industry 5.0: Network Applications for Robotics,” *Procedia Computer Science*, vol. 232, pp. 675–687, Jan. 2024, doi: <https://doi.org/10.1016/j.procs.2024.01.067>.
- [88] P. R. Chelliah and K. Sheng, “6G communication for next-generation metaverse systems” *Advances in Computers*, pp. 473–505, 2025, doi: <https://doi.org/10.1016/bs.adcom.2025.03.012>.
- [89] A. Yuan *et al*, “Evolution of Satellite Communication Systems Toward 5G/6G for 2030 and Beyond,” *Engineering*, Jun. 2025, doi: <https://doi.org/10.1016/j.eng.2025.06.025>.
- [90] A. Elshrkasi *et al*, “Enhancement of cellular networks via an improved clustering technique with D2D communication for mission-critical applications”, *Journal of Network and Computer Applications*, vol. 206, p. 103482, Oct. 2022, doi: <https://doi.org/10.1016/j.jnca.2022.103482>.
- [91] H. Purohit and S. Bhattacharyya, “MBSE for Contingency Planning for Cellular Networks with OPM,” *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 690–697, Oct. 2024, doi: <https://doi.org/10.1109/uemcon62879.2024.10754722>.
- [92] S. Loss *et al*, “A Framework for Live Situational Awareness in Stream-Based 5G Applications,” *2025 IEEE Latin Conference on IoT (LCIoT)*, pp. 202–205, Apr. 2025, doi: <https://doi.org/10.1109/lciot64881.2025.11118567>.
- [93] M. Yağcıoğlu, “Machine learning based dynamic resource sharing and frequency reuse in 5G hetnets with droncells,” *Computer Networks*, vol. 258, p. 111046, Feb. 2025, doi: <https://doi.org/10.1016/j.comnet.2025.111046>.
- [94] Tapio Savunen *et al*, “Mobile network operators’ business risks in next-generation public safety services,” *Telecommunications Policy*, vol. 48, no. 4, pp. 102733–102733, May 2024, doi: <https://doi.org/10.1016/j.telpol.2024.102733>.

- [95] Sarantis Kalafatidis *et al*, “SwarmCatcher: An AI-Powered Anti-Drone Surveillance System for Public Safety Over 5G and Beyond Ecosystems,” pp. 173–180, Mar. 2025, doi: <https://doi.org/10.1109/icin64016.2025.10943055>.
- [96] G. Zhang *et al.*, “UGV-awareness task placement in edge-cloud based urban intelligent video systems,” *Cluster Computing*, vol. 27, no. 5, pp. 6563–6577, Mar. 2024, doi: <https://doi.org/10.1007/s10586-024-04305-w>.
- [97] A. S. Mahomed and A. K. Saha, “Unleashing the Potential of 5G for Smart Cities: A Focus on Real-Time Digital Twin Integration,” *Smart Cities*, vol. 8, no. 2, pp. 70–70, Apr. 2025, doi: <https://doi.org/10.3390/smartcities8020070>.
- [98] J. Wallace *et al*, “A High-Performance 5G/6G Framework for Smart Cities Supporting Multi-Level Artificial Intelligence” *2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)*, pp. 1–9, Feb. 2025, doi: <https://doi.org/10.1109/icaisc64594.2025.10959390>.
- [99] W. Khan *et al.*, “Enhancing security in 6G-enabled wireless sensor networks for smart cities: a multi-deep learning intrusion detection approach,” *Frontiers in Sustainable Cities*, vol. 7, May 2025, doi: <https://doi.org/10.3389/frsc.2025.1580006>.
- [100] S.-H. Lee *et al*, “Research on the Design and Implementation of a Mesh Network Communication System for Fire and Hazardous Gas Detection and Response,” *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 247–249, Jul. 2024, doi: <https://doi.org/10.1109/icufn61752.2024.10625080>.
- [101] I. Farhat *et al*, “A Multi-Area Architecture for Real-Time Feedback-Based Optimization of Distribution Grids,” *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 1448–1461, Mar. 2025, doi: <https://doi.org/10.1109/tsg.2024.3524622>.
- [102] J. Liao *et al*, “Research on Intelligent Operation Support Technology for 5G Nuclear-Powered Ships,” *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)*, pp. 500–504, Oct. 2021, doi: <https://doi.org/10.1109/aiam54119.2021.00105>.
- [103] M. Elwekeil *et al*, “Power Control in Cell-Free Massive MIMO Networks for UAVs URLLC Under the Finite Blocklength Regime,” *IEEE Transactions on Communications*, vol. 71, no. 2, pp. 1126–1140, Feb. 2023, doi: <https://doi.org/10.1109/tcomm.2022.3227230>.
- [104] B. C. Tedeschini *et al*, “Message Passing Neural Network Versus Message Passing Algorithm for Cooperative Positioning,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 6, pp. 1666–1676, Dec. 2023, doi: <https://doi.org/10.1109/tccn.2023.3307953>.

- [105] M. He *et al*, “BWSAR: A Single-Drone Search-and-Rescue Methodology Leveraging 5G-NR Beam Sweeping Technologies for Victim Localization,” *Electronics*, vol. 13, no. 21, p. 4317, Nov. 2024, doi: <https://doi.org/10.3390/electronics13214317>.
- [106] D. Kim, “Trace Angle and QoS-Aware Hybrid Handover Algorithm for LEO Satellite Networks,” *Journal of Korea Multimedia Society*, vol. 28, no. 9, pp. 1331–1338, Sep. 2025, doi: <https://doi.org/10.9717/kmms.2025.28.9.1331>.
- [107] Amir Mohammadisarab *et al*, “Resilient Disaster Relief in Industrial IoT: UAV Trajectory Design and Resource Allocation in 6G Non-Terrestrial Networks,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1827–1845, Jan. 2024, doi: <https://doi.org/10.1109/ojcoms.2024.3376335>.
- [108] W. G. Negassa *et al*, “Design and performance of UAV-employed hybrid FSO/RF systems for weather-resilient 6G and beyond networks,” *Physical Communication*, vol. 75, p. 103040, Mar. 2026, doi: <https://doi.org/10.1016/j.phycom.2026.103040>.
- [109] S. Chakraborty *et al.*, “Creating a shared public safety radio data,” *2024 IEEE World Forum on Public Safety Technology (WFPST)*, pp. 188–191, May 2024, doi: <https://doi.org/10.1109/wfpst58552.2024.00018>.
- [110] C. Tata and M. Kadoch, “Network Coding-Based D2D Transmission for Public Safety Networks over LTE HetNets and 5G Networks,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–15, Mar. 2022, doi: <https://doi.org/10.1155/2022/8889718>.
- [111] M. Li and H.-L. Tsai, “Energy-Efficient Device Discovery Mechanism for Device-to-Device Communications in 5G Networks,” *Energies*, vol. 14, no. 2, p. 270, Jan. 2021, doi: <https://doi.org/10.3390/en14020270>.
- [112] S. Rekik and S. Mehmood, “A Hybrid Graph Neural Network and Neural ODE Model to Intrusion Detection in Dynamic Network Topologies,” *IEEE Access*, pp. 1–1, 2025, doi: <https://doi.org/10.1109/access.2025.3635385>.
- [113] M. Mahbub and R. M. Shubair, “Coverage enhancement of UAV-enabled 6G networks via intelligent reflecting surfaces: towards optimal SINR,” *Telecommunication Systems*, vol. 83, no. 2, pp. 147–157, May 2023, doi: <https://doi.org/10.1007/s11235-023-00999-2>.
- [114] J. Alotaibi *et al*, “Optimizing disaster response with UAV-mounted RIS and HAP-enabled edge computing in 6G networks,” *Journal of Network and Computer Applications*, vol. 241, p. 104213, May 2025, doi: <https://doi.org/10.1016/j.jnca.2025.104213>.

