6GSNS

Smart Networks and Services Joint Undertaking (SNS JU)

Technology Board (TB)

White Paper

Smart Networks and Services Innovation to Support Public Protection and Disaster Relief (PPDR)

DOI: 10.5281/zenodo.18613557
URL: https://doi.org/10.5281/zenodo.18613557

June 2026

EXECUTIVE SUMMARY

Europe's capacity to protect its citizens and support its first responders depends on communication infrastructures that are resilient, interoperable, and intelligent across every condition a crisis can produce. The transition to 6G is not simply a performance upgrade, it is an opportunity to build preparedness, resilience, and cross-border interoperability into the foundational architecture of European safety communications from the outset.

This white paper maps the work of the Smart Networks and Services Joint Undertaking (SNS JU) research portfolio against the operational realities, values, and policy ambitions of Europe's Public Protection and Disaster Relief (PPDR) community, identifies where that work is already well-aligned, and sets out where future research should focus to maximise its societal impact.

By 2040, a European first responder should be able to arrive at any incident, anywhere in Europe, and connect immediately via their normal tools to a shared operational picture that includes every other agency and asset involved in the response. The network should anticipate threats before they escalate, continue to function when infrastructure is destroyed, and support recovery, learning, and preparation once the incident is over. Preparedness is now explicitly a whole-of-society responsibility: 6G must also support the communities, schools, hospitals, and individual citizens who are expected to be self-sufficient for 72 hours when central infrastructure fails. Reaching this vision means treating 6G not as a faster network but as a genuine foundation for European societal resilience.

The policy and values frame is demanding. The EU Critical Communication System (EUCCS), due to connect all European law enforcement and safety responders through an interoperable broadband platform by 2030, sets the most immediate benchmark. Alongside it, the Preparedness Union Strategy, the Niinistö Report, the Digital Networks Act, NIS2, the Cyber Resilience Act, and the EU AI Act together define a regulatory environment in which resilience, security, interoperability, and accountability are legal requirements to be built into 6G architecture from the start. PPDR practitioners reinforce these demands with their own value-based goals: systems that work across every environment and agency boundary, that reduce cognitive load rather than adding to it, that earn and sustain the trust of the agencies and communities they serve, and that leave no person or place behind.

The SNS portfolio is strongly aligned with these priorities. Projects address the scenarios practitioners and policymakers consistently identify as highest-stakes: natural disasters, large public events, maritime environments, critical infrastructure, and healthcare emergencies. Multi-layered space-air-ground connectivity, edge computing, AI-driven network management, zero-trust security frameworks, integrated sensing and communication, and energy-autonomous operation are all represented. Four technology

domains stand out as particularly consequential. Hybrid terrestrial and non-terrestrial network architectures are building the connectivity redundancy that ensures responders can communicate when fixed infrastructure is destroyed. Edge and cloud-native infrastructure is pushing real-time intelligence to the point of need. AI and machine learning are enabling closed-loop network self-optimisation, reducing operator burden at the moment when cognitive load is highest. Integrated sensing and communication is transforming the network from a passive data pipeline into a native sensing environment capable of tracking personnel and monitoring conditions where conventional sensors cannot function.

The portfolio also has clear areas for development. The most consistent challenge is the gap between what performs well in a testbed and what can be trusted in the field: closing it requires operational stress-testing to become a design standard, shared operationally representative datasets, and evaluation frameworks that include operational metrics alongside network KPIs. Interoperability remains the most urgent priority, not just technical protocol compatibility, but the capacity for responders from different agencies and nations, arriving with different systems and no shared preparation, to achieve a common operational picture in real time. The portfolio is strongest in the response phase; future work should engage more deliberately with prevention, recovery, post-incident learning, and community-level resilience. The governance and accountability dimensions of AI-driven systems, and the supply chain trustworthiness of critical components, deserve more systematic attention as design considerations from the outset. Digital literacy and public trust are conditions that determine whether technically capable systems produce the outcomes they are designed for and should be treated as research design inputs rather than downstream considerations.

Translating the portfolio's technical foundations into societal impact requires deliberate, coordinated action across the research community, policymakers, practitioners, standardisation bodies, and industry. Making research evidence available in forms that policy and standardisation audiences can use and engaging actively with the processes that will determine whether research outputs are ever deployed at scale, is one of the most consequential contributions the programme can make. The goal is not technically impressive demonstrations but operationally validated, governance-ready, and universally accessible capabilities that European PPDR agencies, and the communities they serve, can actually depend on.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

3GPP	3rd Generation Partnership Project
5G	5th Generation
6G	6th Generation
6G IA	6G Infrastructure Association
AI	Artificial Intelligence
APN	Access Point Name
AR	Augmented Reality
ATSSS	Access Traffic Steering, Switching and Splitting
B5G	Beyond 5G
BLE	Bluetooth Low Energy
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CER	Critical Entities Resilience (Directive)
CI/CD	Continuous Integration/Continuous Deployment
CNF	Cloud-native Network Function
CRA	Cyber Resilience Act
CSA	EU Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CU	Central Unit
DDoS	Distributed Denial of Service
DNA	Digital Networks Act
DU	Distributed Unit
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU-CyCLONe	EU Cyber Crisis Liaison Organisation Network
EUCC	European Common Criteria
EUCCS	EU Critical Communication System
FR1	Frequency Range 1
FR3	Frequency Range 3
GDPR	General Data Protection Regulation
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GPU	Graphics Processing Unit
HAPS	High-Altitude Platform Station
IAB	Integrated Access and Backhaul
IMT	International Mobile Telecommunications
IoT	Internet of Things
ISAC	Integrated Sensing and Communication
JCCSP	Joint Communication, Computation, Sensing and Power (transfer)
KPI	Key Performance Indicator
KVI	Key Value Indicator
LEO	Low Earth Orbit
LLM	Large Language Model

LoTAF	Level of Trust Assessment Function
MCPTT	Mission Critical Push-to-Talk
MCVideo	Mission Critical Video
MCX	Mission Critical technology (voice, video, data)
MEC	Mobile Edge Computing
ML	Machine Learning
MPTCP	Multi-Path Transmission Control Protocol
MPQUIC	Multi-Path Quick UDP Internet Connections
NFV	Network Function Virtualization
NIS2	Network and Information Security (Directive)
NTN	Non-Terrestrial Network
O-DU	O-RAN Distributed Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
OPEX	Operating Expense
PHY	Physical Layer
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
PQC	Post-Quantum Cryptography
PSCE	Public Safety Communication Europe
QKD	Quantum Key Distribution
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RIC	RAN Intelligent Controller
RIS	Reconfigurable Intelligent Surface
RU	Radio Unit
SDR	Software Defined Radio
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprise
SNS JU	Smart Networks and Services Joint Undertaking
SSLA	Service and Security Level Agreement
SWaP	Size, Weight, and Power
TEF	Trust Evaluation Function
TN	Terrestrial Network
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communications
USV	Unmanned Surface Vehicle
VNF	Virtual Network Function
VR	Virtual Reality
VPN	Private Virtual Network
XAI	Explainable Artificial Intelligence
XR	Extended Reality
ZSM	Zero-Touch Network & Service Management

1. INTRODUCTION

Europe's capacity to protect its citizens and support its first responders depends increasingly on robust and resilient communication infrastructures. These dependencies are made more complex as public safety becomes increasingly cross-border, multi-agency, based in operational mobility, and requiring European-wide compatible systems. As communication networks transition toward 6G, research and funding priorities will help define the next generation of crisis management. This white paper aims to align the technical ambitions of the Smart Networks and Services Joint Undertaking (SNS JU) research community with the operational realities of the public safety and disaster relief (PPDR) people and agencies who will rely on these networks.

This paper describes the current SNS portfolio, highlight areas of strong alignment and identifies areas where the portfolio could develop further. The paper identifies pathways to combine the technical results with the human, organisational, and governance dimensions of PPDR that ensure deployability and operational success. This work blends literature research, previous workshop results, and an overview of current SNS JU project activities gained from a targeted survey was given to current projects with PPDR relevance. The survey gathered official inputs from project partners and coordinators, highlighting the drivers in operation, technology ambitions, and challenges at the foundation of each project.

The ambition for European PPDR communications is defined in policy as much as in operations or research. The policy roadmap has progressed since the European Council Conclusions on the Protection of Public Spaces in 2021, leading to 'Creation of the European Critical Communication System (EUCCS)' as a policy priority in the European Commission's work programme 2026.

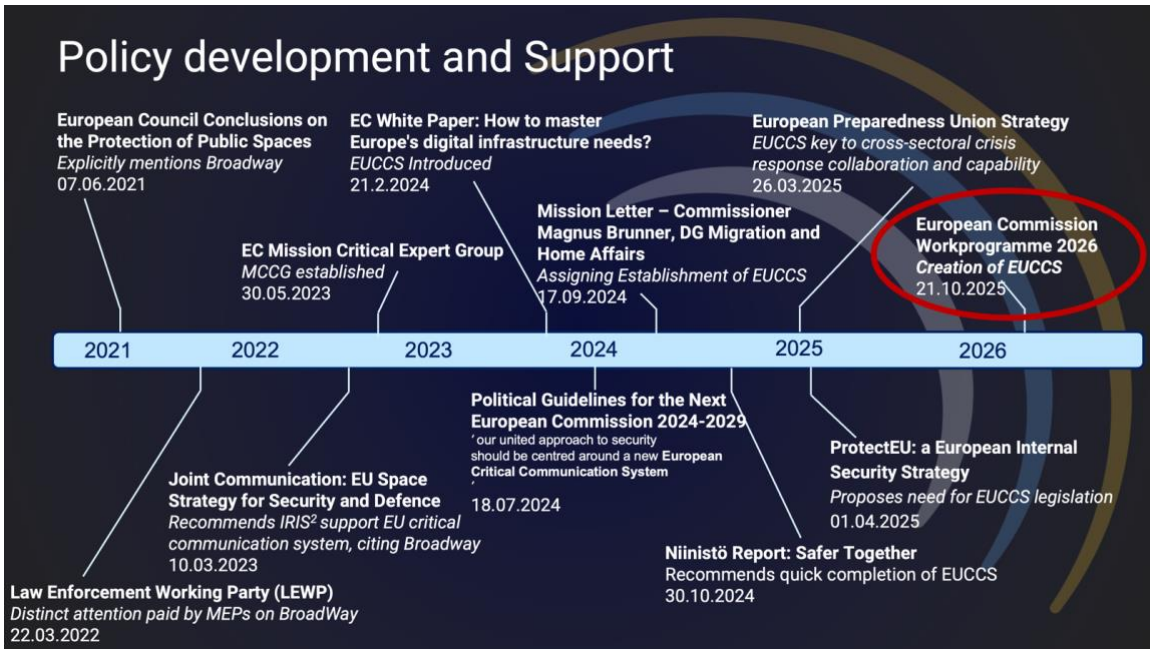


Figure 1 EU Policy Development and Support for towards EUCCS.

The upcoming EU Critical Communication System (EUCCS) aims to connect all European law enforcement and disaster responders through an interoperable broadband platform by 2030. The EUCCS Regulation will be presented from European Commission to the European Council and Parliament during 2026. It is expected that this would be agreed within 2 years, leading to the establishment of EUCCS by 2030, involving 7-8 interconnected national Mission Critical mobile broadband systems. A further group of countries will join in 2033 and the final group of countries will connect their national system in 2036.

Further policies also guide this work. The Preparedness Union Strategy treats resilience as a whole-of-society responsibility, requiring it to be built into every layer of European infrastructure from the outset. The Digital Networks Act requires a Union Preparedness Plan for stressed and damaged digital infrastructures. These frameworks are the benchmarks for success. By mapping Smart Networks and Services (SNS) research onto these mandates, this paper identifies where the current portfolio excels and where future work should focus.

Realising the full potential of 6G for emergency response demands that engineers and practitioners develop a genuinely shared understanding of each other's worlds. This paper bridges technology and policy domains with that goal in mind, drawing on a needs and values framework developed with PPDR practitioners, industry experts, and academics. By contrasting 6G innovation with the requirements, policies, and values that drive the emergency response community, it works to identify the motivations and aspirations that will shape the next decade of emergency communications.

Many of the most important requirements for that future are rooted in operational reality, where there is a need to connect scattered teams across diverse systems, maintaining command under pressure, sustaining trust when it matters most, and ensuring on one gets left behind. By linking these human missions to specific 6G challenges, this paper gives engineers a richer set of measures for success: not just technical compliance, but the inherent preparedness and operational readiness required to protect citizens.

This work also seeks to make the SNS JU community's contributions accessible to the wider range of stakeholders whose decisions will shape the future of the field. The SNS portfolio represents a significant investment in Europe's technical sovereignty, yet its impact depends on the adoption of its findings by PPDR agencies and representative organisations. By consolidating the portfolio's contributions across use cases, technologies, challenges, the paper demonstrates how the SNS community is building the evidence base and technical foundations that European safety infrastructure will need by 2040.

To achieve its goals, this white paper is organised into five chapters that transition from high-level policy and operational values to specific use cases, technological innovations and future pathways:

- **Relevant PPDR Policy and Value Frame** (Chapter 2): This chapter establishes the frame for the document by examining the strategic goals of the PPDR community and the European regulatory landscape. It defines the values, policy and PPDR operational drivers, that serve as foundational design parameters for future systems.
- **PPDR Problems and Use Cases** (Chapter 3): This section details the concrete use cases and operational gaps faced by first responders that are being addressed within

the SNS community: situational awareness, network reliability and performance, management of events and emergencies, and critical communication infrastructure

- **Investigated Technologies** (Chapter 4): This chapter explores the 6G technical solutions being developed to meet PPDR needs. It covers radio access and connectivity, edge and cloud-native infrastructure, AI/ML-driven automation, security and trust, devices and sensing, and energy efficiency.
- **Main Challenges and Envisioned Solutions** (Chapter 5): Moving from research to operational reality, this section identifies critical hurdles, such as maintaining connectivity when infrastructure fails, that projects are facing and describes the emerging solutions being pursued by SNS JU projects.
- **Added Value and Future Pathways** (Chapter 6): The final chapter articulates a 2040 vision for European public safety, outlining how 6G can enable a preparedness-by-design model.

2. RELEVANT PPDR POLICY AND VALUE FRAME

The development of 6G for European public safety depends on three inseparable factors: the strategic needs of PPDR practitioners, the regulatory and policy frameworks that define what European 6G systems must be capable of, and the values and operational priorities articulated by practitioners. The most effective 6G systems will be those where technical innovation is anchored on this foundation. This chapter provides an overview of these drivers to establish the frame from within which Smart Network Services projects can select their problems, design use cases, and choose technologies to develop or innovate. This frame should also inform the evaluation of the technology and the priorities for future research investment.

2.1. STRATEGIC GOALS AND UNDERLYING NEEDS OF THE PPDR COMMUNITY

Previous work with PPDR stakeholders has highlighted specific strategic goals and needs they envisions for the future of connectivity and what that connectivity must achieve for PPDR [1]. These include:

Operational mobility: The ability to communicate using mobile broadband wherever they are, whenever they need to communicate, and with whoever they are tasked to cooperate.

Seamless Mobility/Availability/Ubiquity: the ability to have communication working everywhere, information available from anywhere to anywhere, empowering informed decisions and coordinated actions. Communication must be seamless when cross administrative boundaries, including cross board roaming. There should be no communication outage.

Borderless Networks: the ability to use of flexible, bi- & multi-directional, interoperable communication systems to enable information exchange, informed decisions, coordinated actions and common understanding.

Rapid Deployment: the ability to rapidly deploy and coordinate multidisciplinary teams from anywhere across Europe to improve how responders save lives and help communities get back to normal faster.

Shared Situational Awareness: the ability to exchange knowledge and data regardless of jurisdiction or discipline to provide a dynamic overview of assets, directions, information.

Real-Time Continuous Monitoring: the capacity to monitor responders' health, location, equipment, overall resources, and the situation so as to ensure safety of responders and citizens, readiness of responders to be called upon, and confidence of both responders and the public in public safety policies and leadership.

Learning from Experts not at the Scene: Nothing can replace the expert hands of a search and rescue teams, paramedics, or fire services, but having the ability to share skills or assess needs onsite before an expert can arrive can greatly improve both preparations prior to arrival on scene as well as response outcomes. Local responders need to be supported by specialists who are not onsite, providing an added layer of knowledge and expertise that a phone call cannot provide or that would take too long if they had to wait for the expert to arrive.

Better use of Limited Resources: Response agencies often have limited resources but high need, where efficiency and effectiveness primarily focus on saving time and saving lives. But they also need the ability to reach more people with their services, equalising benefits via technology, responsibility and accountability structures.

Dynamic Allocation of Capacity: Dynamically allocate connectivity capacities to address the changing communication and knowledge needs of different phases of a crisis. For example, much more information might need to be gathered and shared in the first 24 hours of a wildfire (from sensors, satellites, city data, etc.) to establish the scene than after the fire is partially contained, when the public might need more capacity to contact loved ones and ask for help.

To support these strategic goals, systems need to address a series of high-level needs that describe what connectivity systems must actually accomplish.

To start, PPDR practitioners need **systems that work across diversity to ensure resilience**: of environments; or local, national, or European requirements; of standards and applications. Safety demands communication that draws together multiple modes and methods across different geographies and populations, and must function in collapsed buildings, ravines, mountains, dense urban canyons, at sea, in the air, under mobility, and when infrastructure is stressed or damaged. New systems must also build on what already exists, accommodating different networks, security levels, typologies, and onboarding processes while supporting the shift to future capability. Not all organisations or regions will adopt new systems at the same rate or of the same type, yet they must be able to work together. This means attending to governance, training, readiness, funding, and public cooperation — without which differences in semantics, culture, process, and motivation will continue to impede cooperation across the disaster management cycle. Above all, systems must be affordable and available across this diversity.

Genuine **interoperability means responders from different agencies and countries can achieve shared command and situational awareness even when they have never worked together before**, spanning sensors, satellite feeds, data streams, radio, and mapping. This must be paired with intelligent information management so that each responder receives only what is relevant to their task.

Continuous coverage is a baseline requirement, inside buildings, across dense cities and rural areas, and during blackouts, without changing the tools in responders' hands. Dynamic capacity allocation means redirecting bandwidth to specific streams at critical moments: re-routing when local infrastructure fails, scaling up for aerial data transfers when needed. These decisions, particularly where automated or AI-driven, require clear accountability

structures. Connectivity is itself a limited resource and must be prioritised accordingly, and ideally managed in ways that do not harm the environment or local economies.

Any new technology must create **simple, worry-free processes that allow responders to focus on the task rather than the system**. Standards must be flexible enough to accommodate local and cultural differences while enabling the cross-border collaboration that safety requires. The public should be treated as an active stakeholder: community willingness to communicate and cooperate with emergency services is a condition of effective response, not a given. Equally, practitioner trust must be a foundational design requirement rather than an expected outcome — secure technology alone does not create it. What is required is common purpose defined in advance, novel governance structures, and demonstrated reliability that makes agencies willing to share data across boundaries. Key Policy that are relevant to SNS and PPDR

The European Union has established a comprehensive and rapidly evolving regulatory framework that governs how 6G networks must be designed, deployed, and operated, much of it intended to support PPDR activities. Taken together, these instruments reflect a fundamental shift in European policy philosophy: from reactive crisis management toward mandating preparedness-by-design, in which resilience, security, and interoperability are requirements to be built into the foundational architecture of next-generation communications infrastructure from the outset. For 6G to fulfil its role as a strategic enabler of societal resilience, it must navigate these policies governing critical infrastructure protection, cybersecurity, equipment integrity, operational coordination, telecommunications regulation, and comprehensive preparedness.