- [115] B. D. Deebak *et al*, “Lightweight Blockchain Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems,” *IEEE Internet of Things Journal*, pp. 1–1, 2022, doi: <https://doi.org/10.1109/JIOT.2022.3152546>.
- [116] A. Rehman and O. Alharbi, “QESIF: A Lightweight Quantum-Enhanced IoT Security Framework for Smart Cities,” *Smart Cities*, vol. 8, no. 4, pp. 116–116, Jul. 2025, doi: <https://doi.org/10.3390/smartcities8040116>.
- [117] W. Lu *et al*, “Variational Mode Decomposition-Based Method for Separation of Measured Responses of Structures,” *SSRN Electronic Journal*, 2022, doi: <https://doi.org/10.2139/ssrn.4049644>.
- [118] S. Garg *et al*, “Guest Editorial: Blockchain Envisioned Drones: Realizing 5G-Enabled Flying Automation,” *IEEE Network*, vol. 35, no. 1, pp. 16–19, Jan. 2021, doi: <https://doi.org/10.1109/mnet.2021.9355047>.
- [119] R. Sakai *et al*, “Impact of Emission Noise and Electromagnetic Shielding on Mobile Communication Systems in Unmanned Aerial Vehicles,” Sep. 2023, doi: <https://doi.org/10.1109/emceurope57790.2023.10274281>.
- [120] E. Mittag *et al.*, “Introducing a 6G-Enabled Multi-Connectivity Robotic Teleoperation Platform,” *2025 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1851–1857, Jun. 2025, doi: <https://doi.org/10.1109/iccworkshops67674.2025.11162322>.
- [121] C. K. Toh and D. Milojevic, “Recent Advances in Smart Cities” *IEEE Consumer Electronics Magazine*, vol. 10, no. 6, pp. 67–68, Nov. 2021, doi: <https://doi.org/10.1109/mce.2021.3095705>.
- [122] Y. Wang *et al*, “Mobile crowdsourcing based on 5G and 6G: A survey” *Neurocomputing*, vol. 618, p. 128993, Feb. 2025, doi: <https://doi.org/10.1016/j.neucom.2024.128993>.
- [123] P. Purushotham *et al*, “Disaster Analysis Using Machine Learning” Nov. 2022, doi: <https://doi.org/10.1109/assic55218.2022.10088390>.
- [124] I. Nasim *et al*, “5G Communications in Nuclear: Potential Use Cases and Security Considerations” *IEEE Access*, vol. 13, pp. 37611–37623, 2025, doi: <https://doi.org/10.1109/access.2025.3544962>.
- [125] Y. Chen *et al*, “Analysis of Electromagnetic Risk in Nuclear Power Plant” pp. 1–5, Oct. 2023, doi: <https://doi.org/10.1109/isemc58300.2023.10370516>.
- [126] Jong Wan Seo *et al*, “Deep learning based Nuclear Power Plant Monitoring System using UAV” *2021 International Conference on Electronics, Information, and Communication (ICEIC)*, Jan. 2021, doi: <https://doi.org/10.1109/iceic51217.2021.9369789>.

- [127] J. Meng and L. B. Yang, "Research on 5G Communication System Transmission Scheme Through Penetrations in Reactor Buildings of In-service Nuclear Power Plants," *2024 8th International Conference on Communication and Information Systems (ICCIS)*, pp. 126–133, Oct. 2024, doi: <https://doi.org/10.1109/iccis63642.2024.10779436>.
- [128] Q. Duan *et al*, "Research on Key Technologies of 5G Radio Access Network(RAN) for Nuclear Power Plant Industry Applications" *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pp. 195–199, Jan. 2023, doi: <https://doi.org/10.1109/iccece58074.2023.10135392>.
- [129] Q. Duan *et al*, "Research on the Virtual Private Network Security of 5G Smart Nuclear Power Plants" *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pp. 186–190, Jan. 2023, doi: <https://doi.org/10.1109/iccece58074.2023.10135311>.
- [130] I. M. Braga *et al*, "Sum-Rate Maximization in Beyond 5G Systems with Limited NTN Backhaul," pp. 1–6, Nov. 2023, doi: <https://doi.org/10.1109/wcnps60622.2023.10344717>.
- [131] A. Gupta and S. K. Gupta, "UAV Aided Fog Network (UAFN): A Proposal Framework for Better QoS," *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, pp. 265–270, Jan. 2022, doi: <https://doi.org/10.1109/iccit52419.2022.9711624>.
- [132] D. Amendola *et al*, "Special Issue on 5G/6G Precise Positioning on Cooperative Intelligent Transportation Systems (C-ITS) and Connected Automated Vehicles (CAV)—Part I," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 12, pp. 3713–3718, Dec. 2023, doi: <https://doi.org/10.1109/jsac.2023.3322051>.
- [133] D. Amendola *et al*, "Special Issue on 5G/6G Precise Positioning on Cooperative Intelligent Transportation Systems (C-ITS) and Connected Automated Vehicles (CAV)—Part II," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 1, pp. 1–5, Jan. 2024, doi: <https://doi.org/10.1109/jsac.2023.3322070>.
- [134] L. Barbieri *et al*, "Deep Learning-Based Cooperative LiDAR Sensing for Improved Vehicle Positioning," *IEEE Transactions on Signal Processing*, vol. 72, pp. 1666–1682, 2024, doi: <https://doi.org/10.1109/tsp.2024.3377375>.
- [135] P. Zhang *et al*, "Secure Communication of Integrated Air-Space-Ground-Maritime Networks: Technologies, Application and Challenges," *IEEE Internet of Things Magazine*, vol. 8, no. 4, pp. 124–131, Jul. 2025, doi: <https://doi.org/10.1109/iotm.001.2500015>.
- [136] B. Poke and S. Uludag, "Empirical Evaluation of a LoRa Mesh Network for Emergency Communication Systems," *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile*

Communication Conference (UEMCON), pp. 0637–0646, Oct. 2023, doi: <https://doi.org/10.1109/uemcon59035.2023.10316084>.

[137] A. C. Coch *et al*, “Communication Technologies in Emergency Situations,” *Electronics*, vol. 11, no. 7, p. 1155, Jan. 2022, doi: <https://doi.org/10.3390/electronics11071155>.

[138] D. Cicek and B. Kantarci, “Use of Mobile Crowdsensing in Disaster Management: A Systematic Review, Challenges, and Open Issues,” *Sensors*, Vol 23, Iss 1699, p 1699 (2023), p. 1, 2023, doi: <https://doi.org/10.3390/s23031699>.

[139] P. Priya, “Comparative Analysis Of 5g-Enabled Iot Architecture: Performance, Scalability, And Real-World Applicability,” *Journal of Emerging Technologies and Innovative Research*, vol. 12, no. 7, 2025, doi: <https://doi.org/10.56975/jetir.v12i7.565874>.

[140] M. A. Al-Absi *et al*, “Moving Ad Hoc Networks—A Comparative Study,” *Sustainability*, vol. 13, no. 11, p. 6187, May 2021, doi: <https://doi.org/10.3390/su13116187>.

[141] K. Sharma *et al*, “A Disaster Management Framework Using Internet of Things-Based Interconnected Devices,” *Mathematical Problems in Engineering*, vol. 2021, pp. 1–21, May 2021, doi: <https://doi.org/10.1155/2021/9916440>.

[142] R. Agrawal *et al*, “Classification and comparison of ad hoc networks: A review,” *Egyptian Informatics Journal*, vol. 24, no. 1, pp. 1–25, Mar. 2023, doi: <https://doi.org/10.1016/j.eij.2022.10.004>.

[143] J. Li *et al*, “A survey of maritime unmanned search system: Theory, applications and future directions,” *Ocean Engineering*, vol. 285, pp. 115359–115359, Oct. 2023, doi: <https://doi.org/10.1016/j.oceaneng.2023.115359>.

[144] S. M. Khan *et al*, “A Systematic Review of Disaster Management Systems: Approaches, Challenges, and Future Directions,” *Land*, vol. 12, no. 8, p. 1514, Aug. 2023, doi: <https://doi.org/10.3390/land12081514>.

[145] S. K. Abid *et al*, “Toward an Integrated Disaster Management Approach: How Artificial Intelligence Can Boost Disaster Management,” *Sustainability*, vol. 13, no. 22, p. 12560, Nov. 2021, doi: <https://doi.org/10.3390/su132212560>.

[146] M. Elkhodr *et al*, “A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness,” *Future Internet*, vol. 16, no. 1, p. 22, Jan. 2024, doi: <https://doi.org/10.3390/fi16010022>.

[147] N. K. Kaur *et al*, “Emerging applications and ongoing challenges in WSN assisted IoT networks,” *World Journal of Advanced Engineering Technology and Sciences*, vol. 11, no. 2, pp. 501–507, Apr. 2024, doi: <https://doi.org/10.30574/wjaets.2024.11.2.0143>.

- [148] Z. Nurlan *et al*, “Wireless Sensor Network as a Mesh: Vision and Challenges,” *IEEE Access*, vol. 10, pp. 46–67, 2022, doi: <https://doi.org/10.1109/access.2021.3137341>.
- [149] Y. Wang *et al*, “Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions,” *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2021, doi: <https://doi.org/10.1109/comst.2021.3131711>.
- [150] V. R. Kebande and Ali Ismail Awad, “Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions,” *ACM Computing Surveys*, vol. 56, no. 5, Dec. 2023, doi: <https://doi.org/10.1145/3635030>.
- [151] V. Chamola *et al*, “Disaster and Pandemic Management Using Machine Learning: A Survey,” *IEEE Internet of Things Journal*, pp. 1–1, 2020, doi: <https://doi.org/10.1109/jiot.2020.3044966>.
- [152] Ghaihab Hassan Adday *et al*, “Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey,” *IEEE access*, pp. 1–1, Jan. 2024, doi: <https://doi.org/10.1109/access.2024.3362889>.
- [153] S. Alraih *et al.*, “Revolution or Evolution? Technical Requirements and Considerations towards 6G Mobile Communications,” *Sensors*, vol. 22, no. 3, p. 762, Jan. 2022, doi: <https://doi.org/10.3390/s22030762>.
- [154] M. F. Ali *et al*, “Recent Trends in Underwater Visible Light Communication (UVLC) Systems,” *IEEE Access*, vol. 10, pp. 22169–22225, 2022, doi: <https://doi.org/10.1109/ACCESS.2022.3150093>.
- [155] Z. Kaleem *et al*, “Intelligent Unmanned Air Vehicles for Public Safety Networks: Emerging Technologies and Research Directions,” *Unmanned System Technologies*, pp. 1–17, 2022, doi: https://doi.org/10.1007/978-981-19-1292-4_1.
- [156] X. Tao *et al.*, “The Monitoring and Early Warning System of Geological Disaster Mass Survey and Prevention in Linzhi,” *2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, Apr. 2021, doi: <https://doi.org/10.1109/ipec51340.2021.9421179>.
- [157] W. Jiang, “Software defined satellite networks: A survey,” *Digital Communications and Networks*, Jan. 2023, doi: <https://doi.org/10.1016/j.dcan.2023.01.016>.
- [158] M. R. Patruni *et al*, “Intelligent IoT-Blockchain Ecosystem: A security perspective, applications, and challenges,” *Computer Science Review*, vol. 59, p. 100843, Oct. 2025, doi: <https://doi.org/10.1016/j.cosrev.2025.100843>.