Preparedness, Proactivity, and Strategic Autonomy

Key to PPDR and 6G is the Preparedness Union Strategy, which combines the Niinistö and Draghi reports [2] [3] [4] [5]. This is a roadmap for an All-Hazards and Whole-of-Society proactive approach to crises, security, and public safety. Under this frame, 6G infrastructure and technology must work regardless of if facing a wildfire or a state-sponsored hack. In addition, preparedness is no longer just for the military or police. It involves every school, business, and citizen.

The Niinistö report, *Safer Together*, argues that Europe is unprepared for the complexity of modern threats, seeking to create a whole-of-society model that considers preparedness for PPDR, military, as well as the general public, including schools, hospitals, and individuals. The report advocates for intelligence sharing, ideally via a single EU structure, to monitor and respond to threats. As part of this, the report asks to strengthen the EU Emergency Response Coordination Centre into a proactive, rather than reactive, hub. It pushes for a cultural shift where any citizen should be able to be self-sufficient for 72 hours in a crisis, which would need to consider the impact of communication services going down on such self-sufficiency. Overall, the report suggests increasing dual-use technologies and networks, joint public, civil and military training prior before a crisis hits, and further activities to build social trust in preparedness technology and processes.

The Draghi Report and the Competitive Compass for the EU further strengthen this [6]. They aim for strategic autonomy and technological sovereignty by reducing dependencies on foreign technology and services, increasing security, as well as increasing internal innovation and competitiveness. They seek to do so by improving skills and coordination, including spectrum harmony across all Member States (e.g. to maintain interoperable communication systems and keeping the EU running during a crisis more generally), and in doing so, improving preparedness. Tied to this is decarbonisation of innovation, technology, and society as a whole, including PPDR. The Preparedness Union Strategy takes this and ensures that sovereign hardware is backed by EU-wide emergency protocols, such as the newly established EU Crisis Hub, which integrates real-time data from 6G-enabled sensors in disaster zones. Preparedness-by-design is now a priority.

The emerging Digital Networks Act is expected to accelerate this transition by consolidating the fragmented national telecom market into a single European system, including NTN [7] [8]. The DNA requires the creation of a Union Preparedness Plan for Digital Infrastructures that includes protocols for stressed or damaged infrastructure, technological sovereignty, and requires 112 services to be available even during major natural disasters. It also aims to address the cybersecurity of 6G and facilitating the decommissioning of legacy copper networks, supporting the shift toward more energy-efficient and secure fibre and 5G/6G infrastructures. This modernisation is critical as legacy TETRA systems are old, expensive, and vendor locked. Member states are in favour of a resilient-by-design framework combining dedicated Mission Critical mobile broadband PPDR assets with commercial Radio Access networks.

Interoperability, Cross-Border and the EUCCS

One of the most significant policy initiatives for the trajectory of PPDR communications is the EU Critical Communication System (EUCCS) [7]. This strategic initiative aims to establish a Pan-European interoperable mobile broadband platform by 2030, ensuring seamless operational mobility. The current lack of cross-border interoperability between national emergency communication systems within the EU and Schengen Area creates communication and coordination challenges for first responders working across borders, during both routine operations and large-scale crisis management. To address this, it aims to connect all European law-enforcement and safety responders through a unified, with secure cross-border and cross-industry interoperability of PPDR communication solutions becoming the default. It seeks to do this via mission critical technology (3GPP MCX Services) that supports voice, video, and data exchange between different agencies from different countries in order to support real-time collaboration. The key to this is the requirement for priority and pre-emption of services during crises.

The Niinistö Report frames this objective within a broader whole-of-society approach to resilience, emphasising civil-military synergy and the need for 6G to support both real-time situational awareness [4] [3]. The report explicitly links 6G research to the operational needs of first responders and mandates prioritising interoperability and cross-border functionality in support of EUCCS delivery.

Transitioning to multi-media PPDR communications

European telecommunications policy is increasingly shaped by 6G-specific strategic initiatives and is evolving to reflect the expanded role of communications infrastructure in societal resilience [10] [11]. The Next Generation 112 (NG112) framework supports the transition from voice-based to multi-media emergency services. It modernises emergency call handling beyond voice to encompass real-time video, text, and location data, establishing a baseline expectation for the data richness that PPDR communication systems must support [12] [10].

Spectrum policy is also evolving. The Radio Spectrum Policy Group has emphasised the need for inter-service spectrum sharing frameworks that guarantee PPDR agencies the capacity they require alongside commercial users [9]. They have identified the native integration of Non-Terrestrial Networks as a strategic priority for service continuity in remote areas and during major terrestrial infrastructure failures.

Critical Services Protection

The Critical Entities Resilience (CER) Directive and the NIS2 Directive work in tandem to ensure that 6G networks can sustain PPDR operations under all conditions, physical and digital, routine and catastrophic [13] [14]. Together they constitute an all-hazards approach that treats communication infrastructure not merely as a commercial service but as an essential pillar of societal function [3].

The CER Directive formally classifies digital infrastructure, including public electronic communications providers, as a critical sector. This recognition ensures that the systems supporting emergency communications are recognised and protected as part of the Union's critical infrastructure [15]. It requires essential services for societal and economic continuity to implement resilience plans ensuring that they remain unobstructed during natural disasters, terrorist attacks, or hybrid threats [13] [5] [16]. For PPDR agencies, this means that the physical assets underpinning 6G communications, including base stations, data centres, and backbone links, must be protected and, where disrupted, rapidly restored.

The NIS2 Directive addresses the cyber layer of the same infrastructure, requiring state-of-the-art cybersecurity measures that protect against everything from systems failures, like the loss of connectivity and hardware breakdowns, that result from everything from human error, hackers, to environmental or disaster stress [14] [17]. All entities designated as critical under CER are automatically classified as essential under NIS2, which means future networks used by PPDR agencies will require the most stringent cybersecurity oversight and enforcement measures. The combined effect is a dual-layered protection obligation that addresses both physical and cyber dimensions.

The 2025 EU Cyber Blueprint, structures large-scale cyber crises, to ensure a secure EU-wide communication system [18] [19]. While the previous framework was voluntary, the Cyber Blueprint creates a mandatory harmonised operational model for European cyber crisis management that instructs governments and EU agencies how to act and how to coordinate with each other on detection, analysis, escalation, response, and recovery. It

explicitly integrates civilian and military coordination, acknowledging that 6G infrastructure increasingly serves dual-use purposes. It guides technical (e.g. via CSIRT Network), operational (e.g. supported by EU-CyCLONe), and political (e.g. via Integrated Political Crisis Response) continuity to facilitate rapid information exchange during severe cyber incident, with mandatory 24-hour reporting obligations for significant disruptions applying to both network operators and manufacturers.

The Cyber Solidarity Act complements this by creating an EU Cybersecurity Reserve of trusted private-sector providers deployable to assist Member States or PPDR agencies following a major network failure [20]. It establishes the European Cyber Shield, a pan-European network of Security Operations Centres for real-time cross-border threat detection. It also creates an incident review mechanism, led by ENISA, that can learn from past events to create binding recommendations.

Equipment Integrity and Certification

The Cyber Resilience Act (CRA) and the EU Cybersecurity Act (CSA) address the trustworthiness of the technology itself [21] [22] [23]. The CRA imposes security-by-design and default requirements on all products with digital elements, ensuring that the hardware and software components of future SNS networks are inherently resistant to exploitation and receive mandatory security updates throughout their operational lifecycle. All products should have identity management and authentication, protect integrity and confidentiality of data, and, extremely important for the complexity 6G is expected to bring, they should minimise attack surfaces. It also mandates vulnerability disclosure. This is particularly significant for PPDR, where supply chain vulnerabilities in components such as routers, operating systems, and microprocessors could have mission-critical implications.

The CSA complements the CRA by providing a voluntary certification framework through which SNS components can demonstrate conformity with recognised European standards. The CSA empowers ENISA to establish a European cybersecurity certification framework [24]. It creates a de-risk framework for high-risk entities that allows the EU to mandate them to be phased out or withdrawn. A 2025 amendment to the CSA extends this framework to cover managed security services ensuring that third-party providers supporting PPDR networks are subject to the same quality and reliability standards as the infrastructure itself [23] [24]. For high-criticality PPDR services, high certification under the EUCC (European Common Criteria) can provide verifiable evidence that infrastructure can resist sophisticated, state-sponsored attacks [25]. This certification pathway bridges between technically validated research outputs and the procurable, deployable systems that PPDR agencies can actually adopt.

The EU AI Act addresses the use of AI as part of these systems [26]. The Act classifies as high-risk any AI systems used to evaluate and classify emergency calls, to dispatch or prioritise emergency first response services, signal optimisation, or to manage priority of traffic (which would affect priority and pre-emption, for example). If an AI decides which drone to send or which sensor data is most important, it must undergo strict conformity assessments and have human-in-the-loop overrides. It requires pre-emptive and iterative risk management. It also creates a chain of responsibility between the provider, deployer,

and integration of third-party systems, shifting how high-risk is defined and assessed in 6G research activities (looking at design in isolation is no longer enough).

Privacy and Access

Even in emergency contexts, the General Data Protection Regulation applies, with specific provisions for public interest and emergency situations [27]. 6G PPDR systems handling biometric data, location tracking, or sensitive inter-agency communications must be designed to balance operational effectiveness with privacy protections, not as competing requirements but as co-design constraints. Complementary to this is the Data Act, which allows public sector PPDR services to request data from private companies (like 6G network operators or smart building owners) in cases of public emergency [28]. This means that, if, for example, a smart building collapses in an earthquake, a PPDR team has a legal right to demand access to the building's IoT sensors or the network's local traffic data to find survivors.

2.2. VALUE FRAME

If the policy framework establishes what European 6G systems must be, **the values articulated by PPDR practitioners establish what success looks like when those systems are actually used**. In practice, these values function as the drivers and measures of success, providing the necessary evidence as to whether technical performance and policy compliance has the potential to translate into the intended societal outcomes during a crisis. Technical specs are only as good as the response they enable; a value-aligned response is not just a byproduct of good tech, it is a deliberate design choice. By embedding these practitioner-led values into 6G design, the final infrastructure is engineered to meet the complex demands and desired outcomes of crisis management.

The following synthesis draws on a collaborative workshop involving nearly 40 PPDR practitioners, industry experts, and academics conducted at the PSCE conference in May 2025 [29]. It captures how practitioners understand these values, how they see them as interconnected, and how they look for them in the systems and solutions presented to them.

Figure 2 Core Societal Values for PPDR

Core Values

Practitioners understand values not as a checklist but as a deeply interconnected system, in which addressing one dimension without attending to the others produces incomplete and ultimately fragile results. Four values consistently emerged as primary.

Safety operates on two interdependent levels that must both be served. Citizen safety means ensuring that no person is left behind, particularly those dependent on essential services during crises, and that response systems are fast, reliable, and reach the most vulnerable. First responder safety means that communication systems support rather than burden those in the field: responders should be able to focus on their mission rather than managing technical failures. Practitioners measure this value in concrete proxies, including decreased response times, faster victim location, and reduced technological overhead during operations.

Resilience encompasses three interdependent dimensions. System resilience is the capacity of communication networks to maintain critical functions during infrastructure failures, whether caused by blackouts, wildfires, floods, or cyberattacks. Community resilience is the capacity of social structures to absorb shocks, maintain solidarity, and sustain mutual aid when institutional systems are under strain. Individual resilience is the mental and psychological capacity of both responders and citizens to function effectively under prolonged duress. Practitioners emphasise that these dimensions are not separable: resilient technical infrastructure enables resilient communities, which in turn build the trust and solidarity that effective disaster response requires.

Trustworthiness and trust emerged as the value most consistently identified as a prerequisite for everything else. Without trust, agencies will not share data across organisational boundaries; citizens will not heed warnings; and safety efforts fragment precisely when coordination is most needed. Trust is built through consistent, transparent action, through systems that protect privacy even while enabling surveillance, and through demonstrated competence before a crisis rather than assurances issued during one. Critically, the sources of trust shift with context: in a pandemic, trust in institutions and in responders as community partners is paramount; in a wildfire, trust in the reliability of the data itself becomes the focus.

Quality of life and well-being were identified as among the core outcomes for citizens, and are important links to the whole-of-society perspective of resilience, preparedness and response. This means community safety, solidarity, decreased vulnerability, and freedom from fear, key foundations of preparedness. However, its priority can shift based on the severity of the disaster; for example, in a blackout, keeping people alive might supersede improved sense of safety.

Supporting Values and Socio-Technical Enablers

Beyond the four core values, practitioners identified a set of supporting values and operational enablers that create the conditions in which the core values can be achieved.

These are not secondary concerns; they are the practical prerequisites that determine whether core values are realised in the field.

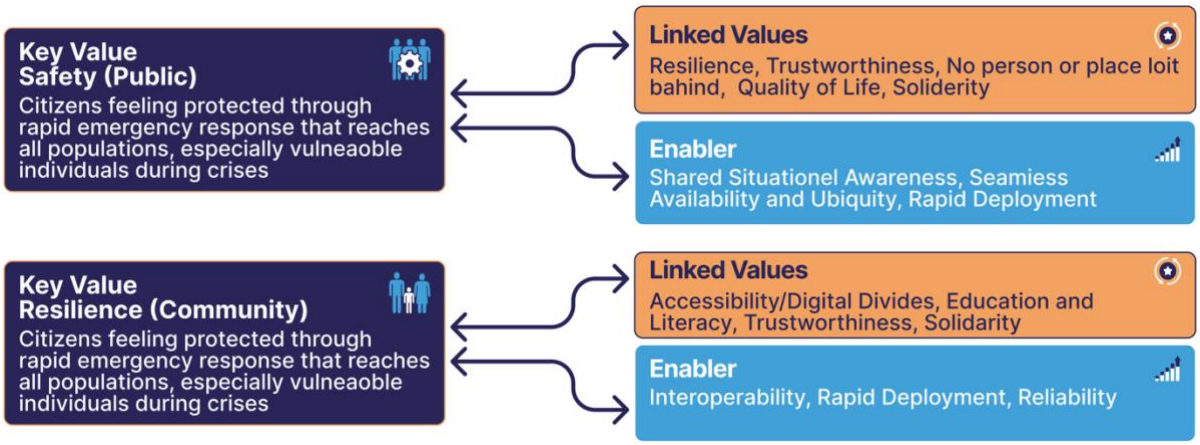


Figure 3 Interconnection between values and enablers

Education and literacy emerged as foundational. Resilient communities require citizens and responders who can engage confidently with new technologies, make informed decisions under pressure, and resist misinformation during crises. Technology that outpaces the capacity of its users to operate it confidently undermines rather than enhances safety.

Solidarity, the social cohesion that enables mutual aid, local self-organisation, and cross-border cooperation, is the human substrate on which technically capable systems depend. **Accessibility and the principle of leaving no person or place behind** ensures that the safety and connectivity benefits of 6G do not accrue only to well-resourced urban areas, deepening existing inequalities in crisis vulnerability.

2.3. WHAT THIS ASKS OF SNS RESEARCH

The strategic goals, policy instruments, and practitioner values described in this chapter converge on a shared set of expectations for what next-generation PPDR communications must be and do. The following themes cut across all three layers of this frame that should shape how SNS JU projects design their work and how that work is evaluated.

Preparedness by design: The shift from reactive to proactive crisis management is now a policy mandate and a practitioner imperative. Systems should be conceived and evaluated not only for how they perform during an incident but for how they reduce vulnerability before one occurs, how they support the training and readiness of responders and communities, and how they contribute to a culture in which preparedness is a normal condition of society rather than an emergency mode.

Resilience across all dimensions: The vision moves toward a multi-layered convergence of ground, aerial, and satellite assets, where resilience is an engineered property maintained through self-healing functions and energy-autonomous nodes even when physical

infrastructure is destroyed. But technical resilience alone is not sufficient. Community resilience and individual resilience are equally part of what 6G PPDR systems must support, and design choices that strengthen one dimension while neglecting the others produce outcomes that are fragile precisely when they matter most.

Interoperability and operational mobility: By 2040 a responder should be able to experience that patchwork of national systems as if they are one. They should cross any border and connect immediately to a shared operational picture and communicate as needed with every agency involved in the response. Achieving this means interoperability is the default and encompassing not just technology but governance structures, training, and readiness that spans organisational boundaries, as well as infrastructure that builds on what already exists rather than requiring wholesale replacement.

A pan-European vision for safety: Safety infrastructure cannot be built or sustained by a single country or solution alone, and systems that cannot scale to cross-border operation fall short of the policy ambition regardless of their technical performance. Strategic autonomy and technological sovereignty are foundational requirements involving reducing dependence on components and supply chains outside European control

Security across the ecosystem: Security must be present from initial design through operational deployment and beyond. This means minimising attack surfaces as cloud-native architectures expand points of vulnerability, protecting the integrity and confidentiality of data that agencies depend on for life-or-death decisions, and maintaining accountability structures and supply chain trustworthiness that recognise security as a condition of the human work on the ground.

Trust as a design requirement: Trust between agencies, between responders and their tools, and between institutions and the public is a pre-condition for effective PPDR activities. Trust must be designed in through transparency, demonstrated reliability, clear accountability for automated decisions, and governance structures that give all parties confidence in how the system behaves and who is responsible for it.

Safety for everyone: The principle of leaving no person or place behind is both a value and a design constraint. 6G solutions should work as effectively in a remote ravine or a collapsed building as in a smart city, and that smaller agencies and rural communities should have access to the same life-saving capabilities as well-resourced urban teams.

Human-centred operation: Systems that increase cognitive load, require specialist knowledge to operate under stress, or place the burden of managing technology on responders in the middle of an incident will underperform when they matter most. The measure of success is whether practitioners can focus on the mission, and whether society benefits from their actions, rather than if the tool is efficient.

Sustainability as operational necessity: Sustainability must be treated as a dimension of operational reliability, not a parallel agenda, including energy autonomy, environmental resilience, and the avoidance of long-term harm to the communities and ecosystems that PPDR systems serve.

3. PPDR PROBLEMS BEING ADDRESSED IN SNS JU PROJECTS

Public Protection and Disaster Relief agencies are at the centre of Europe's capacity to prepare for, respond to, and recover from public safety and social stability emergencies. Nevertheless, these organisations are faced with a range of operational and technological challenges, from fragmented communication infrastructures and interoperability to data silos, cyber-attacks and the growing complexity in cross-border crisis management. The transition towards more digital, networked, and information-centric emergency operations amplifies the need for robust, resilient, and intelligent communication systems capable of supporting mission-critical services in all circumstances.

In the context of the Smart Networks and Services (SNS) Partnership, an increasing number of projects address these challenges head-on by aligning high-level network research with PPDR operational needs. Collectively, these initiatives examine how the future generation of connectivity, 5G evolution, Beyond-5G (B5G), and future 6G features can provide secure, trusted, and resilient infrastructures for first responders and crisis management organisations.