Appendix A: “Primary Research Papers Included in the Study”

Paper\Criteria	Disaster management phase (crisis lifecycle)					Key research challenges						Evaluation method					Network Layer / OSI Perspective				
	Preparedness (training, simulation, early-warning communication)	Response (real-time coordination, mission-critical communication)	Recovery (infrastructure restoration, long-term resilience communication)	Mitigation (proactive risk reduction using predictive communication)		Reliability & resilience (fault tolerance, redundancy)	Latency & QoS (real-time response)	Security & privacy	Interoperability & standards (cross-agency, cross-technology)	Energy efficiency & sustainability		Theoretical / simulation-based studies	Testbed experiments (lab prototypes, emulators)	Field trials and pilot deployments	Cross-disciplinary frameworks (technical + policy/ethics?)		Physical Layer (resilient spectrum use, satellite links, energy-efficient)	Data Link / Network Layer (routing protocols for MANETs/VANETs,	Transport Layer (congestion control, latency-sensitive designs in	Application Layer (alert systems, citizen apps, sensor dashboards)	Cross-Layer / Holistic Approaches (AI-native resilience, QoS + security
[31] E. Di Fina <i>et al</i> , “Emerging Technologies for Crisis: Challenges for Applying 5G to Public Protection and Disaster Relief Scenarios” 2024	strong	strong	moderate	moderate		very strong	very strong	moderate	very strong	moderate		very strong	weak	weak	moderate		moderate	moderate	moderate	moderate	very strong

[7] R. Sakai, <i>et al</i> , “Impact of Emission Noise and Electromagnetic Shielding on Mobile Communication Systems in Unmanned Aerial Vehicles” 2023	moderate	strong	moderate	strong		strong	strong	strong	moderate	moderate		very strong	weak	weak	moderate		moderate	strong	moderate	moderate	very strong
[8] E. Mittag <i>et al</i> , “Introducing a 6G-Enabled Multi-Connectivity Robotic Teleoperation Platform” 2025	moderate	very strong	strong	very strong		strong	strong	very strong	moderate	moderate		very strong	weak	weak	moderate		moderate	strong	moderate	strong	very strong
[68] I. Darman <i>et al</i> , “Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications” 2022	strong	moderate	moderate	very strong		strong	strong	moderate	moderate	moderate		very strong	strong	weak	moderate		very strong	moderate	weak	weak	moderate
[71] M. Peng <i>et al</i> , “Learning-Based IoT Data Aggregation for Disaster Scenarios” 2020	strong	very strong	moderate	strong		strong	strong	moderate	moderate	moderate		moderate	very strong	weak	moderate		strong	very strong	strong	moderate	very strong

[15] P Purushotham <i>et al</i> , “Disaster Analysis Using Machine Learning” 2022	strong	strong	moderate	very strong		strong	moderate	strong	strong	moderate		strong	moderate	moderate	very strong		moderate	strong	moderate	very strong	very strong
[69] B. Poke and S. Uludag “Empirical Evaluation of a LoRa Mesh Network for Emergency Communication Systems” 2023	strong	very strong	moderate	strong		strong	strong	moderate	moderate	moderate		strong	moderate	moderate	weak		strong	very strong	strong	moderate	very strong
[23] M. Matraccia <i>et al</i> , “On the Topological Aspects of UAV-Assisted Post-Disaster Wireless Communication Networks” 2021	strong	very strong	moderate	very strong		moderate	moderate	strong	moderate	moderate		strong	weak	weak	moderate		moderate	very strong	strong	strong	very strong
[18] P.K. Thiruvassagam <i>et al</i> , “Resilient and Latency-Aware Orchestration of Network Slices Using Multi-Connectivity in MEC-Enabled 5G Networks” 2021	strong	very strong	moderate	very strong		strong	strong	strong	moderate	weak		strong	strong	weak	moderate		moderate	very strong	strong	strong	very strong

[74] J. Bai <i>et al</i> , “Satellite-ground Network Handover Method Based on QoS Mapping Mechanism in Emergency Communication Network” 2022	strong	very strong	very strong	Str ong		strong	strong	moderate	moderate	strong		strong	weak	weak	moderate		moderate	very strong	strong	strong	very strong
[73] E. Grigoriou <i>et al</i> , “Towards the RESPOND-A initiative: Next-generation equipment tools and mission-critical strategies for First Responders,” 2022	strong	moderate	moderate	strong		strong	moderate	moderate	strong	moderate		strong	weak	weak	moderate		moderate	moderate	weak	very strong	very strong
[49] Z. Kaleem <i>et al</i> , “UAV-Empowered Disaster-Resilient Edge Architecture for Delay-Sensitive Communication” 2019	very strong	very strong	moderate	moderate		moderate	moderate	moderate	weak	strong		weak	strong	moderate	weak		strong	very strong	moderate	moderate	weak
[24] I. Nasim <i>et al</i> , “5G Communications in Nuclear: Potential Use Cases and Security Considerations” 2025	very strong	very strong	very strong	strong		strong	strong	strong	strong	strong		weak	very strong	moderate	strong		strong	very strong	moderate	strong	very strong

[25] Y. Chen <i>et al</i> , “Analysis of Electromagnetic Risk in Nuclear Power Plant” 2023	strong	very strong	strong	moderate		very strong	very strong	strong	very strong	moderate		weak	very strong	moderate	strong		moderate	very strong	strong	strong	very strong
[26] Jong Wan Seo, <i>et al</i> , “Deep learning based Nuclear Power Plant Monitoring System using UAV,” 2021	moderate	very strong	very strong	moderate		very strong	moderate	weak	moderate	weak		very strong	weak	weak	moderate		very strong	strong	moderate	weak	moderate
[27] J. Meng and L. B. Yang, “Research on 5G Communication System Transmission Scheme Through Penetrations in Reactor Buildings of In-service Nuclear Power Plants,” 2024	strong	very strong	very strong	moderate		very strong	very strong	moderate	moderate	weak		very strong	weak	weak	moderate		very strong	very strong	strong	moderate	weak
[29] Q. Duan, <i>et al</i> , “Research on Key Technologies of 5G Radio Access Network for Nuclear Power Plant Industry Applications” 2023	moderate	very strong	strong	moderate		very strong	strong	moderate	weak	weak		very strong	weak	weak	moderate		very strong	strong	moderate	moderate	moderate

[30] Q. Duan <i>et al</i> , “Research on the Virtual Private Network Security of 5G Smart Nuclear Power Plants,” 2023	very strong	very strong	strong	strong		very strong	very strong	moderate	very strong	moderate		weak	moderate	very strong	very strong		strong	very strong	moderate	strong	very strong
[65] F. Z. Rabahi and A. A. Saadi, “IoT-Enhanced Hybrid 5G-UAV Networks for Post-Catastrophe Assessment” 2024	moderate	weak	strong	very strong		strong	very strong	very strong	strong	moderate		very strong	weak	weak	moderate		strong	moderate	moderate	strong	very strong
[35] I. M. Braga, <i>et al</i> , “Sum-Rate Maximization in Beyond 5G Systems with Limited NTN Backhaul” 2023	strong	weak	moderate	very strong		moderate	moderate	moderate	very strong	weak		very strong	weak	weak	strong		very strong	weak	weak	moderate	moderate
[36] A. Gupta and S. K. Gupta, “UAV Aided Fog Network (UAFN): A Proposal Framework for Better QoS” 2022	strong	moderate	moderate	very strong		moderate	strong	weak	moderate	weak		moderate	very strong	weak	weak		moderate	moderate	moderate	very strong	strong