This chapter highlights the primary PPDR challenges that SNS JU projects seek to address and provides information about:

- Main objectives: Projects' missions and their relationship to the broader PPDR innovation ecosystem
- Problem definition: The specific PPDR challenges being addressed and how were they defined (e.g. from previous initiatives, stakeholder input, experience from actual operations).
- Use cases: Scenarios or application areas being addressed.
- Prioritisation rationale: The rationale for selecting these problems and use cases and their strategic value they add to the PPDR environment.
- Involvement of stakeholders: The partnerships between PPDR actors, technology vendors, and policy or regulatory stakeholders.
- Geographic extent: The geographical roll out areas and cross-border relationships being enabled.
- Stages in managing crises: The focus on prevention, preparedness, response, and recovery.

Based on this analysis, this chapter presents a picture of how SNS-funded projects are advancing PPDR capabilities in Europe. While projects vary in scope, maturity, and thematic focus, several shared priorities emerge: It highlights diversity of approach, complementarity of action, and common ambition to deliver future-proof solutions to emergency communications and crisis management. While each project varies in scope, maturity, and

thematic focus, a number of patterns and shared priorities emerge throughout the dataset, including the pursuit of reliable and resilient connectivity, the integration of AI-enabled situational awareness, the deployment of edge intelligence, and the quest for seamless cross-domain interoperability. This consolidated view identifies both short-term advances and longer-term research directions that should shape the evolution of B5G and 6G technologies for public safety.

3.1. KEY PPDR DRIVERS CURRENTLY BEING ADDRESSED

The operational gaps related to the PPDR domain currently addressed by SNS JU projects span different environments, including urban, rural, maritime, industrial and large-event management. However, these often consider the same type of problems or challenges. These can be encapsulated into four overarching thematic clusters: situational awareness; management of events or emergency conditions; critical communications; and network reliability and performance constraints. All these types combined, reflect the most important operational gaps faced by first responders, crisis managers, and safety-critical operators.

Figure 4 Overview of Operational Areas Covered

Situational Awareness

A dominant theme across many projects is the persistent lack of real-time situational awareness, including general lack of monitoring in crowded environments, delays in detecting anomalies like crowd congestion, unauthorized access, hazardous defects or environmental risks, limited visibility for responders in hazardous or low-visibility conditions, and no predictive intelligence for the anticipation of floods or fire propagation. Several projects have also identified the challenge of integrating heterogeneous data sources- ranging from CCTV networks to UAV video feeds, sensor systems, and fire-detection tools- into a coherent, timely picture that will enable effective decision-making. Gaps in sensing, positioning, and GNSS-degraded environments further hamper the ability to reliably track assets, people, or threats.

Management of Events or Emergency Situations

Projects also focus on the gaps in managing emergency situations as well as large events. Challenges include poor incident response times due to fragmented or delayed information flows, a general lack of real-time network resource adaptation tools, and a scarcity of human-centred security mechanisms taking into consideration operator workload and pressures on decision making. During major events, such as festivals, transport hubs, or critical infrastructure operations, projects aim for smarter crowd management, quicker identification of dangerous situations, and more coordinated decision-support for multi-agency teams. Predictive and automated crisis evolution support is scarce, particularly in flooding, wildfire, or maritime incidents.

Critical Communications and Infrastructure

A third cluster concerns the limitations of current communication systems: most still voice-centric and incapable of supporting data-rich, multimedia exchanges needed in contemporary PPDR operations. Projects report problematic real-time communication when public networks become congested or fail, limited bandwidth for high-resolution video or drone feeds, and unreliable connectivity in mission-critical use cases such as UAV coordination, autonomous vehicles, robotic inspection, or remote operation in hazardous environments. Some projects further point out challenges in guaranteeing on-demand coverage for mission-critical (MCx) services with particularly stringent latency and reliability requirements, as well as vulnerability to intentional or unintentional interference during disaster scenarios where first responders depend on uninterrupted communications. Poor interoperability between networks and information systems, particularly in cross-agency coordination, transport systems, or operators of critical infrastructure, remains a major obstacle.

Network Reliability and Performance Constraints

Finally, a large number of projects point to performance, resiliency, and scalability challenges of networks supporting PPDR operations: no coverage in rural or remote areas or during disasters; high latency and limited upload capacity for high-resolution sensing and video analytics; vulnerability to cyberattacks; and difficulties managing surges of traffic generated by autonomous systems, robotics, or multi-camera surveillance networks. In addition, some projects emphasize the need for network architectures capable of seamlessly transitioning between terrestrial networks (TN) and non-terrestrial networks (NTN) to maintain service continuity when infrastructure is disrupted. The growing adoption of cloud-native and virtualized deployments creates new vulnerabilities by enlarging the potential attack surface and exposing mission-critical functions to a variety of risks, including unauthorized access or disruption of control planes. Most of the projects stress the need for energy-efficient nodes, dynamic edge-assisted processing, and resilient network architectures capable of guaranteeing continuity of services even in disruptive or hostile environments. Clearly emerging priorities include integration of heterogeneous networks and secure orchestration of so-called ISAC - Integrated Sensing and Communication - functionalities. Taken together, these problem categories outline the complexity of the PPDR landscape and the requirement for next-generation connectivity solutions. While each

project approaches these issues from different angles, overall challenges strongly align with one another, which underlines common operational pain points and coordinated research needs within the SNS framework.

Taken together, these problem categories illustrate the complexity of the PPDR landscape and the necessity for next-generation connectivity solutions. Although each project encounters these issues from different angles, the overall challenges strongly align, which highlights shared operational pain points and the need for coordinated research efforts within the SNS framework.

In parallel with these technical and operational gaps, the survey responses also highlight that the identification of such challenges is shaped by the stakeholder engagement processes underpinning each project. Rather than being defined purely from a research or technology-driven perspective, the problems captured across the four clusters reflect insights gathered from previous initiatives, real operational experience, and structured input from PPDR agencies and technology partners. This collective engagement provides the foundation through which projects validate the relevance of the issues they target and ensure alignment with the practical realities faced by first responders and crisis-management operators.

Several projects reported that their initial problem framing was shaped by experiences accumulated in earlier Horizon 2020, 5G-PPP, national pilots, or cross-border civil protection exercises, where gaps in interoperability, sensing, and resilient communications had already been observed. These prior initiatives exposed operational limitations such as unreliable coverage in rural or hazardous zones, fragmented information flows between agencies, and challenges integrating heterogeneous sensor and video systems, all of which are echoed consistently across the present survey.

A significant portion of responses emphasised structured engagement with PPDR end-users, including police forces, fire brigades, emergency medical teams, maritime authorities, border-control units, and municipal civil protection services. Through requirement-definition workshops, co-design sessions, technical reviews, and field demonstrations, these stakeholders helped validate the operational relevance of the problem statements. Their input proved especially valuable in identifying real-world constraints, such as workload pressures in control rooms, the lack of predictive tools for evolving emergencies, the difficulty of coordinating multi-agency responses during large events, or the operational consequences of network outages.

Projects also reported engagement with mobile network operators, equipment vendors, SMEs, cybersecurity experts and research organisations, whose contributions helped assess the technological feasibility of proposed solutions and pinpoint integration barriers with existing 5G/B5G infrastructures. Their insights reinforced the urgency of addressing constraints such as latency under high traffic loads, the need for energy-efficient distributed processing, cybersecurity vulnerabilities, including the additional security risks that arise in cloud-native and virtualised deployments, particularly the expansion of attack surfaces and

increased control-plane vulnerabilities, and the limitations of current communication systems when supporting AI-enabled sensing, UAV operations, robotics or other autonomy-driven use cases.

The stakeholder engagement reflected in the survey responses shows that the problem definitions adopted by SNS JU projects arise from a hybrid process of operational validation and technological assessment, combining real-world PPDR experience, feedback from technical partners and evidence drawn from previous deployments. Together, these sources help identify the recurring gaps that first responders and crisis-management organisations encounter across Europe. This ensures that the chosen PPDR problems, and the research actions that follow, are grounded in actual needs, and directly support the evolution of resilient, intelligent, and mission-critical communication systems for the coming B5G/6G era.

3.2. USE CASES AND SCENARIOS BEING DEVELOPED TO ADDRESS THESE PROBLEMS

SNS JU projects seek to actively translate the gaps into concrete, operational use cases aimed at the validation of innovative concepts and technologies behind 6G in realistic environments. These use cases account for the practical layer of the PPDR innovation landscape, providing environments where newly emerging communication systems, sensing capabilities, and intelligent network functions can be tested against the complex, real-world constraints related to emergency response, public safety operations, critical infrastructure protection, and disaster management. Within these use cases, the projects explore a wide range of scenarios, including early-warning fire detection, flood prediction, emergency connectivity deployment, remote medical intervention, secure maritime surveillance, autonomous vehicle coordination, and resilient cyberdefence mechanisms, just to name a few.

By analysing how these use cases are conceived, deployed, and validated, it becomes possible to understand not only the technical directions pursued by SNS initiatives but also the practical pathways through which next-generation communication systems are expected to enhance PPDR capabilities across Europe. The following subsections give a structured overview of these categories, illustrating how each contributes to addressing the operational gaps faced by modern first responders and crisis-management agencies.

Situational Awareness

Situational awareness represents one of the most fundamental requirements across PPDR operations, enabling authorities to understand evolving conditions on the ground and anticipate potential risks. Across European research initiatives, numerous projects explore how 5G and emerging 6G technologies strengthen situational awareness through advanced sensing, data fusion, and real-time analytics.

Projects such as TRIALSNET, with its Smart Crowd Monitoring use case in Madrid, demonstrate how AI-driven video analytics and edge computing can process real-time camera feeds to detect crowd densities, identify anomalies, and provide early-warning indicators during large public gatherings. Similarly, 5G-FIRE and 6G-LEADER, through their respective demonstrations, highlight the role of multi-camera surveillance, UAV-based observations, and secure mission-critical communications in enhancing the visibility of responders during fast-evolving situations.

Urban environments also benefit from coordinated sensing deployments, as illustrated by 6G-PATH, which explores security coordination in smart cities using integrated camera networks and multi-agency data exchange. Complementing these efforts, AMAZING-6G develops capabilities for real-time situational insight in harsh environments, Mission Critical (MCX) communications that support emergency operations, and cross-operator slice orchestration that enables AR/VR-assisted PPDR control rooms. Other projects such as CRITICAL, iSEE-6G, FOR-5G, RESCUE-5G, and SaferFlow extend situational awareness to domains such as telemedicine, smart highways, port security, and environmental monitoring, respectively. An innovative example includes the TRIALSNET Control Room in the Metaverse, which reimagines how responders might visualize and interact with multimodal information in next-generation command centres.

Together, these projects illustrate how situational awareness is evolving from isolated sensor readings to integrated, intelligent, and predictive operational systems. To deepen its impact further, future work could give more systematic attention to two dimensions that the practitioner frame identifies as central. The first is the shared and cross-boundary nature of situational awareness: the challenge is not only assembling a coherent operational picture within a single system but making that picture available continuously and in real time to multiple agencies, including those operating across jurisdictional boundaries with different tools and data standards. Extending the multi-agency data exchange work already present in projects toward genuinely cross-border scenarios would strengthen this significantly. The second is the human dimension of awareness: as sensor fusion, AI analytics, and immersive interfaces generate increasingly rich data environments, the cognitive demands placed on operators grow with them. Designing for manageable workload and interpretable outputs, not just technical performance, would make situational awareness capabilities more robust in the conditions under which they will actually be used.

Management of Events or Emergency Situations

Managing emergencies, from natural disasters to large public events, requires not only reliable communication but also coordinated decision-making supported by real-time intelligence. European PPDR-related projects increasingly combine sensing, automation, and mission-critical communications to enable faster and more informed responses.

Several projects, including 5G-FIRE, 6G-LEADER, and 6G-PATH, demonstrate technologies for early detection of hazards such as fires, security threats in urban areas, or abnormal incidents during major events. These systems integrate drone-based imaging, sensor networks, and AI-enhanced alerting into a unified operational flow that assists first

responders. AMAZING-6G contributes capabilities such as mission-critical (MCX) services, resilient emergency communications, and AR/VR-enabled decision-support systems that facilitate multi-agency coordination. In domains such as emergency medical care, the CRITICAL project explores how low-latency, high-bandwidth links can support real-time telemedicine, enabling clinicians to advise paramedics during transport or in remote locations.

Additional examples include iSEE-6G, which focuses on emergency response in smart highway contexts, and FOR-5G, which develops frameworks for enhanced decision-making during disasters. Projects such as RESCUE-5G and SaferFlow bring this focus to ports and flood-prone zones, where early-warning systems and coordinated command structures can significantly reduce response times. Finally, the TRIALSNET Metaverse Control Room illustrates the future of emergency management, where responders operate within immersive 3D environments populated with real-time data feeds.

These initiatives collectively highlight how 5G/6G networks enhance preparedness, response coordination, and crisis evolution tracking in complex emergency scenarios. To build further on this strong foundation, use cases in this cluster could be designed to address the practitioners' expected outcomes in terms of reduced response times, fewer unassisted health incidents, and more enablers for responders to focus on their mission rather than on their tools. Embedding these as validation criteria alongside network metrics would strengthen the case for adoption. There is also significant scope to extend use case design toward multi-agency, multi-national contexts, where responders from different countries with different systems must coordinate in real time. This coordination challenge directly impacts the EU Critical Communication System (EUCCS) programme and the Digital Networks Act (DNA). Finally, use cases that address pre-crisis training, joint simulation, and the dynamic allocation of connectivity capacity across competing demands in the chaotic opening phase of an incident would extend the portfolio's contribution to preparedness.

Critical Communications and Infrastructure

Critical infrastructures, such as airports, ports, borders, roads, and public utilities, form the backbone of modern society, and their protection is a priority for PPDR organisations. Across multiple projects, 5G and 6G technologies are applied to improve surveillance, automate inspection tasks, and detect emerging threats.

Autonomous robotic platforms connected via high-capacity networks support detailed inspections in locations such as airports, as demonstrated by the Airway project. In border control environments, ABYSS integrates sensing and communication to detect anomalies and facilitate secure monitoring operations. Port infrastructures, essential for trade and logistics, are addressed by ADAPT-G, which explores enhanced security solutions using integrated sensing and communication as well as robotic and drone-assisted observations.

Infrastructure resilience also benefits from sensor networks and environmental analytics, as showcased by SaferFlow, which examines how flood monitoring systems can protect roads, transport corridors, and coastal infrastructures. Additionally, TRIALSNET contributes through

its Public Infrastructure Asset Management use case in Athens, applying AI-enabled analytics, UAV imaging, and 5G connectivity to monitor road surfaces, bridges, and other urban assets.

Through these diverse applications, critical infrastructure protection emerges as a domain where real-time sensing, automation, and high-reliability communications converge to ensure secure and continuous operation. To continue to translate these into impact, future work could engage more systematically with the ecosystem to which new capabilities must apply. The value of next-generation solutions depends partly on how well they can coexist with, complement, and eventually enable transition away from existing systems. Additionally, where use cases incorporate AI-driven decision support, the high-risk requirements should be folded into use case design from the outset. Developing coexistence strategies and transition pathways alongside technical demonstrations would make project outputs more directly useful to procurement and deployment decisions.

However, security and degraded-condition operation deserve more systematic treatment: critical infrastructure is simultaneously a target and a victim in complex emergencies, and use cases should test resilience mechanisms under the pressure of physical damage, network congestion, and active cyber. Solutions also need to work across heterogeneous environments.

Network Reliability and Performance Constraints

As PPDR missions become increasingly data-intensive, the underlying networks must deliver high performance, resilience, and resistance to disruption. This category groups use cases and research activities aimed at guaranteeing service continuity in emergencies, maintaining connectivity despite infrastructure failures, and securing the communication backbone against cyber threats.

Several projects explore hybrid network architectures that combine terrestrial and non-terrestrial networks. Examples such as 5G-STARDUST, 6G-NTN, and UNITY-6G demonstrate how satellite or aerial communication layers can compensate for damaged or overloaded terrestrial networks during disasters. Meanwhile, AMAZING-6G investigates several key enablers of resilient communication, including interoperability for mission-critical systems, robust private networks, advanced MCX services, and secure slice orchestration across multiple operators.

Further developments appear in the FIRESCAN project, which focuses on mission-critical communications tailored to fire-response operations, and in NANCY, whose scenarios explore fronthaul topologies, coverage expansion, and connectivity for mobile nodes under varying conditions. The RIGOUROUS platform additionally contributes an IoT framework designed to support PPDR situational awareness with secure, reliable data exchange.

Collectively, these use cases underline the necessity of robust communication infrastructures capable of withstanding physical damage, cyberattacks, high user density, or extreme operational conditions, ensuring that PPDR teams retain access to mission-

critical information when they need it most. In particular, the portfolio's investment in hybrid TN-NTN architectures, resilient slicing, and edge computing reflects a strong understanding of the performance requirements that PPDR operations impose, and projects are building architectures that could genuinely serve as the backbone of next-generation emergency communications.

Two areas offer directions for further development. The first is operational simplicity under stress: the capacity to rapidly deploy a capable network in the chaotic opening phase of a major incident, when infrastructure may be absent and responders from multiple agencies are converging without a shared playbook. The second is the governance and coordination layer that makes dynamic spectrum use real in practice. The requirement for better and dynamic use of limited resources, including spectrum sharing, prioritisation, and pre-emption across heterogeneous operators, is addressed by several projects at a technical level, but the regulatory and coordination frameworks needed to operationalise these capabilities in multi-operator, multi-country scenarios remain a recognised gap between what technology can offer and what practitioners can currently deploy. Projects should work to inform the policy and practice to bridge this gap in order to make the most of the technology being developed.

Overall view

While SNS JU projects identify a wide spectrum of PPDR challenges, individual prioritisation was necessary in order to focus research and validation efforts within available project constraints. Rather than attempting to cover the full range of PPDR needs, these projects narrowed their scope to a limited set of operational scenarios and, when possible, stakeholder expectations, where the role of advanced communication systems could be meaningfully explored and validated within simulated real-world conditions. This selection process also depended on the feasibility of deployment, experimentation, and evaluation in available environments, as well as by the availability of clear performance metrics. The selected problems lent themselves to structured testing and comparison, while also reflecting partner expertise, and readiness for implementation. Therefore, the use cases addressed in the current SNS JU projects were chosen because they represent the most accessible, high-impact challenges for PPDR operations, where reliable connectivity, low latency, situational awareness, security, and timely decision-making are critical to evaluating system performance.

The selected scenarios and use cases, ranging from crowd and traffic safety, firefighting, flooding, ports, highways, healthcare emergencies, and infrastructure monitoring, directly affect responder safety, coordination, and operational effectiveness in highly dynamic and often infrastructure-disrupted environments. They also impose stringent and measurable network requirements (e.g. latency, reliability, throughput, localisation, energy efficiency, security, and privacy), making them representative and scalable testbeds for validating advanced 5G/6G capabilities such as AI-driven optimisation, integrated sensing and communication, NTN support, edge computing, and cloud-native architectures. From the projects' questionnaires it is evident that prioritisation was further guided by stakeholder

needs, partner competencies, and design-thinking processes, as well as feasibility, speed of validation, and potential for real-world deployment and transferability to other PPDR missions. While other issues were identified, these problems offered the highest combined societal, operational, and technological impact within the project scope and available resources.