[28] S. K. Jagatheesaperumal, <i>et al</i> , “Blockchain-Based Security Architecture for Uncrewed Aerial Systems in B5G/6G Services and Beyond: A Comprehensive Approach” 2025	strong	weak	strong	very strong		strong	moderate	moderate	moderate	weak		very strong	weak	weak	moderate		very strong	weak	moderate	weak	moderate
[50] J. Wu <i>et al</i> , “Joint Power and Coverage Control of Massive UAVs in Post-Disaster Emergency Networks: An Aggregative Game-Theoretic Learning Approach” 2024	moderate	strong	strong	moderate		strong	very strong	strong	very strong	moderate		moderate	strong	moderate	strong		strong	strong	moderate	moderate	very strong
[64] S. Hashima, <i>et al</i> , “Next-Gen UAV-Satellite Communications: AI Innovations and Future Prospects,” 2025	strong	very strong	strong	very strong		strong	very strong	strong	strong	moderate		strong	weak	weak	strong		moderate	strong	moderate	very strong	very strong

[59] S. Yu, <i>et al</i> , “EC-SAGINs: Edge-Computing-Enhanced Space–Air–Ground-Integrated Networks for Internet of Vehicles,” 2022	moderate	strong	strong	strong		very strong	very strong	strong	very strong	weak		strong	weak	weak	moderate		strong	very strong	strong	moderate	strong
[78] M. Kumar, <i>et al</i> , “Investigating Action Recognition Approaches for Accident Detection in Smart City Transport Systems,” 2025	moderate	strong	strong	very strong		strong	moderate	very strong	very strong	weak		strong	weak	weak	very strong		moderate	moderate	strong	moderate	very strong
[79] Y. Ye et al., “QoI-Aware Mobile Crowdsensing for Metaverse by Multi-Agent Deep Reinforcement Learning,” 2024	strong	very strong	strong	moderate		strong	very strong	moderate	strong	moderate		strong	weak	weak	very strong		moderate	moderate	strong	very strong	very strong

[79] H. Raghukumar <i>et al</i> , “Smart Communities, Smart Responders - Artificial Intelligence for Internet of Things Competition: A Case Study in Organizing a Public Safety Innovation Challenge” 2024	moderate	very strong	strong	moderate		strong	very strong	weak	moderate	strong		very strong	weak	weak	moderate		strong	very strong	strong	moderate	strong
[55] H. Raghukumar <i>et al</i> , “Smart Communities, Smart Responders - Artificial Intelligence for Internet of Things Competition: A Case Study in Organizing a Public Safety Innovation Challenge” 2024	moderate	weak	weak	strong		weak	weak	very strong	weak	weak		very strong	weak	weak	very strong		weak	weak	weak	moderate	strong
[80] I L. Tello-Oquendo <i>et al</i> , “Enabling LEO Satellite Vertical Handover for Massive 6G IoT Random Access” 2024	moderate	moderate	strong	moderate		moderate	moderate	weak	strong	strong		very strong	weak	weak	moderate		very strong	strong	moderate	weak	strong

[81] M. K. Shehzad, <i>et al</i> , “RNN-Based Twin Channel Predictors for CSI Acquisition in UAV-Assisted 5G+ Networks” 2021	moderate	strong	moderate	moderate		moderate	very strong	moderate	moderate	moderate		moderate	weak	weak	moderate		moderate	strong	strong	moderate	very strong
[47] Ladan Khaloopour <i>et al.</i> , “Resilience-by-Design in 6G Networks: Literature Review and Novel Enabling Concepts” 2024	strong	moderate	weak	strong		strong	moderate	very strong	strong	strong		moderate	weak	weak	very strong		strong	very strong	strong	strong	very strong
[40] P. He <i>et al.</i> , “Non terrestrial Network Technologies: Applications and Future Prospects” 2025	very strong	moderate	strong	strong		very strong	strong	moderate	strong	moderate		moderate	weak	weak	strong		moderate	strong	strong	moderate	very strong
[82] M. Ashraf, <i>et al</i> , “Low Complexity Algorithms for Mission Completion Time Minimization in UAV-Based Emergency Response” 2024	moderate	very strong	strong	moderate		strong	very strong	weak	moderate	very strong		very strong	weak	weak	moderate		strong	moderate	weak	moderate	strong

[83] M. Xu, <i>et al</i> , “Trustworthy Precipitation Prediction via Communication- Efficient Lightweight Trend Perception Network” 2025	very strong	moderate	weak	strong		strong	very strong	strong	very strong	moderate		very strong	weak	weak	moderate		very strong	strong	moderate	strong	very strong
[84] A. Agrawal and A. K. Pal, “Adaptive Hybrid Genetic-Ant Colony Optimization for Dynamic Self- Healing and Network Performance Optimization in 5G/6G Networks” 2025	strong	strong	moderate	moderate		strong	very strong	moderate	very strong	strong		very strong	weak	weak	moderate		strong	strong	moderate	strong	very strong
[70] Sudeep <i>et al</i> , “Blockchain-assisted industrial automation beyond 5G networks” 2022	very strong	moderate	weak	moderate		strong	strong	moderate	very strong	weak		moderate	weak	weak	strong		very strong	strong	moderate	strong	very strong

[24] S. P. Dash, <i>et al</i> “Introduction to integrated sensing and communications for the next generation of wireless connectivity” 2025	strong	very strong	moderate	strong		moderate	very strong	moderate	moderate	weak		moderate	weak	weak	moderate		weak	weak	moderate	very strong	strong
[85] H.-S. Jang and J. Yeo, “Current status analysis of 5G mobile communication services industry using business model canvas in South Korea” 2024	strong	very strong	moderate	strong		strong	very strong	weak	moderate	strong		very strong	weak	weak	moderate		strong	moderate	strong	moderate	very strong
[2] M. Kordi and M. Ertz, “Deciphering technological advancements for efficient disaster management and community resilience” 2026	very strong	moderate	moderate	strong		moderate	moderate	strong	very strong	strong		weak	weak	weak	strong		weak	moderate	moderate	very strong	strong

[86] Azita Laily Yusof, <i>et al</i> “Handover management for UAV communication in 5G networks: A systematic literature review,” 2025	very strong	moderate	weak	strong		very strong	strong	very strong	very strong	strong		very strong	weak	weak	moderate		very strong	moderate	moderate	moderate	very strong
[42] E. A. Vijai <i>et al</i> , “Trust-aware energy-efficient and secure routing in MANETs using explicit feature interaction graph neural networks” 2026	very strong	very strong	moderate	strong		strong	very strong	moderate	very strong	moderate		weak	strong	strong	very strong		weak	moderate	moderate	very strong	strong
[87] C. C. Lessi, <i>et al</i> , “5G and Beyond 5G Technologies Enabling Industry 5.0: Network Applications for Robotics”2024	very strong	moderate	weak	strong		very strong	strong	weak	very strong	strong		very strong	weak	weak	moderate		strong	strong	moderate	moderate	strong
[75] F. Parzysz, <i>et al</i> , “Use cases for 6G NTN: combining sustainability and performance” 2026	very strong	moderate	weak	strong		strong	moderate	weak	strong	very strong		very strong	weak	weak	moderate		strong	weak	moderate	weak	moderate

[25] P. Loganathan, <i>et al</i> , “Towards 6G technologies: Insight into architecture, communication, AI applications and use cases” 2025	very strong	strong	moderate	very strong		strong	strong	very strong	moderate	moderate		moderate	weak	weak	strong		strong	moderate	weak	moderate	strong
[88] P. R. Chelliah and K. Sheng, “6G communication for next-generation metaverse systems” 2025	very strong	moderate	strong	very strong		very strong	moderate	very strong	strong	moderate		moderate	weak	weak	very strong		strong	strong	moderate	moderate	very strong
[89] A. Yuan, <i>et al</i> , “Evolution of Satellite Communication Systems Toward 5G/6G for 2030 and Beyond” 2025	very strong	strong	strong	strong		very strong	strong	moderate	very strong	strong		moderate	weak	weak	strong		very strong	strong	moderate	strong	very strong
[54] V. Charpentier, <i>et al</i> , “From 5G to 6G: Empowering vertical industries with next-gen technologies and trial facilities” 2025	moderate	very strong	weak	moderate		strong	very strong	weak	moderate	moderate		very strong	weak	weak	weak		strong	moderate	weak	moderate	moderate

[63] S. Chandra, <i>et al</i> , “Intelligent resource management in 5G/6G network by adopting edge intelligence for higher education systems” 2024	strong	very strong	moderate	strong		very strong	very strong	very strong	strong	moderate		weak	weak	weak	strong		strong	moderate	moderate	strong	very strong
[21] D. K. R. and S. Chavhan, “Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts” 2022	very strong	moderate	weak	strong		strong	strong	weak	moderate	strong		very strong	weak	weak	moderate		weak	weak	moderate	strong	moderate
[52] A. Jahid, <i>et al</i> , “The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap” 2023	strong	moderate	weak	very strong		weak	moderate	moderate	moderate	weak		strong	weak	weak	weak		weak	weak	weak	strong	moderate
[26] H. Shin <i>et al.</i> , “The future service scenarios of 6G telecommunications technology”, 2024	moderate	very strong	weak	weak		moderate	strong	moderate	strong	very strong		weak	strong	strong	moderate		strong	very strong	moderate	moderate	moderate

[90] A. Elshrkasi, <i>et al</i> , “Enhancement of cellular networks via an improved clustering technique with D2D communication for mission-critical applications”, 2025	strong	moderate	strong	very strong		very strong	strong	very strong	very strong	very strong		weak	strong	moderate	very strong		strong	moderate	strong	very strong	very strong
[91] H. Purohit and S. Bhattacharyya, “MBSE for Contingency Planning for Cellular Networks with OPM,” 2024	moderate	very strong	weak	weak		strong	very strong	weak	strong	moderate		strong	weak	weak	moderate		moderate	strong	strong	moderate	moderate
[92] S. Loss <i>et al</i> “A Framework for Live Situational Awareness in Stream-Based 5G Applications”, 2025	strong	very strong	moderate	moderate		very strong	very strong	moderate	strong	strong		very strong	weak	weak	moderate		strong	strong	very strong	strong	very strong
[46] W. Elleuch <i>et al</i> , “Evaluation of 5G Relay-Empowered and Device-to-Device Communications for Rescue Mission” 2025	strong	very strong	very strong	moderate		very strong	strong	moderate	very strong	moderate		weak	very strong	very strong	strong		strong	very strong	strong	moderate	very strong

[7] S. Majumdar <i>et al</i> , “First Responder Communication Systems: A Technical Analysis of Interoperability and Situational Awareness Optimization”, 2022	strong	very strong	moderate	weak		very strong	strong	strong	very strong	moderate		weak	weak	weak	very strong		very strong	moderate	strong	very strong	very strong
[51] H. Dahmani and M. Al-Hubaishi, “Intelligent Detection System for SMF-AMF Stream Multiplexing Attacks in 5G-Enabled Smart Cities ” 2025	moderate	very strong	moderate	strong		very strong	very strong	weak	moderate	strong		very strong	weak	weak	moderate		weak	very strong	weak	weak	strong
[93] M. Yağcıoğlu, “Machine learning based dynamic resource sharing and frequency reuse in 5G hetnets with dronecells”, 2025	moderate	strong	moderate	very strong		strong	very strong	very strong	moderate	moderate		strong	weak	weak	moderate		moderate	weak	weak	strong	moderate
[17] F. Rastoceanu, <i>et al</i> , “Mission-Critical Services in 4G/5G and Beyond: Standardization, Key Challenges, and Future Perspectives” 2025	strong	moderate	weak	strong		moderate	very strong	moderate	very strong	strong		very strong	weak	weak	moderate		strong	weak	weak	weak	very strong

[94] T. Savunen <i>et al</i> , “Mobile network operators’ business risks in next-generation public safety services”, 2024	very strong	moderate	weak	strong		moderate	very strong	moderate	strong	moderate		weak	weak	moderate	strong		moderate	weak	weak	strong	moderate
[43] R. Castelhana <i>et al</i> , “Service-Aware Multipath for Heterogeneous Networks with Non-Terrestrial Technologies”, 2025	very strong	very strong	strong	very strong		very strong	strong	strong	very strong	very strong		strong	weak	moderate	very strong		weak	weak	weak	strong	moderate
[95] S. Kalafatidis <i>et al</i> , “SwarmCatcher: An AI-Powered Anti-Drone Surveillance System for Public Safety Over 5G and Beyond Ecosystems” 2025	moderate	very strong	moderate	strong		very strong	very strong	moderate	very strong	moderate		strong	weak	weak	moderate		strong	very strong	moderate	weak	moderate
[96] G. Zhang <i>et al</i> , “UGV-awareness task placement in edge-cloud based urban intelligent video systems” 2020	very strong	strong	moderate	very strong		very strong	very strong	strong	very strong	strong		strong	weak	moderate	very strong		moderate	moderate	moderate	moderate	very strong