Across the spectrum of PPDR-related 5G and 6G use cases, several trends clearly emerge. First, real-time situational awareness is a dominant priority. Projects consistently stress the need to integrate heterogeneous sensing technologies, ranging from CCTV and UAVs to IoT sensors, LiDAR, and GNSS-independent positioning, into unified intelligence frameworks enhanced by AI and edge computing. This reflects a sector-wide shift from static monitoring to predictive, data-rich operational environments capable of early detection of anomalies, hazards, and emergent crises.

Second, many initiatives address challenges related to the management of emergencies and large-scale events, emphasizing faster response times, reduced cognitive load for operators, and enhanced decision-support tools. From metaverse-enabled control rooms to automated crisis modelling and advanced telemedicine, projects are converging on the need for smarter, more efficient, and more integrated emergency management ecosystems.

Third, the evolution of critical communications and infrastructure emerges as an essential trend. Traditional voice-centric PPDR systems are no longer sufficient to support data-heavy operations involving high-resolution video, robotic inspection, autonomous vehicles, and coordinated UAV systems. As a result, capabilities such as MCX over 5G/6G, cross-operator slicing, and the fusion of terrestrial and non-terrestrial networks are gaining momentum to ensure uninterrupted mission-critical connectivity.

Finally, concerns regarding network reliability, cybersecurity, and performance constraints are widely shared across projects. Rural coverage gaps, network congestion during crises, vulnerabilities in virtualized infrastructures, and the surge of traffic generated by dense sensing and robotic systems all highlight the need for resilient, secure, and energy-efficient architectures. Emerging approaches include post-quantum-ready security, AI-based threat detection, autonomous RAN optimization, ISAC-driven orchestration, and hybrid TN-NTN configurations.

3.3. PPDR LIFECYCLE COVERAGE IN SNS JU PROJECTS

The projects approach the PPDR lifecycle through different configurations of its four key concepts: Prevention, Preparedness, Response and Recovery. These phases provide a common framework for understanding how emergency operations are structured, from anticipating risks to restoring normality after an incident. However, the survey responses show that projects rarely focus on a single phase. Instead, they combine these phases in strategic ways that reflect their technological scope and intended operational impact. A

small number of low-TRL projects reported no explicit alignment to PPDR lifecycle phases, given their exploratory nature.

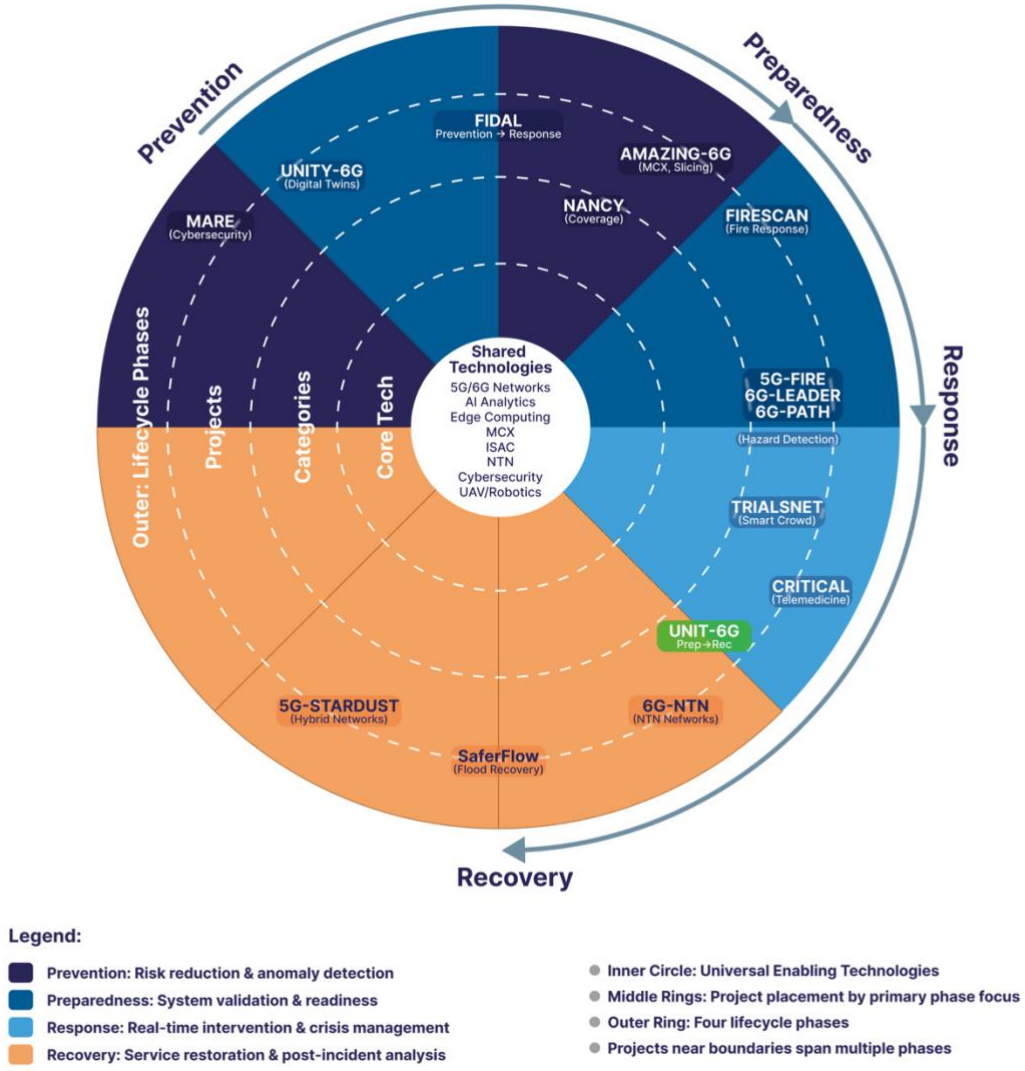


Figure 5 Phases of Disaster Risk Management Engaged

Prevention - Preparedness - Response: The Most Common Configuration

The most frequent combination identified is the integration of prevention, preparedness and response phases. This pattern is characteristic of projects that aim to manage the full front-end of emergency operations by detecting risks early, ensuring technical readiness and supporting real-time intervention. Solutions such as AI-assisted fire detection, crowd behaviour monitoring, port surveillance and flood prediction all share this profile. Their rationale is clear: early anomaly identification reduces escalation, preparedness guarantees that the system behaves as required under PPDR constraints, and response capabilities transform real-time data and edge processing into actionable situational

awareness. These three phases naturally reinforce one another in use cases where rapid detection and rapid reaction are inseparable. Projects such as MARE also follow this combination, placing a particularly strong emphasis on preventing and mitigating security breaches in future 6G systems, while supporting response-oriented validation of defence strategies under realistic threat conditions.

Preparedness - Response: Operational Solutions Requiring High Readiness

The second most common combination is preparedness alongside response. This pattern dominates in solutions that depend on high-performance connectivity during active incidents, such as UAV and XR coordination, deployable private networks or robotic and sensor-based inspection systems. These projects centre their value on real-time operations and therefore rely on thorough testing and configuration beforehand. The logic behind this combination reflects a practical orientation: these systems deliver impact during the event, but they must be validated and reliable in advance.

Prevention - Preparedness: Risk Reduction and System Assurance

A smaller but important group of projects works across prevention and preparedness, particularly in areas tied to cybersecurity, network assurance and infrastructure monitoring. Here the priority is to reduce vulnerabilities and detect anomalies before they propagate into critical failures. Post-quantum cryptography, Zero Trust frameworks, threat modelling, DevSecOps and AI-based inspection, all fall into this category. Recovery and response phases have less relevance for these systems because their primary purpose is to avoid crises from emerging at all, while ensuring that defences and monitoring mechanisms are consistently validated. Recent feedback confirms this trend with UNITY-6G explicitly positioned in this category, using digital-twin technologies to enhance prevention and preparedness capabilities rather than operational response.

Preparedness - Response - Recovery: Bridging Action and Post-Event Continuity

Several projects span preparedness, response and recovery, especially where the operational cycle naturally extends beyond the incident itself. Medical emergency support, flood management systems and digital-twin based coordination tools exemplify this structure. These projects prepare the system and workflows beforehand, deliver real-time situational awareness and coordination when the incident occurs, and continue to support post-event through restoration, analytics or remote monitoring. The rationale for including recovery is clear in domains where post-incident stabilisation is essential, such as healthcare or critical infrastructure. UNITY-6G, 6G-NTN, and 5G-STARDUST contribute to this pattern, with the latter two leaning more heavily on system architecture design and development to enable resilient response and subsequent recovery phases.

Response - Recovery: Reactive and Restorative Solutions

A smaller subset focuses on response and recovery only. This pattern appears in cyber-resilience mechanisms with autonomous anomaly mitigation, self-healing networks and continuity-of-operations tools, as well as in medical follow-up solutions. Because these systems intervene during an incident and extend their role into the restoration phase, their contribution is primarily reactive and restorative rather than preventive or preparatory.

Full Lifecycle: Prevention - Preparedness - Response - Recovery

Only a few projects cover all four phases of the PPDR lifecycle. These are predominantly cybersecurity and resilience frameworks designed to secure the entire operational chain end-to-end. Their logic is rooted in the understanding that cyberthreats can appear at any point in the lifecycle. Therefore, prevention through modelling, preparedness through validation, response via real-time detection and mitigation, and recovery through autonomous service restoration are all necessary components of a complete resilience strategy.

Taken together, these combinations demonstrate that the SNS JU projects contribute to the PPDR lifecycle in complementary ways rather than competing ones. Response and Preparedness emerge as the most prevalent phases, reflecting the need for high-performance, reliable and validated communications during emergencies. Prevention appears strongly where monitoring and cybersecurity are predominant, while Recovery features especially in medical, cyber-resilience and system-restoration domains. The distribution of combinations ultimately reveals a strategically balanced ecosystem, in which the SNS programme strengthens both the operational core of PPDR activities and the broader resilience of the systems that support them.

3.4. STRENGTHS AND AREAS FOR GROWTH

SNS JU PPDR initiatives are strongly rooted in the everyday realities faced by first responders, emergency managers, and public authorities across Europe. Rather than treating technology in isolation, these projects are oriented toward the conditions in which lives are at risk, decisions must be made quickly, and communication failures have consequences. This people-centred orientation offers valuable lessons for shaping future priorities in research and innovation.

What the portfolio does well

A clear strength is the grounding of projects in scenarios that safety organisations actually face: wildfires, floods, large public events, accidents, health emergencies, and border security. These are not hypothetical use cases but operational realities, and by addressing them directly the portfolio supports public safety, protects responders, and sustains vital services, all of which will remain central societal concerns in the next decade.

Equally important is the attention paid to how emergencies are managed in practice. Many projects are built around real operational workflows: how control rooms function, how teams coordinate, how information is shared, and how decisions are made under pressure. The consistent emphasis on situational awareness, interoperability, and clear communication reflects a shared understanding among stakeholders that technology is only useful if it makes situations clearer, supports better decisions, and allows teams to act faster and more safely.

The portfolio also demonstrates strong awareness that public trust in emergency services depends on the reliability of the systems responders use. Projects consistently address how communications must keep working when networks are congested, damaged, or under attack, and the security and resilience work responds directly to urgent practitioner concerns: cyberattacks on mission-critical systems, coverage loss during infrastructure failure, and vulnerabilities in increasingly virtualised network environments. By spanning the full PPDR lifecycle, the portfolio is well positioned to meet the preparedness-by-design mandate of the Preparedness Union Strategy. The cross-sector engagement across researchers, industry, policymakers, standardisation bodies, and PPDR agencies is a foundation to build on.

Where future work could go further

Several directions emerge where future work could deepen this foundation.

Cross-border and pan-European interoperability remains the most urgent priority: not just technical compatibility, but the capacity for responders from different agencies and nations, arriving with different systems and limited shared preparation, to achieve situational awareness and coordinated command in real time. The EUCCS ambition of seamless, borderless connectivity for all European safety responders by 2030 requires shared governance, harmonised spectrum, common standards, and demonstrated cross-border interoperability. The most concrete near-term blockers are the absence of a Pan-European IPX roaming hub and the lack of MCX-to-MCX interconnection standards. Progress must be validated through live field trials and cross-border exercises with PPDR agencies, not only lab and simulation environments, generating the operational evidence that the EUCCS programme and prospective adopters need. Stakeholders are equally clear, however, that the governance layer is the harder problem: who commands when incidents cross borders, how data-sharing is pre-agreed before a crisis rather than negotiated during one, and how standard operating procedures translate across agencies and languages. SNS research that solves the technical interoperability problem without engaging the governance layer will not achieve operational deployment.

Human-centred design deserves to become standard in use case development. The value of even the most capable system depends on whether it reduces cognitive load, fits within existing command structures, and can be deployed without specialist support. This means designing for differentiated roles: the field operator needs a hands-free minimal interface; the tactical officer needs tablet-level situational awareness; the incident commander

needs full data access, all on a shared underlying platform. Similarly, the responder in the field needs a small device that can fit neatly on their uniform as they crawl through buildings yet still connect to the outside world. All of these need to be able to engage on the same platform. Deeper integration of end-user communities throughout design and testing, rather than primarily at validation stages, would strengthen both relevance and transferability across the diversity of European PPDR contexts.

Preparedness offers significant scope for development, and is taken up in detail in the next chapter. Practitioners consistently identify training, readiness, and pre-crisis coordination as foundational to effective response, and the Preparedness Union Strategy makes preparedness-by-design a policy mandate that future work should explicitly address. Use cases should be designed not only for primary operating conditions but across the full PACE hierarchy (Primary, Alternate, Contingency, Emergency): a use case that only works when the preferred system is available is not a reliable guide to what practitioners will actually need. Stress-testing scenarios against contingency and emergency conditions would generate more realistic requirements and more useful evidence for both the EUCCS programme and prospective adopters.

Resilience should structure use case design. A consistent finding from operational experience is that the equally as consequential as a single point of failure is the absence of graceful degradation. When one element fails and the whole system collapses, it does so at precisely the moment when structured fallback would matter most. Resilience as a design value therefore means engineering for continued function at reduced capacity under progressive failure, not simply providing backup layers that are themselves dependent on the same infrastructure they are meant to replace.

4. WHAT TECHNOLOGIES ARE BEING INVESTIGATED

The use cases and operational gaps identified in Chapter 3, such as connectivity that collapses when terrestrial infrastructure is damaged, situational awareness that fragments at agency and national boundaries, and decision-making under conditions of extreme cognitive load, each demand a technical response. But no single technology resolves them. What the SNS community has developed is an interconnected set of capabilities, each addressing a distinct layer of the operational problem and each depending on the others to deliver its value under crisis conditions.

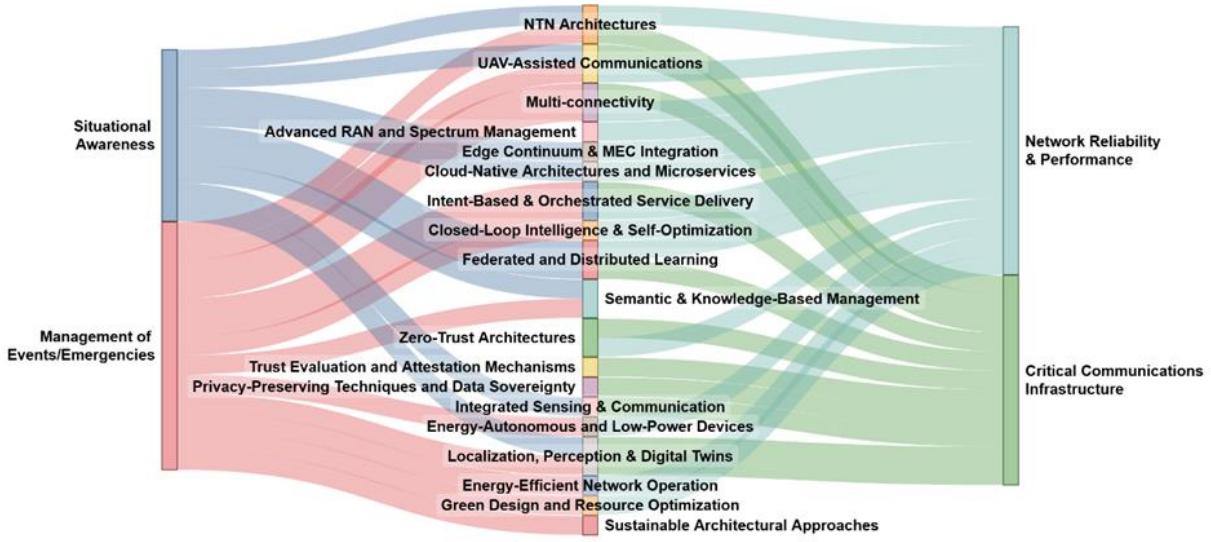


Figure 6 Overview of Technology as applied to PPDR Use Cases in SNS JU projects

This chapter surveys that portfolio across six technology domains, reading them not as parallel workstreams but as a layered architecture designed in response to the requirements that Chapter 3 established:

- The foundation is radio access and connectivity, where multi-layered space–air–ground architectures ensure communication survives when terrestrial nodes are damaged or overloaded by combining NTN satellite links, UAV-mounted base stations, resilience-aware RAN slicing, and multi-connectivity frameworks.
- The intelligence needed to make that connectivity operationally useful sits one layer up, in edge and cloud-native infrastructure, where MEC integration, intent-based orchestration, and cloud-native microservice design push real-time decision-making to the field, enabling the low-latency performance that situational awareness, telemedicine, and multi-agency coordination demand.
- Driving the adaptation of both layers is AI/ML-driven management and automation, where closed-loop control, federated learning across distributed agencies, and semantic reasoning allow networks to self-optimise, self-heal, and translate high-

level mission objectives into autonomous network reconfiguration; thus, reducing operator burden at exactly the moment cognitive load is highest.

- Securing this increasingly virtualised and multi-domain architecture is the work of the security, trust and privacy domain, which addresses the expanded attack surface that cloud-native deployments and cross-agency data exchange introduce, through zero-trust architectures, automated trust assessment, and privacy-preserving computation.
- The devices and sensing domain extends the network's perceptual reach, using Integrated ISAC, digital twins, and advanced localisation to transform 6G from a passive connectivity layer into a native sensing environment capable of tracking personnel and monitoring hazardous conditions in GNSS-degraded or smoke-obscured environments.
- Energy efficiency and sustainability complete the picture by treating energy autonomy as a direct resilience requirement; thus, ensuring that nodes, devices, and edge infrastructure sustain operations when power supply itself is disrupted by disaster.

An operational alignment section closes the chapter by mapping these six domains to the use case clusters of Chapter 3 and identifying where the portfolio's combined contribution is strongest and where future work should focus.