[97] A. S. Mahomed and A. K. Saha, “Unleashing the Potential of 5G for Smart Cities: A Focus on Real-Time Digital Twin Integration”, 2025	moderate	very strong	moderate	strong		very strong	strong	very strong	moderate	very strong		very strong	weak	weak	moderate		weak	very strong	weak	weak	strong
[98] J. Wallace <i>et al</i> , “A High-Performance 5G/6G Framework for Smart Cities Supporting Multi-Level Artificial Intelligence,” 2025	very strong	very strong	moderate	strong		strong	very strong	strong	very strong	moderate		moderate	strong	moderate	very strong		weak	moderate	weak	strong	very strong
[99] W. Khan <i>et al</i> , “Enhancing security in 6G-enabled wireless sensor networks for smart cities: a multi-deep learning intrusion detection approach” 2025	strong	very strong	strong	moderate		very strong	very strong	strong	very strong	very strong		moderate	weak	weak	very strong		strong	strong	weak	moderate	strong

[27] S. Zyoud and A. H. Zyoud, "Advancing sustainable cities and communities with internet of things: Global insights, trends, and research priorities for SDG 11" 2025	strong	strong	moderate	very strong		very strong	very strong	strong	strong	strong		moderate	weak	weak	strong		moderate	moderate	weak	moderate	very strong
[60] R. Giuliano and E. Innocenti, "Machine Learning Techniques for Non-Terrestrial Networks", 2023	strong	strong	moderate	very strong		very strong	very strong	very strong	strong	strong		moderate	weak	weak	very strong		strong	weak	weak	moderate	moderate
[19] J. Bravo-Arrabal <i>et al</i> , "The Internet of Cooperative Agents Architecture (X-IoCA) for Robots, Hybrid Sensor Networks, and MEC Centers in Complex Environments: A Search and Rescue Case Study" 2021	moderate	strong	strong	strong		very strong	very strong	moderate	strong	strong		moderate	weak	weak	very strong		very strong	very strong	weak	weak	strong

[56] F. Franchi <i>et al</i> , “A Cloud-Edge Architecture to Support Post-Earthquake Reconstruction in Central Italy ” 2024	strong	very strong	strong	very strong		strong	very strong	moderate	very strong	strong		moderate	strong	strong	very strong		moderate	strong	moderate	very strong	very strong
[100] S.-H. Lee <i>et al</i> , “Research on the Design and Implementation of a Mesh Network Communication System for Fire and Hazardous Gas Detection and Response” 2024	moderate	strong	moderate	very strong		moderate	very strong	weak	moderate	very strong		very strong	weak	weak	moderate		moderate	strong	weak	weak	strong
[69] Dr. G. Nanthakumar, <i>et al</i> , “Improved User Authenticated Key Management Scheme for 6G based Industrial Applications,” 2023	strong	very strong	moderate	very strong		very strong	very strong	strong	strong	very strong		strong	weak	weak	very strong		moderate	moderate	weak	weak	strong

[101] I. Farhat <i>et al</i> , “A Multi-Area Architecture for Real-Time Feedback-Based Optimization of Distribution Grids”, 2025	moderate	strong	moderate	very strong		strong	moderate	very strong	strong	moderate		strong	weak	weak	very strong		moderate	moderate	weak	moderate	strong
[10] Salwa Saafi <i>et al</i> , “Enabling Next-Generation Public Safety Operations with Mission-Critical Networks and Wearable Applications” 2021	strong	very strong	strong	very strong		moderate	very strong	moderate	strong	moderate		moderate	weak	weak	very strong		weak	moderate	weak	moderate	weak
[102] J. Liao <i>et al</i> , “Research on Intelligent Operation Support Technology for 5G Nuclear-Powered Ships,” 2021	very strong	very strong	strong	very strong		very strong	very strong	strong	very strong	very strong		strong	weak	weak	very strong		strong	strong	weak	moderate	very strong
[35] B. Tola <i>et al</i> “Model-Driven Availability Assessment of the NFV-MANO with Software Rejuvenation”, 2021	weak	very strong	strong	moderate		very strong	very strong	weak	moderate	very strong		very strong	weak	weak	moderate		weak	moderate	weak	weak	weak

[36] Y. Wu, <i>et al</i> , “Reliability-Aware VNF Placement Using a Probability-Based Approach”, 2021	very strong	very strong	strong	strong		very strong	very strong	strong	very strong	moderate		moderate	weak	moderate	very strong		weak	weak	weak	moderate	moderate
[34] K. Nguyen <i>et al</i> , and H. Sekiya, “Empowering 5G Mobile Devices With Network Softwarization,” 2021	moderate	strong	moderate	weak		moderate	moderate	weak	moderate	strong		moderate	strong	very strong	moderate		moderate	moderate	weak	weak	weak
[33] M. T. Raza <i>et al</i> , “Highly Available Service Access Through Proactive Events Execution in LTE NFV,” 2021	very strong	moderate	weak	strong		moderate	moderate	weak	moderate	weak		strong	weak	weak	moderate		weak	weak	weak	moderate	weak
[103] M. Elwekeil <i>et al</i> , “Power Control in Cell-Free Massive MIMO Networks for UAVs URLLC Under the Finite Block length Regime”, 2023	strong	very strong	strong	moderate		very strong	moderate	moderate	very strong	moderate		strong	weak	weak	strong		weak	moderate	weak	weak	moderate

[48] Z. Xiao <i>et al</i> , “Resilience Enhancement and Evaluation Methods for Space-Air-Ground Integrated Network” 2025	strong	very strong	strong	moderate		very strong	very strong	moderate	strong	moderate		very strong	weak	weak	moderate		moderate	very strong	weak	moderate	very strong
[58] W. Feng <i>et al</i> , “Structured Satellite-UAV-Terrestrial Networks for 6G Internet of Things”, 2024	weak	very strong	strong	moderate		strong	very strong	weak	strong	moderate		strong	weak	weak	moderate		moderate	strong	weak	moderate	strong
[66] A. Ahmed <i>et al</i> , “Integrated Terrestrial-Wired and LEO Satellite With Offline Bidirectional Cooperation for 6G IoT Networks”2024	moderate	very strong	strong	moderate		very strong	very strong	moderate	very strong	strong		strong	weak	weak	strong		moderate	moderate	weak	strong	very strong
[104] B. C. Tedeschini <i>et al</i> , “Message Passing Neural Network Versus Message Passing Algorithm for Cooperative Positioning” 2023	weak	very strong	moderate	weak		very strong	moderate	weak	moderate	moderate		very strong	weak	weak	moderate		strong	strong	weak	weak	moderate