4.1. RADIO ACCESS AND CONNECTIVITY

The research within SNS JU projects is focused on advancing new paradigms of ubiquitous and resilient connectivity via the convergence of multiple types of networks, such as terrestrial, aerial, and non-terrestrial networks. These advancements have the potential to greatly contribute to PPDR scenarios where continuous communication, dynamic adaptation of the network's topology, and rapid restoration after an infrastructure failure will be needed. The areas of study currently being pursued include NTN architecture, UAV-assisted communication, multi-connectivity techniques, and intelligent-spectrum/RAN-based methods that allow for the adaptation and efficiency of the network. These technologies enable the practical implementation for the operational requirements stated in Section 5 which identify the need for robust communication networks and real-time situational awareness in those PPDR scenarios where the traditional infrastructure may be unavailable or significantly degraded. By grounding 6G research in mission-critical use cases, the resulting impact is a higher quality of life and well-being, defined by the ability to preserve life and maintain societal functions under all circumstances. This includes ensuring that responders can focus on their mission rather than managing connectivity, which is as much a safety requirement as any network performance metric.

Figure 7 Key connectivity technologies being addressed in PPDR SNS JU projects

NTN Architectures (GEO/LEO/HAPS)

The most widely adopted technological approach across PPDR-focused SNS JU projects is the adoption of multi-layered system architectures, which combine conventional terrestrial networks with LEO and GEO satellites as well as opportunistic aerial platforms, such as HAPS or UAVs. The main focus for improving 6G performance through advanced technology is the implementation of regenerative payloads on LEO nodes to decrease end-to-end latency compared to traditional payloads. Projects explore different configurations of functional splits, ranging from full gNB or IAB-donor functions onboard the LEO node for direct access to hybrid configurations placing RU and PHY onboard satellites and DU/CU/Core on feeder or ground segments [ADROIT6G, 6G-NTN]. The design priorities include low-latency connectivity in post-disaster recovery [6Green], minimization of signalling delays using multi-connectivity [5G-STARDUST], and gateway-independent communication continuity [6G-NTN]. In addition, Hexa-X-II advances these architectures through intelligent beamforming and adaptive link management for GEO–LEO coordination, while iSEE-6G introduces the Joint Communication, Computation, Sensing and Power (JCCSP) paradigm, extending NTN to support situational awareness and energy transfer. Collectively, these developments turn NTN from a backup layer into a distributed, intelligent, and compute-enabled substrate for resilient 6G operations. Last but not least, the UNITY-6G project develops a unified architecture embracing NTN and terrestrial 6G components building on disaggregated RAN concepts, with an overarching AI-based multi-domain orchestration necessary to achieve sustainable data communication operations during both preparedness and disaster response phases. These NTN architectures are closely tied to use cases that involve emergency connectivity deployments and therefore utilize LEO and GEO satellites for gateway-independent communication continuity in order to provide ubiquity and seamless availability when the terrestrial infrastructure is destroyed. The underlying

technical capability enabling this redundancy is a direct improvement of system's resilience, which provides the necessary redundancy to enable critical functions to continue operating when terrestrial infrastructure is disabled by a blackout, wildfire or other disaster.

UAV-Assisted Communications

UAVs and drones are extensively employed in PPDR-oriented architectures to provide rapid connectivity restoration and on-demand coverage. In most cases, UAVs form part of integrated space–air–ground systems that ensure service continuity when terrestrial infrastructure is damaged. Several projects use regenerative payloads in HAPs or UAVs acting as lightweight gNBs for direct access or IAB donors for indirect access [6G-NTN, ADROIT6G, 6G-PATH]. UAVs also enable real-time situational awareness through sensor deployment, video capture, and environmental mapping [6Green]. iSEE-6G expands the UAV role by embedding communication, computation, sensing, and power transfer capabilities into UAV-based platforms, while 6G-LEADER explores XR interaction supported by UAV connectivity for first responder operations. Hexa-X-II introduces AI-assisted coordination among UAVs through intent-based management, enabling them to operate as autonomous aerial agents that dynamically allocate communication and sensing tasks. NANCY integrates distributed MEC nodes on UAVs to locally host virtualized network functions and analytics, whereas 6G-NTN explores hierarchical control between terrestrial and aerial layers to improve link stability and efficiency. 6G-PATH integrates the UAV as gNBs for direct access but also as relay from satellite connectivity to private 5G coverage. Overall, UAV-assisted networks evolve into intelligent, compute-augmented communication agents central to PPDR resilience, especially in use cases such as maritime surveillance, fire response, and providing real time situational awareness and supporting XR assisted mission capabilities. The result is an improvement in safety of first responders since they can focus on performing their jobs versus managing the technology.

Multi-Connectivity

Multi-connectivity enhances both reliability and throughput, enabling simultaneous use of terrestrial and non-terrestrial links. Two configurations prevail: NTN–NTN, where UEs connect to distinct satellite layers (e.g., LEO–GEO), and TN–NTN, enabling seamless handovers between terrestrial and satellite domains. This mechanism is vital for maintaining connectivity in disaster zones or during network restoration phases [5G-STARDUST, 6G-NTN], by also exploiting multi-path protocols (i.e. MPTCP and MPQUIC) and ATSSS functionalities. Seamless transitions require adaptation of control protocols and timing mechanisms to compensate for varying latencies. Beyond redundancy, projects now employ multi-connectivity for adaptive link selection and intelligent traffic steering. ADROIT6G and iSEE-6G extend this concept with dynamic service migration between terrestrial, aerial, and satellite resources through distributed orchestration. ROBUST-6G incorporates AI-driven link control and self-healing strategies to maintain connectivity under infrastructure stress. Together, these approaches redefine multi-connectivity as an intelligent resilience mechanism rather than static redundancy, which is critical for providing the necessary functionalities in disaster areas. The impact on both trustworthiness and trust is a result of

ensuring the reliability of data for emergency responders who are relying on this data in high-risk situations.

Advanced Ran and Spectrum Management

Several projects introduce advanced RAN functions that move beyond conventional cell-centric design toward flexible, software-defined, and spectrum-aware architectures. Spectrum sharing across heterogeneous systems is a key research theme, with SHARE6G focusing on coexistence in the 7–15 GHz range, integrating AI/ML for dynamic resource allocation among IMT, radar, and NTN links. Hexa-X-II and FIDAL develop RAN orchestration mechanisms that exploit AI for energy-efficient operations and fine-grained service differentiation. 6Green examines cross-layer scheduling policies for green spectrum use, while ROBUST-6G introduces resilience-aware RAN slicing to ensure service continuity during partial network failure. 5G-STARDUST and 6G-NTN in turn focus on spectrum management (sharing and co-existence) as part of the unification of TN and NTN segments. In addition, 6G-LEADER aims to develop an Open Radio Unit (RU) operating in both the FR1 and FR3 spectrum bands, while integrating ML-driven xApps that will provide spectrum management capabilities in near realp-time. Collectively, these efforts converge toward intelligent spectrum management systems capable of autonomously balancing performance, energy efficiency, and resilience in dynamically evolving PPDR environments. They support a plethora of PPDR use case including smart crowd monitoring and security coordination in smart cities, which will utilize AI/ML to dynamically allocate resources based on real-time conditions within the network. As automation and AI play an increasing role in these allocation decisions, ensuring transparent and accountable mechanisms for how spectrum priority is assigned, particularly between PPDR and commercial users during an emergency, becomes a design requirement alongside technical performance. As such, this directly improve citizen safety, providing quantifiable impacts such as reduced response times and the capability to find victims quicker.

4.2. EDGE AND CLOUD-NATIVE INFRASTRUCTURE

Based on the operational needs for real-time situational awareness and fast incident response times that are defined in section 5, section 6.2 explores how MEC integration, cloud-native microservice design, and intent-based orchestration can be implemented to enable those operational requirements in the field. The migration of intelligent procedures from centralized nodes to the edge enables the establishment of distributed, composable frameworks that will support service continuity and deterministic performance under mission-critical emergency conditions. Edge and cloud-native infrastructure support the preparedness-by-design principle by improving resilience and allowing to sustain critical societal functionality under extreme duress.

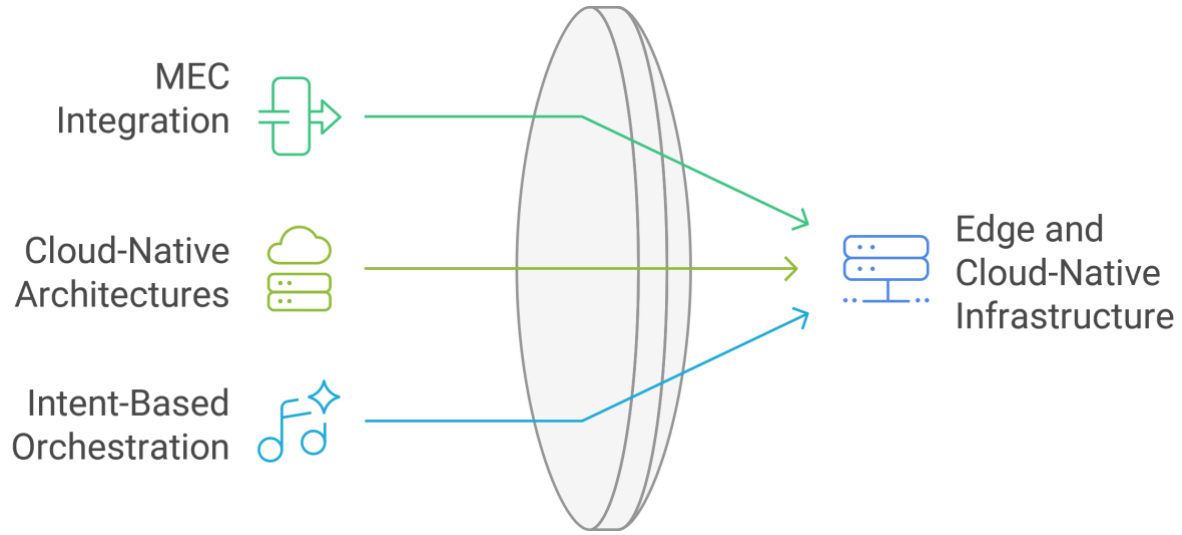


Figure 8 Edge and cloud native technologies being addressed in PPDR SNS JU projects

Edge Continuum and MEC Integration

The integration of Multi-Access Edge Computing (MEC) into the network continuum is a fundamental enabler for low-latency PPDR applications. ADROIT6G adopts a distributed edge-cloud continuum with lightweight containers to support adaptive service deployment close to users. iSEE-6G integrates MEC and satellite edge nodes to perform joint computation, sensing, and communication, enabling energy-efficient offloading and local decision-making. 6G-Cloud proposes a hierarchical edge architecture for service-oriented design, allowing PPDR applications to dynamically instantiate edge services based on demand and network state. Hexa-X-II extends edge computing resource orchestration with AI-assisted mechanisms to manage heterogeneous computing tiers, also considering trust levels across the diverse continuum layers and involved devices. ELASTIC focuses on mobility-aware edge clusters ensuring deterministic performance under emergency conditions. Furthermore, 6G-LEADER will develop digital over-the-air computation algorithms, supporting edge AI tasks, integrating it in an O-RAN architecture. Finally, 5G-STARDUST and UNITY-6G address the potentials of edge-cloud continuum across ground and space segments to achieve a more effective service coverage through distributed edge servers. Together, these projects emphasize distributed, composable edge frameworks ensuring robustness and flexibility in crisis scenarios. Edge continuum and MEC integration infuses PPDR applications, such as real time telemedicine and mobility aware clusters for emergency conditions, with the ability to achieve the low latency requirements. Therefore, by enabling localized inference and efficient offloading, it contributes to reduced response times. In addition, this technology enables the ability to potentially save lives in remote or disaster-struck areas where the ability to rapidly respond may not be a given.

Cloud-Native Architectures and Microservices

Cloud-native design principles are adopted widely to ensure scalability, resilience, and automation in 6G infrastructures. ADROIT6G, UNITY-6G, and NANCY employ service mesh and container orchestration frameworks, enabling lightweight deployment of VNFs and

CNFs across edge and core. IMAGINE-B5G highlights the shift from monolithic NFV frameworks to microservice-based orchestration, improving reliability and lifecycle automation. 6G-Cloud applies these paradigms to build service-oriented platforms capable of supporting critical PPDR workloads across federated edge clusters. Cloud-native network functions are combined with CI/CD pipelines to allow rapid updates and self-healing, a critical feature for dynamically evolving PPDR environments. This transition to using microservice-based orchestration to enable scalability and self-healing of critical workloads provides the necessary reliability and resilience required to meet the operational requirements of safety and system resilience, while at the same time it enables both physical and digital 6G infrastructure to remain unobstructed during crisis situations.

Intent-Based and Orchestrated Service Delivery

Intent-based management enables declarative network control, where high-level mission objectives are translated automatically into orchestrated service configurations. Hexa-X-II explores AI-assisted intent translation for resource orchestration across distributed domains, also demonstrated in the context of the project's System PoC: more specifically, intents related to collaborative robot-powered industrial logistics tasks are received by the application interface; intents are automatically translated into concrete network and compute resource-related actions, e.g. Inventory audit inspection for warehouse sector X to be realised by a specific UAV node. Gains are also reported in the last project PoC-driven deliverables. ADROIT6G demonstrates policy-based service composition using cloud-native frameworks. FIDAL extends orchestration through semantic models supporting adaptive intent resolution and cross-domain lifecycle management. CASTOR focuses on mapping Service and Security Level Agreements (SSLAs) into network policies through telemetry-based orchestration. NANCY designed a Blockchain-based Marketplace for mobile network operators, which can be used to exchange services and sign Service Level Agreements (SLAs) between operators. Finally, UNITY-6G develops a cross-domain orchestration concept able to tune the network operations according to the use cases dynamics, hence proving particularly suitable to network restoration operations during PPDR situations. The convergence of these technologies ensures that PPDR services can be automatically deployed, monitored, and optimized based on operational intent rather than manual configuration. At the same time, this achieves the measurable impacts of operational efficiency and trustworthiness, which enables the reliable and deterministic performance of complex multi-agency responses to emergencies.

4.3. AI/ML-DRIVEN MANAGEMENT AND AUTOMATION

This section delves into the AI-based, predictive operational environment needed to support the various PPDR use cases described in Section 5. Intelligent management and system automation provides a direct solution to the previously identified operational gaps such as lack of predictive intelligence in real-time for fire and flood propagation and extremely high cognitive load on first responders. In this direction, this section explores the AI/ML enablers being developed to enable automated responses and optimized network performance; these technologies allow state-of-the-art networks to manage the extremely large volumes

of sensor and UAV generated data while providing the extremely reliable service required for mission-critical operations. All in all, this section presents the vision of the SNS-JU projects to transform the principle of preparedness-by-design into that of predictive autonomous systems. Realising this vision responsibly requires that autonomous behaviours are interpretable, that human oversight is preserved for high-stakes decisions, and that the systems performing them can be held accountable, requirements that are now codified in the EU AI Act for high-risk applications in emergency contexts.

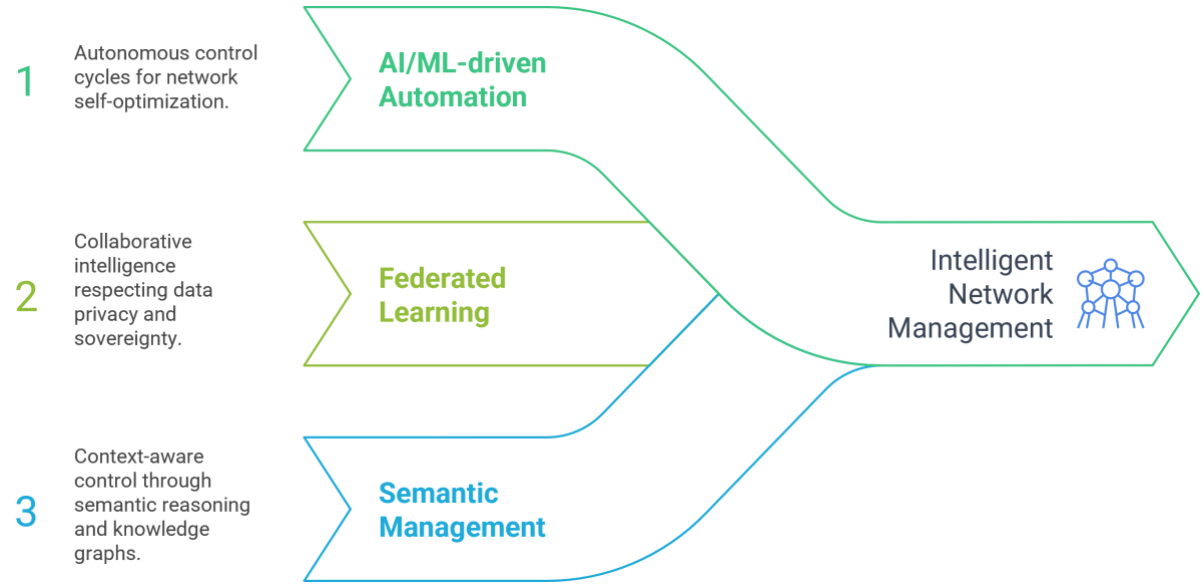


Figure 9 AI and related activities being considered in PPDR SNS JU projects

Closed-Loop Intelligence and Self-Optimization

AI-driven automation is at the core of next-generation network operation. Closed-loop management integrates monitoring, analytics, and reconfiguration into autonomous control cycles. Hexa-X-II, UNITY-6G, and ADROIT6G employ AI controllers for self-optimization across RAN, edge, and core, while ROBUST-6G introduces multi-agent systems for distributed decision-making under uncertainty. 6Green focuses on energy-aware learning loops for adaptive performance tuning. FIDAL contributes digital twins and data-driven feedback loops for continuous network adaptation. In addition, 6G-LEADER targets to extend the current O-RAN closed-loop control with xApps operating at 10 ms time scales and dApps deployed at the O-DU for sub-10 ms control of RAN functionalities. These AI-enabled mechanisms collectively improve service reliability, responsiveness, and resilience, particularly in highly dynamic PPDR environments. They contribute to the needs for network restoration, emergency response, and other real-time adaptation requirements to address infrastructure damage or rapid increases in traffic.

Federated and Distributed Learning

To address data privacy and distributed operation constraints, several projects adopt federated learning for model training across heterogeneous domains. Hexa-X-II implements hierarchical federated learning across RAN and edge to optimize radio

parameters without centralizing data. NANCY applies privacy-preserving learning in MEC nodes for localized threat detection. ADROIT6G and IMAGINE-B5G integrate distributed AI pipelines allowing PPDR systems to benefit from collaborative intelligence while respecting data locality and sovereignty. Also, 6G-LEADER will support federated learning by exploiting its digital over-the-air computing solutions to exchange in an energy- and spectral-efficient manner model parameters from distributed edge nodes. Federated frameworks also reduce communication overhead and provide a scalable path for incremental intelligence deployment across edge and core tiers. By training models on heterogeneous domains without the requirement of centralized data, multi-agency coordination and localized threat detection are enabled. This provides trustworthiness and trust by ensuring privacy by design and data sovereignty. The final output is a safer, more trusted operational environment for sharing intelligence amongst agencies without placing sensitive information at risk.

Semantic and Knowledge-Based Management

Semantic and knowledge-based management introduces reasoning capabilities into network automation. FIDAL uses ontology-driven orchestration to align service objectives and network resources. iSEE-6G integrates semantic reasoning for situational awareness in joint communication and sensing, allowing decision-making based on interpreted environmental data. 6G-Cloud extends this with knowledge graphs supporting policy inference and self-consistent orchestration. Another project supporting semantics is 6G-LEADER where integration with O-RAN intelligent applications in the form of xApps will be conducted, reducing control plane overheads and providing information compression tasks in the data plane. Finally, NANCY utilizes explainable AI (XAI) methods in order to provide insights into the decision-making processes of AI models. Also, the outcomes of the XAI methods can be further processed using Large Language Models (LLMs) to assist in the interpretability. These frameworks move network control from purely data-driven to context-aware, supporting intelligent adaptation in PPDR operations; thus, contributing to shared situational awareness.