[105] M. He, <i>et al</i> , “BWSAR: A Single-Drone Search-and-Rescue Methodology Leveraging 5G-NR Beam Sweeping Technologies for Victim Localization” 2024	strong	very strong	strong	moderate		very strong	very strong	strong	strong	strong		moderate	weak	weak	very strong		moderate	moderate	weak	moderate	moderate
[45] E. Demircioglu, “Field Deployment and Performance Evaluation of an NR-V2X C-ITS Test Corridor Over a 5G SA Private Network” 2026	weak	very strong	moderate	weak		strong	very strong	moderate	strong	moderate		weak	strong	moderate	strong		weak	moderate	weak	very strong	strong
[57] Y. Drif <i>et al</i> , “Towards 6G-UAV Disaster-Resilient Networks,” 2024	weak	very strong	moderate	weak		strong	very strong	moderate	strong	moderate		strong	weak	weak	moderate		strong	very strong	moderate	strong	very strong
[61] T. Chaymae <i>et al</i> , “Machine Learning and 5G Edge Computing for Intelligent Traffic Management” 2025	strong	very strong	moderate	moderate		strong	strong	very strong	very strong	moderate		moderate	weak	moderate	very strong		weak	moderate	weak	moderate	moderate

[32] V. Sharma, “5G-Enabled Mission-Critical Networks Design and Performance Analysis”, 2023	moderate	strong	moderate	strong		strong	strong	very strong	moderate	moderate		strong	moderate	weak	moderate		weak	weak	strong	strong	moderate
[106] D. Kim, “Trace Angle and QoS-Aware Hybrid Handover Algorithm for LEO Satellite Networks”, 2025	moderate	strong	strong	moderate		strong	strong	very strong	moderate	moderate		very strong	weak	weak	moderate		strong	moderate	weak	weak	moderate
[107] A. Mohammadisarab <i>et al</i> , “Resilient Disaster Relief in Industrial IoT: UAV Trajectory Design and Resource Allocation in 6G Non-Terrestrial Networks” 2024	moderate	strong	weak	strong		moderate	very strong	moderate	strong	very strong		strong	moderate	weak	moderate		weak	weak	weak	moderate	moderate
[108] W. G. Negassa <i>et al</i> , “Design and performance of UAV-employed hybrid FSO/RF systems for weather-resilient 6G and beyond networks” 2026	strong	very strong	strong	moderate		very strong	very strong	very strong	very strong	moderate		moderate	moderate	strong	very strong		moderate	moderate	moderate	very strong	strong

[12] K. Saini <i>et al</i> “Disaster emergency response framework for smart buildings” 2022	strong	moderate	strong	moderate		very strong	strong	very strong	strong	moderate		weak	weak	moderate	very strong		moderate	moderate	weak	moderate	very strong
[44] M. Matraccia <i>et al</i> “Unleashing the Potential of Aerial RISs in Post-Disaster Scenarios”, 2024	moderate	very strong	weak	weak		strong	very strong	weak	moderate	weak		very strong	weak	weak	weak		strong	weak	weak	moderate	moderate
[109] S. Chakraborty <i>et al</i> , “Creating a shared public safety radio data” 2024	moderate	strong	moderate	moderate		strong	very strong	weak	very strong	weak		moderate	very strong	weak	weak		moderate	very strong	moderate	weak	very strong
[110] C. Tata and M. Kadoch, “Network Coding-Based D2D Transmission for Public Safety Networks over LTE HetNets and 5G Networks”, 2022	strong	very strong	moderate	strong		strong	very strong	strong	very strong	moderate		moderate	strong	very strong	moderate		moderate	weak	moderate	very strong	strong
[111] M. Li and H.-L. Tsai, “Energy-Efficient Device Discovery Mechanism for Device-to-Device Communications in 5G Networks” 2021	strong	strong	moderate	moderate		moderate	very strong	weak	strong	moderate		very strong	weak	weak	moderate		weak	moderate	weak	strong	strong

[111] B. Kożuch and K. Sienkiewicz-Małyjurek, “Building collaborative trust in public safety networks” 2022	strong	very strong	moderate	strong		strong	very strong	moderate	strong	strong		strong	weak	weak	strong		moderate	moderate	weak	moderate	moderate
[112] S. Rekik and S. Mehmood, “A Hybrid Graph Neural Network and Neural ODE Model to Intrusion Detection in Dynamic Network Topologies” 2025	strong	very strong	moderate	strong		very strong	very strong	strong	very strong	strong		moderate	weak	weak	strong		moderate	very strong	weak	weak	weak
[113] M. Mahbub and R. M. Shubair, “Coverage enhancement of UAV-enabled 6G networks via intelligent reflecting surfaces: towards optimal SINR” 2025	moderate	very strong	weak	strong		strong	moderate	very strong	moderate	moderate		strong	moderate	weak	moderate		moderate	very strong	weak	moderate	weak
[114] J. Alotaibi <i>et al</i> , “Optimizing disaster response with UAV-mounted RIS and HAP-enabled edge computing in 6G networks” 2025	moderate	very strong	weak	strong		moderate	moderate	very strong	strong	weak		very strong	strong	weak	moderate		strong	moderate	weak	moderate	strong

[115] B. D. Deebak <i>et al</i> , “Lightweight Blockchain Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems” 2022	moderate	very strong	moderate	strong		very strong	very strong	moderate	strong	moderate		very strong	weak	weak	moderate		moderate	moderate	moderate	weak	very strong
[102] J. Liao <i>et al</i> , “Research on Intelligent Operation Support Technology for 5G Nuclear-Powered Ships” 2021	moderate	very strong	moderate	weak		very strong	strong	weak	strong	moderate		very strong	weak	weak	moderate		strong	weak	weak	strong	moderate
[116] A. Rehman and O. Alharbi, “QESIF: A Lightweight Quantum-Enhanced IoT Security Framework for Smart Cities” 2025	very strong	moderate	weak	moderate		moderate	moderate	strong	strong	very strong		weak	weak	weak	very strong		weak	weak	weak	moderate	moderate
[72] T. Alam, “Cloud-Based IoT Applications and Their Roles in Smart Cities” 2021	strong	moderate	weak	very strong		strong	strong	very strong	strong	strong		weak	weak	weak	strong		weak	weak	weak	strong	strong

[62] M. Raeisi-Varzaneh <i>et al</i> “Resource Scheduling in Edge Computing: Architecture, Taxonomy, Open Issues and Future Research Directions” 2023	very strong	strong	moderate	very strong		strong	very strong	moderate	very strong	moderate		moderate	weak	weak	moderate		very strong	very strong	strong	moderate	strong
[117] W. Lu <i>et al</i> , “Variational Mode Decomposition-Based Method for Separation of Measured Responses of Structures” 2022	strong	very strong	moderate	strong		very strong	very strong	moderate	very strong	moderate		weak	strong	very strong	moderate		strong	strong	weak	very strong	moderate

Author's Statement:

I hereby expressly declare that, according to the article 8 of Law 1559/1986, this dissertation is solely the product of my personal work, does not infringe any intellectual property, personality and personal data rights of third parties, does not contain works/contributions from third parties for which the permission of the authors/beneficiaries is required, is not the product of partial or total plagiarism and that the sources used are limited to across the related literature references alone and meet the rules of scientific citations.