4.4. SECURITY, TRUST AND PRIVACY

Based on the identified critical gaps of section 5, such as vulnerabilities to cyber-attacks, the regulatory burdens of sensitive information and the larger threat surface introduced with cloud native architectures, this section explores the security trust and privacy focused technologies that have been employed by the SNS-JU projects. As such, this section has focused its investigative efforts on zero-trust architectures, automated trust assessments and privacy-preserving technologies to provide assurance that the transition to a data-centric multi-agency response can occur within a resilient framework that adheres to the preparedness-by-design principles necessary for mission-critical operations. These protections must function not only under nominal conditions but under the combined stress of physical infrastructure damage, high traffic load, and active threat, the precise conditions under which PPDR systems are most needed and most vulnerable.

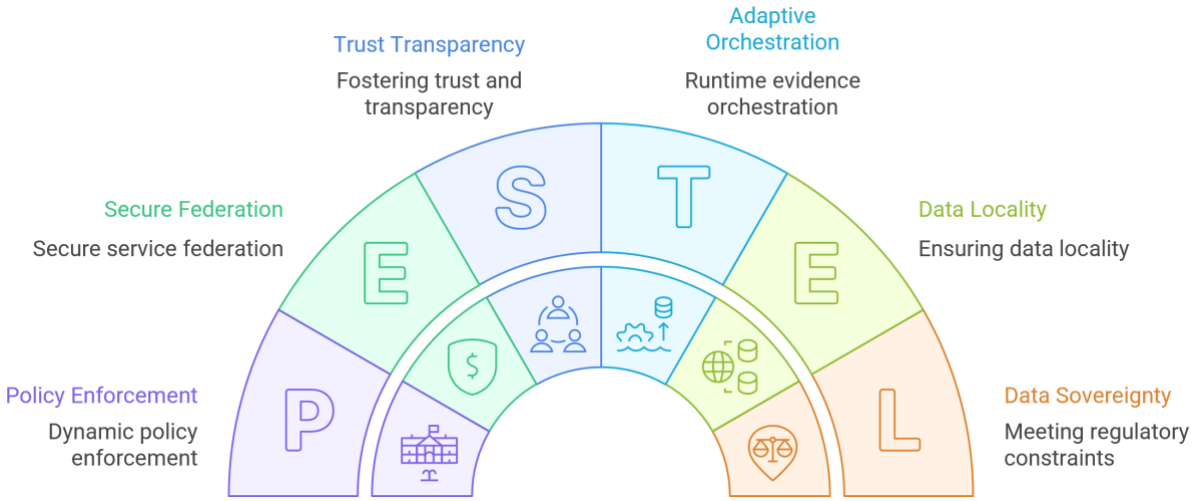


Figure 10 Security, Trust, and Privacy Technology engaged in PPDR SNS JU projects

Zero-Trust Architectures and Policy Enforcement

Security in PPDR networks increasingly relies on zero-trust architectures ensuring continuous verification and dynamic policy enforcement. CASTOR implements SSLA-based orchestration to enforce fine-grained policies across multi-domain networks, targeting to ensure minimum trust levels across the network and compute infrastructure in an end-to-end manner. iTrust6G introduces adaptive trust anchors and distributed identity management to protect service integrity. ROBUST-6G integrates zero-trust control into RAN and edge orchestration frameworks. Hexa-X-II links zero-trust design with exposure APIs for secure service federation, and implements the Trust Evaluation and Level of Trust Assessment Functions (TEF and LoTAF respectively). Together, these frameworks aim to achieve secure-by-design multi-domain operation with dynamic trust recalibration and provide a clear path towards achieving system resilience; thus, having an end impact of safeguarding critical infrastructure and allowing societal functions to continue operating.

Trust Evaluation and Attestation Mechanisms

Trust evaluation is increasingly automated through telemetry-based attestation and behavior analytics. CASTOR and EA6LE develop trust computation frameworks using runtime evidence for adaptive orchestration. iTrust6G focuses on verifiable trust scoring between services, whereas NANCY applies blockchain-inspired attestations for peer-level verification within distributed edge clusters. Moreover, MARE will leverage a complete lifecycle for secure (zero-trust) services development and management in programmable and open end-to-end 6G systems, supporting cross-platform interoperability, and multi-tenant operation. These methods provide PPDR systems with real-time assessment of component integrity and contextual trustworthiness, enhancing security agility under dynamic conditions. In addition, high-stake applications that require information sharing, such as secure maritime surveillance and decentralized situational awareness, in which responders are dependent upon the accuracy of the data are able to utilize this capability. The value of trustworthiness

and trust is fundamental to achieving the required level of cooperation and data sharing to achieve a successful disaster response.

Privacy-Preserving Techniques and Data Sovereignty

Privacy preservation is addressed through edge-based anonymization, differential privacy, and secure data federation. NANCY applies distributed privacy enforcement to maintain confidentiality in data sharing. Moreover, NANCY uses XAI to provide interpretability into the AI-based decisions, thereby fostering trust and transparency in AI models iTrust6G explores privacy-aware federated analytics for mission-critical PPDR use cases. ADROIT6G integrates secure containers to ensure data locality in multi-tenant environments, and IMAGINE-B5G aligns privacy control with orchestration to meet regional regulatory constraints. MARE integrates federated learning to exchange model parameters among security components that perform inference tasks at the core and RAN parts of beyond 5G networks. Together, these technologies build a privacy-preserving, federated operational model for future PPDR systems that are compliant with data privacy directives for applications such as smart crowd monitoring, as well as complying with frameworks such as the European Health Data Space for applications managing sensitive vital signs, such as real-time telemedicine. These enablers are driven by the values of safety and quality of life.

4.5. DEVICES AND SENSING

Based on the identified critical operational needs for situational awareness that were revealed in section 5, including the inability to see through hazardous conditions and GNSS degraded environments that restrict the ability to track persons and objects, this section investigates the 6G enablers to transform the network into a native sensing environment. Through the integration of ISAC, autonomous power consumption and digital twins, it is ensured that the network will be able to provide the predictive and high-resolution data needed to protect responders and citizens during disruptions to the environment. Ultimately, these 6G device and sensing innovations translate the preparedness-by-design paradigm into a perception-based network architecture that targets to improve quality of life and

well-being.

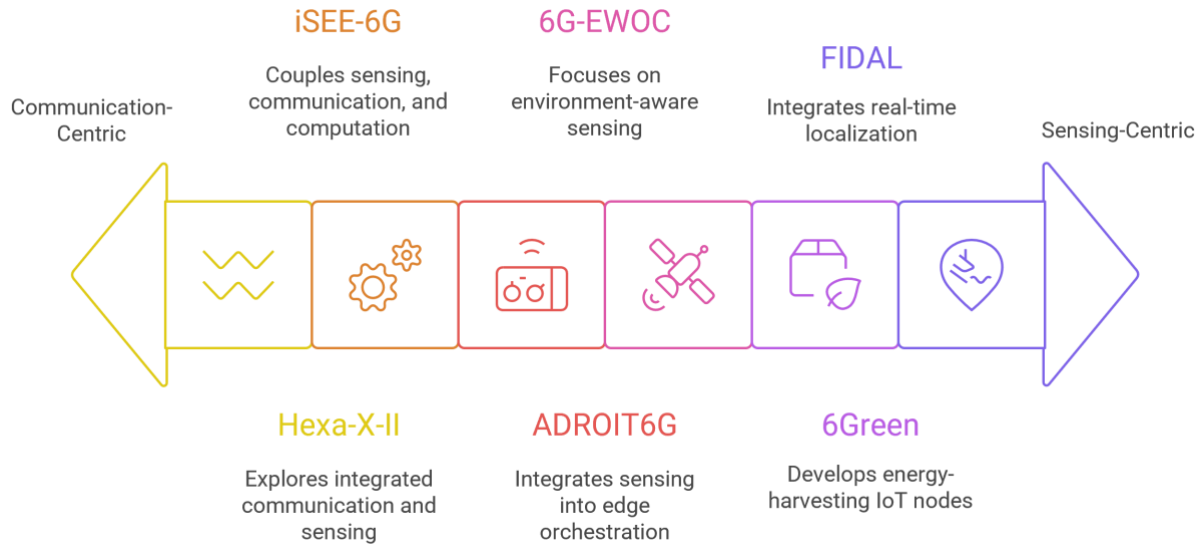


Figure 11 Device and Sensing technologies being addressed in PPDR SNS JU projects

Integrated Sensing and Communication (ISAC)

Integration of sensing and communication enables simultaneous perception and data transfer, crucial for situational awareness in PPDR scenarios. Hexa-X-II explores integrated communication and sensing through radio waveform co-design, enhancing object detection and localization, while it attempts to perform a cross-layer study linking the physical with higher layers of the end-to-end stack, i.e., how application-driven design and intents may introduce certain radio resource management related implications iSEE-6G develops the JCCSP framework coupling sensing, communication, and computation for energy-efficient operation. ADROIT6G integrates sensing into the edge orchestration loop to support adaptive resource allocation. 6G-EWOC focuses on environment-aware sensing for emergency network deployment. These contributions highlight sensing as a native capability of 6G systems rather than an external service. This highlights the importance of ISAC for applications such as smart crowd monitoring and port/infrastructure security, since the detection of crowds and/or unauthorized persons entering secure areas is such a big part of the security process.

Energy-Autonomous and Low-Power Devices

Energy autonomy at the device and sensor level is crucial in PPDR deployments, where recharging or replacement may be infeasible. Projects such as 6Green and iSEE-6G develop energy-harvesting IoT nodes and low-power sensing platforms capable of drawing energy from ambient RF, solar, or kinetic sources. Hexa-X-II examines backscatter communication and ambient RF-based powering for lightweight connected objects, while ADROIT6G applies adaptive power control and local AI inference to optimize device duty cycles. These innovations focus on hardware-level efficiency and self-sustainability, ensuring uninterrupted sensing and communication even in isolated or energy-scarce emergency environments. Driven by the values of environmental sustainability and system resilience,

these technologies ensure that monitoring remains unobstructed during prolonged disasters. In this sense, energy autonomy is not a sustainability feature but a resilience requirement: a sensor that fails during a wildfire because it cannot be recharged has not served its purpose regardless of its technical specification.

Localization, Perception and Digital Twins

Localization and digital twinning play a central role in supporting PPDR decision-making. Hexa-X-II and FIDAL integrate real-time localization and digital twin synchronization into network management, providing visibility across physical and virtual assets. iSEE-6G extends this with semantic data fusion for situational awareness, while ADROIT6G employs digital twins for orchestration testing and predictive optimization. These technologies bridge physical operations and virtual control, improving coordination, planning, and safety. These enablers are driven by the value of trustworthiness, as they ensure the reliability of data that responders depend on for coordination and planning. The impact is a measurable increase in first responder safety, as responders can focus on their core tasks with a higher degree of environmental certainty.

4.6. ENERGY EFFICIENCY AND ENVIRONMENTAL SUSTAINABILITY

This section focuses on energy efficiency and sustainability aspects tied to meeting the requirements for reliable resilient operational continuity. Through AI-based orchestration, sustainable design and adaptive scalability, the situational awareness of first responders is augmented during disaster situations. These enablers are primarily driven by environmental sustainability. The technical shift toward energy autonomy is also a driver for system resilience, ensuring that the network remains unobstructed during blackouts or wildfires.

Figure 12 Environmental sustainability technologies in PPDR SNS JU projects

Energy-Efficient Network Operation

At the system and infrastructure level, energy efficiency is achieved through AI-driven orchestration and adaptive scaling. 6Green develops green orchestration models integrating energy awareness across RAN, transport, and edge domains. Hexa-X-II introduces dynamic topology adaptation and AI-based scheduling to minimize OPEX, power consumption while satisfying the defined SLAs; this is realised by flexible topologies (FlexTop mechanism), which are dynamically adapted based on energy availability, trust levels and incoming application intents. ADROIT6G implements elastic scaling of edge compute resources to prevent idle energy waste, while FIDAL provides cross-domain energy metrics for orchestrators. Moreover, 6G-LEADER aims to control the generation of information and its pertinence to specific goals, leading to a substantial reduction in the volume of data produced and transmitted, thus reducing power consumption and alleviating network congestion. Together, these efforts target network-wide sustainability, balancing resilience and performance under variable operational load.

Green Design and Resource Optimization

Beyond operation, sustainable design includes resource and hardware optimization. 6Green explores life-cycle energy footprint modelling, while Hexa-X-II extends it with design-for-sustainability principles in 6G architectures. IMAGINE-B5G studies efficient resource utilization through adaptive workload placement across federated domains. Regarding energy-aware resource optimization, 6G-LEADER builds several AI/ML-driven xApps to reduce the energy consumption of 6G networks, supporting energy-efficient power control with predictive capabilities and non-orthogonal multiple access. These efforts align 6G technologies with EU environmental goals while ensuring performance and resilience.

Sustainable Architectural Approaches

Sustainability is approached holistically, combining energy, materials, and operational aspects. Hexa-X-II, as the European 6G Flagship defines the primary 6G use cases, the specific sustainability pillars (environmental, social, economic) of each use case, the respective KPIs and KVIs, leading eventually to the end-to-end 6G system blueprint. 6Green introduces end-to-end green-by-design methodologies, ADROIT6G adopts lightweight cloud-native frameworks to minimize infrastructure overhead. iSEE-6G complements these by optimizing communication-computation trade-offs for minimal energy consumption. Then, 6G-LEADER develops a RIS-aided O-RU, exploiting the cost and energy efficiency of RISs, using this technology in the near-field of the base station antenna as an electronically steerable reflectarray for FR1/FR3 operation. Meanwhile, 6G-LEADER will present a conflict management framework where conflicts from diverse intelligent applications (xApps and dApps) will be resolved in a timely manner, thus avoiding performance degradation. Finally, NANCY investigated the use of small/micro base stations to expand the radio coverage, while also reducing the required signal transmission power. These complementary efforts define sustainability as a systemic 6G design principle.

4.7. OPERATIONAL ALIGNMENT

Mapping technologies to use cases

The six technology domains surveyed in this chapter (radio access and connectivity, edge and cloud-native infrastructure, AI/ML-driven management, security and trust, devices and sensing, and energy efficiency) do not function in isolation. Their value for PPDR emerges from how they combine and reinforce one another in service of the operational and societal goals that practitioners and policymakers have articulated.

The most direct expression of this interdependence is in **situational awareness**. ISAC transforms sensing from an external service into a native network capability, enabling simultaneous perception and data transfer at the radio layer. UAV-assisted platforms extend this capacity into environments where fixed infrastructure is absent or damaged, providing real-time video, environmental mapping, and localised computation. NTN architectures, particularly through frameworks such as JCCSP, extend the sensing envelope further, incorporating satellite layers into a unified perception system. These inputs only become operationally useful when processed in real time. Edge continuum and MEC integration provide the low-latency inference needed for real-time decision support, while semantic and knowledge-based management transitions the network from purely data-driven to context-aware, interpreting environmental inputs rather than merely transmitting them. Digital twins and advanced localisation close the loop, providing responders with coherent visibility across physical and virtual assets, including in GNSS-degraded or smoke-obscured environments where conventional positioning fails.

Managing emergencies and large-scale events places greatest demand on the coordination layer of the technology stack. Multi-connectivity, particularly seamless TN-NTN handover, ensures that data paths are maintained as responders move through degraded environments. Closed-loop intelligence and intent-based orchestration translate high-level mission objectives into autonomous network reconfiguration, reducing the burden on operators at exactly the moment when cognitive load is highest. UAV platforms serve here not only as connectivity relays but as compute-augmented agents supporting XR interactions for tactical coordination. MEC provides the deterministic performance needed when multiple agencies are sharing data simultaneously, while semantic management enables intelligent adaptation as the incident evolves. Energy-efficient network operations also play a role in sustained large-scale events, where network congestion from dense deployments and high data volumes must be managed without compromising priority services.

For **critical communications and infrastructure protection**, the technology stack converges on the need for continuity and verifiability. NTN architectures and UAV-assisted communications together ensure data flow persists when terrestrial infrastructure is compromised. ISAC enables intrusion detection and environmental monitoring as a native function of the network rather than requiring separate sensor overlays. Multi-connectivity provides the assured, redundant data paths that mission-critical information requires. At the security layer, zero-trust architectures provide continuous verification against the expanded attack surface that cloud-native and virtualised deployments introduce, a risk explicitly identified in both the NIS2 Directive and by practitioners as a consequence of the

shift away from monolithic systems. Digital twins provide virtual representations of infrastructure assets that support both planning and real-time coordination.

Network reliability and performance is where the architecture as a whole is stress-tested. NTN integration and multi-connectivity provide the redundant communication layer that ensures connectivity when terrestrial nodes are damaged or overloaded. Resilience-aware RAN slicing ensures that critical services are protected even during partial network failures, which is a direct expression of the Cyber Resilience Act's security-by-design principle at the network layer. Mobility-aware edge clusters provide deterministic performance under extreme operational conditions. AI-driven closed-loop intelligence enables autonomous self-optimisation and self-healing, while zero-trust architectures maintain secure multi-domain operation throughout. Energy-efficient scheduling ensures that networks can sustain operations during prolonged disasters, including scenarios, such as blackouts or wildfires, where power supply to infrastructure nodes may itself be disrupted.

Gaps and future directions

Several technology directions already present in the portfolio become more strategically important as demands on 6G PPDR systems grow. Investment in hybrid TN-NTN architectures, resilience-aware RAN slicing, and zero-trust security frameworks directly serves requirements for seamless availability, continuous coverage, and security-by-design. The portfolio's treatment of energy autonomy as an operational resilience requirement, rather than a parallel sustainability objective, is a strength worth preserving: a network node that exhausts its power after an earthquake, or devices whose battery life does not match responders' shifts, has not served its purpose regardless of technical specification. The portfolio is also seeing success where projects link technical KPIs to operational outcomes such as situational awareness continuity, strengthening both the realism of the work and its readiness for adoption.

The following directions identify where further work would most strengthen the portfolio's capacity to deliver the societal outcomes the practitioner and policy frame demands.

Testing and validation in operationally representative conditions is a precondition for robustness. PPDR environments are defined by precisely the conditions that controlled testbeds cannot replicate: damaged infrastructure, degraded environments, and active interference. Fundamental vulnerabilities arise not from any single failure but from the absence of graceful degradation. Testing must move toward the PACE framework (Primary, Alternate, Contingency, Emergency) not as a checklist but as an architectural principle: the goal is a connectivity fabric with no single point of failure, where each layer of the TN-NTN stack, from terrestrial RAN through non-terrestrial and device-to-device mesh, provides a fallback when the layer above it fails, and transitions between layers are seamless rather than disruptive. This is of particular importance as 6G adopts AI: models and sensing systems that perform well in controlled environments can fail in the field, and validation methodologies need to reflect the complexity of real incidents.

Pan-European interoperability requires multi-operator orchestration, spectrum sharing, and NTN integration to function together across heterogeneous devices, different regulatory

environments, and network infrastructures not designed with interoperability as a founding requirement. This is where the most consequential open problems sit, and where progress would most directly advance the EUCCS ambition. The technical foundations are being developed; the priority now is ensuring they are validated in conditions that reflect operational reality, and connected to the EUCCS programme and relevant standardisation processes.

Remote expert guidance and role-differentiated interfaces represent a distinct PPDR strategic goal the portfolio has not yet treated as a technical capability in its own right. Extending specialist expertise to the point of need requires specific requirements for latency, reliability, interface design, and the trust properties that make remote input actionable under stress. Field operators need simple hands-free interfaces; tactical officers need tablet-level awareness; strategic commanders need full data access, all on a shared underlying platform.

Security gaps in two high-criticality areas warrant dedicated focus. Post-quantum cryptography is highly important but low readiness. Device-to-device and mesh connectivity, enabling responders to communicate when all fixed infrastructure has failed, is similarly high criticality and low readiness. These represent a resilience gap the portfolio needs to engaged with. Supply chain trustworthiness should also be treated as a design consideration: systems whose critical components depend on supply chains outside European control introduce vulnerabilities that technical security measures alone cannot address.

Equity and accessibility should be explicit design constraints. Systems that are unaffordable or impractical for smaller agencies or remote deployments are not fulfilling the safety mandate that motivates their development. Total cost of ownership, algorithmic fairness, graceful degradation, and low-bandwidth resilience should be standard measures of performance alongside technical KPIs.

Governance and accountability must develop alongside technical capability. The EU AI Act's classification of emergency dispatch, resource prioritisation, and signal optimisation as high-risk applications establishes clear requirements for human oversight, interpretable outputs, and documented responsibility chains. Practitioners draw a clear distinction between AI for situational awareness, where readiness is moderate, and AI for network management, where readiness is low. Designing for these requirements from the outset is both a compliance necessity and an operational one.

5. MAIN CHALLENGES AND ENVISIONED SOLUTIONS

The technologies surveyed in Chapter 4 represent a substantial and growing body of capabilities that, in combination, address the most demanding requirements that PPDR practitioners and policymakers have articulated: connectivity that survives infrastructure loss, situational awareness that functions in degraded environments, coordination that scales across agencies and borders, and security that holds under active threat. The challenges here are what the research has discovered in the process: the limits of current validation approaches, the integration complexity that emerges when capable components meet heterogeneous real-world infrastructure, the governance questions that autonomous systems raise in life-critical contexts, and the distance between what performs well in a testbed and what can be trusted in the field.

Section 5.1 maps these challenges by domain, grounded in what SNS-JU projects have found as they have pushed toward deployment. Section 5.2 identifies where continued investment would most strengthen the portfolio's capacity to deliver on its operational ambition. Section 5.3 considers the methodological, governance, and strategic orientations that will determine whether the portfolio's technical achievements translate into real-world impact for responders, for communities, and for the European safety infrastructure.

5.1. CHALLENGES

This section introduces key challenges in the PPDR operations field to which SNS JU projects may notably contribute. They are each described along with a brief introduction on how active and past SNS-JU projects may impact on sorting them out.

Guaranteeing Services Continuity in Crises: NTN and Unmanned Aerial Vehicles

First responders operating in disaster zones, remote terrain, or maritime environments cannot wait for fixed infrastructure to be restored. The challenge driving work on NTN and UAV-assisted networks is fundamentally operational: how to ensure that a responder in a collapsed building, on a flood-plain, or beyond coastal coverage can communicate, be located, and receive support without depending on the infrastructure that the disaster may have destroyed.

Taking these concepts from design into deployment exposes where the real complexity lies and where PPDR research still has ground to cover. Across the portfolio, projects are addressing several high-stakes technical hurdles that go beyond the scope of controlled testing. A central focus here is achieving seamless handovers between terrestrial and non-terrestrial nodes under real-world mobility, damages, or congestion, with work ongoing to maintain service continuity as conditions shift. Extending indoor coverage and link capacity

through aerial or satellite nodes brings its own complications. So, too, does the complexity of managing handovers between terrestrial and non-terrestrial nodes without service interruption (ref->6G-NTN). Moreover, the challenge of guaranteeing strict Quality of Service (QoS) and low latency for mission-critical applications (e.g., real-time video, MCPTT) amidst a shared network environment (spectrum coexistence) pose hurdles for rapid deployment.

In this domain, various SNS-JU projects have underlined interoperability and performance challenges. More specifically, trials involving aerial and autonomous systems often face limitations in terms of synchronisation, mobility handling, and backhaul reliability. For instance, iSEE-6G highlights the difficulty of coordinating distributed RUs with UAV nodes in cell-free architectures, requiring microsecond-level timing accuracy and efficient mitigation of Doppler shifts at speeds approaching 100 km/h. Furthermore, field pilots in TRIALSNET and FOR-5G demonstrate that uplink throughput and varying wireless conditions impose constraints on real-time LiDAR, 4K video, and multimodal sensing streams, being more pronounced during autonomous navigation in crowded or obstructed environments.

Also, integration challenges emerge from form-factor, power, and RF constraints. Here, projects such as 5G-FIRE and FIRESCAN show that the integration of 5G modems and multi-antenna modules into small portable enclosures at the UAVs is non-trivial, impacting thermal behaviour, flight stability, and connectivity. In maritime and remote settings ABYSS-5G reports that 5G coverage quality over water is highly affected in distances beyond 2 km from shore, requiring redundancy in the form of other RF or satellite links. Additional challenges have been noted in MARE, related to the provision of secure, low-latency synergies across terrestrial and NTN deployments, as mobility and varying trust levels can threaten coordinated protection and threat detection.

At an architectural level, NTN adoption has several challenges to address. Projects, such as AMAZING-6G, 5G-STARDUST, 6G-NTN, and UNITY-6G stress that integrated terrestrial and non-terrestrial systems, including satellite backhaul for mobile cells, have to deal with standardisation, synchronisation, and reliability issues. These challenges indicate that although the use of UAVs and NTNs is highly beneficial for coverage and reliability in PPDR operations, novel methods for robust synchronisation, interference management, spectrum access, and hybrid terrestrial–non-terrestrial continuity are needed.

Coordinating Multi-Agency Resource Use

When multiple agencies converge on a major incident, each with different data needs, different security requirements, and different tolerances for delay, the network must serve all of them simultaneously without allowing any one to degrade another and while still allowing the public to reach emergency services or family. Network slicing is the technical response to this coordination challenge, but implementing it in conditions of shared, compromised, and mobile infrastructure reveals how far the gap remains between laboratory capability and operational deployment.

Maintaining end-to-end slice isolation across mixed and degraded infrastructure is a real challenge in operational settings. When resource demand spikes unexpectedly, it creates contention with existing traffic. Current contingency models are not always equipped to

handle it. The findings below identify the performance boundaries where architectural intent and operational reality are still being aligned.

Projects like FIDAL and TrialsNet are investigating dynamic prioritization and orchestration validating automated slice lifecycle management in large-scale field trials. They utilise AI-driven orchestration to dynamically reallocate radio and core resources to the PPDR slice in real-time, effectively pre-empting commercial traffic during emergencies to guarantee low latency for Mission Critical Video (MCVideo) and Push-to-Talk (MCPTT).

On the other hand, other projects (like RIGOUROUS and NATWORK) address the security risks of shared infrastructure. They propose Zero-Touch Network & Service Management frameworks to autonomously detect anomalies within a slice. Under this approach, if a public slice is attacked (e.g., DDoS), the system logically isolates it, ensuring that the trustworthiness and performance of the parallel Emergency Response slice remain unaffected.

Extending slices to non-terrestrial domains is a key research area. 6G-NTN, FLECON-6G and iSEE-6G are working on architectural frameworks that allow a network slice to seamlessly span terrestrial base stations, satellites, and UAVs. This would ensure that the Emergency Slice follows first responders into remote or disconnected areas without dropping the session, a capability known as slice mobility. Furthermore, the physical constraints of deployment create severe resource contention issues. As demonstrated in AMAZING-6G, PPDR teams often rely on portable edge cores powered by vehicle batteries. The challenge lies in maintaining strict resource isolation and slice availability while the hardware is mobile and power-constrained. One technical solution involves optimizing Virtual Network Functions (VNFs) for lightweight edge environments and implementing robust slice-level orchestration that can handle intermittent connectivity without dropping critical sessions. This is further complicated in maritime and aerial scenarios; trials in ADAPT-G and RESCUE-5G indicate that slices for UAVs and USVs (Unmanned Surface Vehicles) require continuous adaptation to cope with fluctuating link quality and load variations. The solution here points toward AI-driven dynamic reconfiguration, which autonomously adjusts slice parameters in real-time to maintain service level agreements (SLAs).

A primary technical hurdle, identified in Project Critical and corroborated by recent research on multi-modal emergency communications, is the simultaneous management of conflicting Quality of Service (QoS) requirements within a single operational theatre. Emergency scenarios require dual-stream QoS: high-bandwidth Enhanced Mobile Broadband (eMBB) for real-time video surveillance and Ultra-Reliable Low Latency Communications (URLLC) for vital-sign telemetry. Technical solutions being explored to address this issue involve advanced traffic steering mechanisms and specific APN (Access Point Name) configurations that can dynamically negotiate WebRTC codecs, aiming to ensure that bandwidth-heavy video does not choke latency-sensitive telemetry.

The integration of the Edge-Cloud continuum in the context of the PPDR slice is also being investigated (6G-PATH and AMAZING-6G). The main concept resides on including dedicated edge computing resources for immediate data processing (e.g., AI analysis of drone footage) with the aim of ensuring that the slice can provide a complete, secure

operational environment rather than just a data pipe. The complexity of multi-agency responses is also pointing towards the need for cross-domain slicing. Projects like 6G-PATH and RIGOUROUS highlight that a slice cannot simply exist within one carrier's core; it must span the entire IoT–edge–cloud continuum and traverse multiple operators. Since this capability is beyond current 5G SA standards, technical efforts are focusing on ZSM and federated orchestration frameworks as potential approaches. These are being explored for their potential to allow different agencies to securely interconnect their slices on demand, with the goal of guaranteeing that priority traffic is recognized and preserved end-to-end, a critical capability that early testbeds struggled to provide.

Maintaining Security and Privacy in Crises

Security and privacy challenges are deeply intertwined with PPDR operations, affecting both architectural decisions and deployment feasibility. PPDR operations handle some of the most sensitive data in society, biometric information, location data, operational plans, and vital signs, often across agency boundaries, on infrastructure that may be partially untrusted, and under time pressure that makes manual security management impossible. The security challenges in this domain are not only technical; they reflect the fundamental tension between the openness that cross-agency coordination requires and the protection that mission-critical and privacy-sensitive data demands.

The expanded attack surface that cloud-native and virtualised deployments introduce, already identified in Chapter 4, creates a set of challenges that the portfolio is actively working to resolve but has not yet closed. Three in particular cut across multiple projects and use cases.

Dynamic trust modelling at operational speed remains an open problem. When foreign aid agencies or ad-hoc volunteer networks must connect instantly during a disaster, establishing whether incoming devices and applications can safely share data and systems, fast enough to be operationally useful, is still an open challenge. Projects like iTrust6G and SAFE-6G are making progress, developing ways to continuously calculate scores based on device behaviour, location, and software integrity and revoking access when anomalies are detected. But the latency and computational overhead of doing this at scale under crisis conditions is not yet resolved.

Processing sensitive data, such as facial recognition for missing persons or vital sign analysis, on physically exposed edge nodes that may belong to untrusted third parties remains a vulnerability that hardware-enforced enclaves alone do not fully resolve. CONFIDENTIAL6G and HORSE are demonstrating that Trusted Execution Environments can keep data encrypted within the CPU's memory even under physical compromise, but deployment at the scale and heterogeneity of a real PPDR operation, across hardware from multiple vendors in ad-hoc environments, introduces integration complexity that controlled trials have not yet been fully stress-tested.

Additionally, emergency networks are prime targets for Distributed Denial of Service (DDoS) attacks or jamming that aims to disrupt coordination during a crisis. Static firewalls are too slow to adapt to massive, AI-generated attack traffic. The SNS-JU projects are addressing

the challenges in various ways. NATWORK proposes a bio-inspired cyber-resilience framework. Mimicking a biological immune system, the network uses lightweight AI agents distributed across the infrastructure to detect pathogens (anomalous traffic patterns), and autonomously reconfigure the network topology to heal itself. Similarly, RIGOUROUS focuses on Zero-Touch Security Management, where the network detects intrusion attempts and automatically deploys countermeasures (like isolating a compromised slice) without waiting for a human operator.

PPDR traffic often shares physical infrastructure with public civilian traffic. Several risks may apply, e.g., the risk of side-channel attacks, where an attacker on the public slice analyses traffic patterns to deduce police movements or sensitive operational data. SNS-JU projects like PRIVATEER and FIDAL are validating Privacy-Aware Slicing. In the FIDAL trials, the project demonstrated strictly isolated slices where the PPDR traffic is logically invisible to other users. PRIVATEER adds a layer of privacy by utilizing decentralized analytics, ensuring that metadata from the emergency slice is never exposed to the central orchestrator in a way that could reveal user identities.

Moreover, TRIALSNET emphasise the practical implications of GDPR, including video analytics in public spaces requiring anonymisation, strict access control, and secure transport channels (e.g., private APNs, VPNs), increasing system complexity and latency. Health-oriented pilots like Project Critical pinpoint the regulatory burden when handling mixed media, comprising vital signals and video in the context of recent frameworks, such as the European Health Data Space (EHDS). MARE mentions the limited maturity of 6G security specifications, particularly for programmable security functions, exposure controls, and cross-domain orchestration as relevant challenges.

Additional challenges stem from architectures integrating advanced security mechanisms. NANCY introduces blockchain capabilities to the RAN with PQC and QKD-based security mechanisms, demonstrating strong trust guarantees, while revealing that consensus and quantum-safe processes increase latency, being potentially unsuitable for delay-sensitive mission-critical flows. Additionally, 5G-FIRE and SAFERFLOW report privacy-by-design constraints around real-time video and biosensor data, necessitating careful camera orientation, encryption, and retention policies.

Another concern corresponds to trustworthy operation under unreliable connectivity. Here, 6G-PATH and 6G-LEADER note that AI-driven RAN control and advanced features should be enhanced with novel mechanisms, preserving service levels even during partial outages or link degradation. Maritime trials from ABYSS-5G focus on secure storage and rapid deletion of collected media, satisfying operational privacy in civilian settings. Next, projects working on orchestration aspects, such as RIGOUROUS indicate that harmonised security and privacy policies across multiple PPDR entities increases operational and computational complexity and may result in performance degradation.

Building AI Systems Responders Can Trust

The promise of AI in emergency networks is that the network can do the work of managing itself, freeing responders to focus on their mission rather than their tools. The challenge is

that AI models trained in stable environments encounter exactly the conditions they were not trained for when deployed in a real crisis: smoke, interference, physical destruction, inconsistent data, and behaviour that no dataset anticipated. Making AI-native RAN reliable enough to be trusted in mission-critical operations is as much a question of validation methodology and human oversight as it is of model architecture.

AI models trained in static environments suffer from model drift when deployed in chaotic disaster zones, producing suboptimal reconfiguration or outright network failure under conditions no training dataset anticipated. Projects like 6G-NTN and AMAZING-6G have found that executing heavy AI inference tasks on battery-powered UAVs or portable public safety cells depletes energy reserves intended for mission duration, a direct conflict between AI capability and mission duration. Projects exploring advanced RAN functions, such as iSEE-6G and 6G-LEADER, also noted challenges related to synchronisation accuracy, fronthaul variability, and the difficulty of validating AI-enabled control loops under imperfect field conditions. Distributed and federated architectures, including federated learning approaches that adapt models locally without centralising sensitive data, AI-native air interfaces, and adaptive physical layer reconfiguration are the broad directions projects are pursuing in response, each addressing a distinct failure mode and each carrying its own unresolved demands around interpretability, portability, and operational trust.

The introduction of AI/ML into mission-critical communications also creates new reliability, explainability, and operational safety challenges that are still being worked through. 6G-LEADER highlights the need to go beyond current O-RAN capabilities in terms of closed-control loop. In this sense, semantic communication and AirComp mechanisms require new interfaces, new PHY/MAC support, and highly synchronised distributed operations, designed to be resilient under PPDR scenarios. 6G-LEADER also highlights that traditional throughput-maximization algorithms deplete the battery life of portable PPDR nodes and saturate limited backhaul links. In response, the project is investigating the concept of Goal-Driven RAN as a potential alternative approach. Additionally, 6G-LEADER's work on Predictive PHY explores the use of AI to forecast channel degradation milliseconds in advance, with the aim of enabling proactive handover and parameter adjustment that could prove vital for high-speed UAVs operating in the FR1/FR3 bands. MARE reports that 3GPP and O-RAN standards do not yet fully address AI-assisted automation, especially in deployments integrating NTNs and cloud-continuum environments, a gap that the research community is actively working to inform.

FIDAL and TrialsNet are demonstrating AI-driven Zero-Touch Automation in their field trials. By integrating O-RAN compliant Intelligent Controllers (RICs), these projects are exploring how the network might autonomously reconfigure slicing parameters in milliseconds, detecting a sudden influx of first responders (e.g., during a fire event) and dynamically expanding their slice capacity before congestion occurs.

To address SWaP constraints on aerial platforms, 6G-NTN is proposing lightweight, predictive AI models specifically designed for NTN nodes. These aim to forecast connectivity gaps based on satellite/UAV trajectories, potentially allowing the network to proactively hand over sessions between terrestrial and non-terrestrial layers to maintain connectivity for critical services like Mission Critical Push-to-Talk (MCPTT).

In perception-oriented systems, a major issue involves model generalisation to extreme environments. 5G-FIRE and FOR-5G have found that models trained in controlled conditions often misinterpret smoke, lighting, or dynamic crisis scenes. Meanwhile, SaferFlow has reported false positives in water detection due to environmental interference. NANCY and iSEE-6G underline the difficulty of maintaining prediction accuracy when models experience unseen traffic conditions or highly dynamic UAV mobility, particularly given constraints on training data and intermittent backhaul.

Safety concerns also arise from AI opacity, with projects such as RIGOUROUS reporting that black-box models, adversarial vulnerabilities, and latency overheads undermine the confidence of operators in AI systems deployed in PPDR use cases. Overall, AI-native PPDR networks must balance model complexity, explainability, energy consumption, and real-time responsiveness. The work surveyed here represents meaningful progress toward this balance, while making clear how much remains to be resolved before these capabilities can be fully trusted in mission-critical operations.

Edge Solutions in Chaotic Environments

Processing data close to the point of need is essential when connectivity is unreliable, latency is critical, and the volume of sensor, video, and telemetry data generated by a modern PPDR operation would overwhelm any centralised system. But edge computing in PPDR contexts means deploying compute capability in environments that are power-constrained, physically exposed, and operationally chaotic, conditions that expose the limits of solutions designed for stable data centre environments.

Edge computing offers significant potential for PPDR responsiveness but raises its own challenges in terms of performance, orchestration, security, and energy requirements. High-rate analytics on mobile robots in TRIALSNET have revealed that GPUs and on-board computing are major energy drains, constraining mission duration. Similar constraints have emerged in FOR-5G, where private 5G deployments are finding that they require dynamic resource management to avoid contention between critical and non-critical services.

Portable edge nodes in AMAZING-6G have illustrated the limitations of battery-powered edge cores: running MCX services, AI inference, and core VNFs simultaneously has yielded an autonomy of approximately six hours before recharging is required, a significant constraint in multi-day disaster response operations. 5G-FIRE has found that edge boxes operating on uncompressed video streams experience CPU saturation and synchronisation mismatches, pointing to the need for optimisation and priority-based scheduling. SaferFlow has provided early evidence that integrating renewable power (solar-assisted) has potential to improve resilience, though this requires validation across varied environments before its reliability can be confirmed.

Edge systems may serve as the proper infrastructure for attackers to threaten the system. The power and computing limitations inherit to edge devices, makes impossible to deploy traditional highly complex solutions for security provisioning. The MARE project analyses that scenario considering as an illustrative context several UEs at the edge initiating a simultaneous attack to the network. The proposed solution resides on a proactive approach

where specific security functions are ad-hoc and dynamically created to protect the network. The software-based strategy envisioned in MARE, would be extremely helpful in PPDR contexts, as it would support a completely customized solution suiting the expected needs the best.

In terms of architecture, multi-domain Edge-Cloud systems explored in RIGOUROUS and distributed O-RAN deployments investigated in 6G-LEADER are finding that the efficient orchestration of compute, AI, and resource management tasks across heterogeneous infrastructures remains an open challenge. Meanwhile, device-level limitations, such as thermal load, BLE reliability, and app-level routing, have emerged as critical issues in the work of Project Critical. Equally, 6G-LEADER and NANCY are finding that semantic communication and AirComp-based aggregation require highly structured sensing data and robust channel knowledge, and that real-world uncertainties can significantly degrade performance in ways that controlled testing does not always anticipate.

Moving ISAC to Active Response

Situational awareness in a disaster zone depends on knowing where things are, what is happening, and how conditions are changing, often in environments where conventional sensors cannot be deployed and GPS cannot be trusted. Integrated Sensing and Communications (ISAC) offers a promising response to this challenge by making the communication network itself a sensing system, but moving from this concept to a deployable capability that functions under the interference, mobility, and time pressure of a real incident, involves challenges that cut across standardisation, spectrum management, and the integration of sensing into operational workflows.

ISAC is fundamentally evolving into Joint Communication, Computation, Sensing, and Power transfer (JCCSP). It has the potential to transform PPDR by turning the communication network itself into a high-precision sensor. This unified paradigm aims to enable the simultaneous transmission of critical data and real-time environmental monitoring, which could prove essential for establishing situational awareness in dynamic and cluttered disaster zones where traditional infrastructure may be compromised. By reusing existing hardware and spectrum, ISAC offers the prospect of cost-effective, ubiquitous perceptive mobile networks capable of detecting passive objects, such as non-collaborative drones or survivors, without requiring them to carry active devices.

In mission-critical scenarios, ISAC is being explored for its potential to enhance operational reliability through several key capabilities, spanning unified air interfaces that survive infrastructure loss, slice mobility that follows responders across operational and geographic boundaries, and aerial platforms that function as compute-augmented sensing agents. Each addresses a distinct layer of the continuity problem and each brings its own unresolved demands.

If these capabilities can be realised at operational scale, emergency networks could become no longer just passive conduits for data but active, intelligent participants capable of seeing and adapting to the disaster landscape in ways that could fundamentally change how first responders understand and navigate crisis environments.

PPDR scenarios increasingly point to the need for joint communication-sensing systems, and SNS-JU projects are beginning to reveal the gap between conceptual designs and deployable solutions that must be closed. iSEE-6G has found that advanced JCCSP/ISAC waveforms are not yet standardised, require SDR implementations, and introduce stringent requirements for timing, spectrum management, and synchronisation between RUs and UAVs. Current results suggest that achieving sub-metre sensing accuracy alongside throughput above 1 Gbps, remains feasible only in controlled environments, and that translating this into field-deployable capability is a significant open challenge.

Large-volume sensing applications explored in TRIALSNET, 5G-FIRE, SaferFlow, and FOR-5G have revealed that integrated sensing demands stable uplink rates, end-to-end time alignment, and resilience during mobility or network congestion. The absence of prioritised ISAC support in current testbeds is often forcing compromises in sensing resolution or update rates, underscoring the need for standardisation work that keeps pace with the research.

The Gap Between the Lab and the Field

The most consequential challenge faced by the current portfolio may not be technical at all. It results from the gap between what can be demonstrated in a testbed, and what can be trusted in the field. Validating systems for PPDR use means testing them in conditions that are ethically and logistically difficult to replicate: chaotic environments, multi-agency command structures, degraded infrastructure, and the unpredictable behaviour of people under stress. How projects close this gap will determine whether technically impressive results translate into systems that responders will actually use.

Across projects, the transition from controlled lab setups to real-world PPDR environments is revealing significant gaps. Many projects observed that moving from laboratory conditions to real PPDR-like field environments introduces severe variability. TRIALSNET, FOR-5G, 5G-FIRE, SaferFlow, and ABYSS-5G reported fluctuating radio conditions, uneven coverage, weather effects, interference, and mobility-induced degradation. Integration of heterogeneous components, such as UAVs, USVs, sensors, robots, and edge nodes proved challenging in TRIALSNET, FIRESCAN, NANCY, and RIGOUROUS.

Experimentation and validation for PPDR and MCX face the fundamental challenge of replicating extreme, chaotic operational environments within controlled testbeds. Large-scale trial projects like FIDAL and TRIALSNET have highlighted the difficulty of validating SLAs for critical slices when field trials cannot ethically or logistically interfere with actual live emergency networks. Consequently, validation is often relying on Digital Twins or isolated sandbox environments (as seen in 6G-SANDBOX), which are struggling to accurately model the stochastic behaviour of panic-driven human crowds or the physical destruction of infrastructure found in real disasters. TRIALSNET trials have shown that interference, mobility, and unpredictable human or environmental behaviour significantly affect system stability in ways that pre-trial testing did not anticipate.

From a technical perspective, the integration of novel 6G enablers into legacy-constrained hardware is posing a severe validation hurdle. Testbeds often lack full slice availability or

NTN integration, as observed in FIRESCAN and 6G-NTN, limiting the practical scope of mission-critical benchmarking. iSEE-6G is developing a PoC that will include UAV support for PPDR services but acknowledges it will not be able to emulate a real-world crisis scenario at this stage due to relatively low TRL. iSEE-6G and 6G-LEADER have detailed the complexity of evaluating predictive, self-adaptive PHY and Goal-Driven RAN solutions; since fully compliant 6G hardware does not yet exist, these projects are employing hybrid methodologies combining simulations with partial hardware PoCs that emulate emergency response networks during crisis as the closest currently achievable approximation. AMAZING-6G, ABYSS-5G, and FOR-5G have reported that terrain, maritime conditions, and weather severely impact link quality and autonomous system performance in ways that substantially complicate validation.

Many projects, including FOR-5G and iSEE-6G, are emphasising that KPIs evaluated in testbeds cannot model time volatility where smoke, occlusions, shifting topologies, or sudden load increases distort sensing and networking assumptions. RIGOUROUS has highlighted the need for cross-domain security and slice management validation under realistic loads, an aspect rarely addressed in conventional testbeds. Cross-domain orchestration and interoperability are remaining significant barriers for validating end-to-end MCX chains. 6G-PATH and FLECON-6G have emphasised that valid pilots must span the device-edge-cloud continuum across multiple administrative domains, for example a police drone connecting to a fire department's private 5G bubble. Current validation frameworks are often lacking the multi-stakeholder governance models required to test these handover scenarios legally and technically, which is leading to siloed experiments that fail to capture the complexity of multi-agency emergency response and pointing to a need for shared validation infrastructure and governance frameworks that the community has not yet collectively built.

Stakeholder and regulatory related issues were also significant. UAV/USV operations near airports or ports required complex approvals in ADAPT-G, RESCUE-5G, SaferFlow, and ABYSS-5G. Privacy and GDPR compliance shaped data-collection strategies in TRIALSNET, Project Critical, and other video-centred pilots. Trust and usability were also recurring themes. Several projects found that responders preferred simpler, more ergonomic devices (e.g., bodycams instead of tablets) and needed clearer explanations of AI-based decisions.

5.2. DIRECTIONS IN SOLUTIONS

Across the SNS-JU portfolio, four broad directions are emerging where technically promising capabilities have not yet reached the robustness, robustness, interoperability, or operational trustworthiness that PPDR deployment requires. Progress in each area is increasingly interdependent: deployable connectivity without intelligent control is difficult to manage under stress; security without interoperability creates silos; and sensing without communication is operationally blind. The directions below identify where the most consequential open problems sit.

Keeping responders connected when infrastructure fails

When infrastructure fails in disaster zones, the most immediate requirement is connectivity that operates independently of the local conditions. Multi-layered space-air-ground architectures address this principle, but several gaps remain between current demonstrations and field-trustworthy systems.

- Unified Air Interfaces: Unified, data-driven air interfaces allowing imperceptible switching between terrestrial towers, Low Earth Orbit (LEO) satellites, and UAV-mounted base stations to ensure unbroken connectivity. exist as proof-of-concepts in projects like 6G-NTN and 5G-STARDUST. Advancing these from controlled demonstrations to systems that sustain performance under the mobility, interference, and link variability of a real incident is the open challenge.
- Portable Edge Cores: AMAZING-6G has demonstrated the potential of portable edge cores, powered by vehicle batteries, that employ optimised Virtual Network Functions (VNFs) for lightweight edge environments, even if still constrained. Extending energy autonomy, reducing overhead, and validating performance under the physical stress of field deployment are priorities.
- Slice Mobility: Architectural frameworks for slices that span terrestrial, satellite, and UAV layers are under development in 6G-NTN, FLECON-6G, and iSEE-6G. But slice mobility remains technically and legally unresolved across two important dimensions: geographical, such as a cross-border unit roaming between national infrastructures, and operational, such as a fire drone attempting to use a private 5G network deployed by a police service.

Bridging Intelligence and Reliability

As more agencies and data streams converge on an incident, the research direction points toward AI-native control that handles network complexity autonomously and reduces the burden on operators. The capabilities below are progressing but have not yet been validated under the conditions that determine whether they can be trusted in practice.

- Zero-Touch Automation: O-RAN compliant RIC-based automation is showing promising results in FIDAL and TRIALSNET field trials, but current demonstrations rely on scenarios that do not fully replicate the unpredictability of real incidents, sudden multi-agency convergence, degraded connections, or competing priority signals. Validation under these conditions, and the governance frameworks that determine who is accountable when autonomous reconfiguration affects mission-critical outcomes, need to be considered going forwards.
- Goal-Driven RAN: The concept of RAN that prioritises operational outcomes over raw throughput, explored in 6G-LEADER, addresses a genuine PPDR need of for increased device battery life. The approach is at early conceptual and simulation stage; establishing what goal-driven means across heterogeneous multi-agency operations, and how competing goals are arbitrated, is work that remains ahead.

- Predictive PHY: While AI-based forecasting of channel degradation offers a path toward proactive network management, disaster deployments introduce extreme variables like physical infrastructure destruction and high-velocity mobility. Building on the foundation of simulations and PoCs in 6G-LEADER and iSEE-6G, the next research phase must enhance model generalisability. The goal is to ensure predictive robustness in operational mobility: when operating across unfamiliar network infrastructures, disparate operators, and the heterogeneous regulatory and stressed environments unique to each disaster.
- Distributed Intelligence: The work conducted in NATWORK and 6G-SANDBOX has validated the functional feasibility of federated AI for PPDR, specifically in managing model adaptation without saturating backhaul or compromising data security. With this baseline established, the research trajectory is now focusing on ensuring that locally adapted models remain coherent across a multi-agency operation where different nodes are learning from different environments simultaneously.

Security for Dynamic Multi-Agency Operations

In multi-agency operations, trust is the foundation of coordination. The capabilities below are each necessary for PPDR security as it moves beyond traditional perimeter defence to address the risks of dynamic, multi-agency operations.

- Zero-Trust Architecture: Dynamic trust modelling is progressing in projects like iTrust6G and SAFE-6G. The next step is to do so at scale: to consider the implications of continuously recalculating trust scores across all devices, including ad-hoc device onboarding, in a large-scale multi-agency deployment within mission-critical timing requirements.
- Bio-Inspired Resilience: NATWORK's distributed AI agent framework is a conceptually strong response to the speed at which AI-generated attack traffic can overwhelm static defences. The next step would be to give dedicated research attention to whether that speed of autonomous response remains correct under the combined stress of physical infrastructure damage and simultaneous cyber-attack, when PPDR and civilian traffic share the same degraded physical layer.
- Confidential Computing: Having validated Trusted Execution Environments for protecting data-in-use on physically exposed edge nodes at the component level within CONFIDENTIAL6G and HORSE, the next phase should focus on extending these protections across the heterogeneous heterogeneity of PPDR operations, across hardware from multiple vendors and in ad-hoc environments not preconfigured for secure enclave operation. Exploring this would help bridge between localised security and system-wide interoperability.
- Privacy-Aware Slicing: Privacy-aware slice isolation and decentralised metadata protection have been demonstrated in FIDAL and PRIVATEER. The next research direction is reconciling privacy-by-design with interoperability-by-design, where cross-border PPDR coordination requires data to flow between countries. This is a space where technical and policy research need to advance together.

- Cross-Boundary Security: Work across NANCY, RIGOUROUS, FIRESCAN, and 6G-PATH on secure data sharing, legacy integration, and multi-agency interoperability, extended by 5G-STARDUST, 6G-NTN, and UNITY-6G into non-terrestrial domains, collectively points toward a research priority: the governance and standards architecture needed to manage trust, accountability, and data sovereignty across all of those boundaries simultaneously.

ISAC as Active PPDR Capability

The evolution of the network from passive data conduit to active participant in situational awareness, through, for example, ISAC and its extension into Joint Communication, Computation, Sensing, and Power transfer (JCCSP), is among the most transformative directions in the portfolio. Current results from iSEE-6G and related projects suggest that achieving sub-metre sensing accuracy alongside throughput above 1 Gbps remains feasible only in controlled environments. Advanced JCCSP waveforms are not yet standardised, require SDR implementations, and introduce stringent requirements for timing, spectrum management, and synchronisation between distributed RUs and UAV nodes that field conditions do not consistently support. Translating proof-of-concept ISAC capability into a deployable sensing layer that functions under the interference, mobility, and time pressure of a real incident is a key open challenge. It is also one where standardisation, spectrum management, operational integration, and PPDR practices must all advance together.

5.3. FUTURE DIRECTIONS TO ADDRESS THE CHALLENGES

The directions here concern the methodological, governance, and strategic orientations that will determine whether technically strong outputs translate into deployable, trusted, and equitable PPDR systems.

Validation must reflect operational reality. Closing the gap between lab performance and field reliability requires three parallel shifts: defining success through degraded and failure conditions, not only peak performance; developing shared, operationally representative datasets as a collective portfolio resource for simulations, digital twins, benchmarks, and AI models; and expanding evaluation frameworks to include operational metrics such as situational awareness accuracy, task completion under partial failure, deployment time under stress, and responder cognitive load. Projects that have linked technical performance to operational outcomes have consistently produced more realistic work and stronger cases for adoption. This should become standard practice across the portfolio.

Coexistence and transition pathways must be treated as design requirements. PPDR agencies across Europe operate with heterogeneous and often ageing infrastructure that will remain in use for years alongside whatever 6G capabilities are developed. Coexistence strategies, transition pathways, and total cost of ownership must sit alongside technical performance as standard evaluation criteria, and are the difference between research that informs procurement decisions and research that remains at demonstration stage.

Preparedness-phase capability requires the most dedicated development. The Preparedness Union Strategy makes proactive crisis management a policy mandate, yet the portfolio remains strongest in the response and preparedness-for-response phases. The PACE framework should be a non-negotiable design requirement, ensuring systems continue to function at reduced capacity under progressive failure rather than collapsing entirely. Future work should explicitly address prevention, community-level resilience, tools for simulation and joint training across agencies, and the 72-hour self-sufficiency ambition of the Niinistö Report. Resilience must be understood in its fullest sense: system resilience to physical and cyber stress, community resilience under pressure, and individual resilience of both responders and citizens.

Security requires portfolio-wide discipline beyond individual workstreams. Operational security means: sovereign supply chain integrity and transparency beyond software-only measures; stress-testing protocols to ensure security does not introduce latencies that compromise life-safety missions; vulnerability disclosure practices and documented responsibility chains that function across borders and agencies; and continued minimisation of attack surfaces as cloud-native and virtualised architectures expand points of vulnerability.

Governance and accountability should be treated as research design inputs across the portfolio. Technology that is not certifiable, not governable, and not trusted by the agencies that must use it will not reach operational deployment regardless of technical performance. Designing for AI Act requirements from the outset, rather than treating them as downstream additions, would make outputs more trustworthy and more directly usable.

Structured stakeholder engagement should be a portfolio-wide standard. The portfolio's strongest outputs have consistently come from projects that engaged PPDR agencies, practitioners, and end users throughout design and development, not only at validation stages. Structured engagement should be a standard methodological expectation at every TRL, spanning problem definition, use case design, solution mapping, and ongoing refinement. The mapping between technologies, use cases, and PPDR values established in this report should be maintained as a living reference and updated as the portfolio develops.

6. TOWARDS IMPACT: THE AMBITION OF 6G IN SERVICE OF EUROPEAN PUBLIC SAFETY

The SNS portfolio has built rich technical foundations across the domains that European PPDR requires. Across use cases, technologies, and testing approaches, SNS JU projects are building the technical foundations that Europe will need if its ambition for resilient, interoperable, and intelligent PPDR communications is to be realised. This final chapter looks forward: first at what a fully realised 6G PPDR capability would look like in operational terms, and then at what is needed to translate current 6G research progress into the societal impact that the European preparedness and EUCCS agendas demands.

6.1. WHAT 6G SHOULD MEAN FOR PPDR: THE 2040+ VISION

The European ambition for PPDR communications by 2040 and beyond is part of a fundamental transformation in the capacity of European societies to protect their citizens, support their responders, and maintain essential functions under the full range of threats that Europe faces in the next decade. European policy has converged on a shared vision: a resilient, pan-European critical communications infrastructure that acts as a resilient foundation for European solidarity, moving 6G development well beyond incremental performance improvements toward something altogether more ambitious.

By 2040, a European first responder should possess true operational mobility as a baseline capability. They should be able to arrive at any incident, anywhere in Europe, and connect immediately via their normal tools to shared communication groups and a shared operational picture that includes every other agency and asset involved in the response. This environment must support the ability to bring unique applications and specialised solutions into the system dynamically, ensuring that the network adapts to the mission rather than the responder adapting to the technology. When the incident is over, the same infrastructure should support recovery, after-action analysis, and preparation for the next event, ensuring that the disaster management cycle is a continuous, informed process.

Realising this vision requires 6G to become more than a connectivity layer, it must become an instrumental tool for anticipating and managing crises before they escalate. Through integrated sensing and real-time environmental monitoring, 6G has the potential to provide early warning of developing threats, a shared and interpreted operational picture across all participating agencies, and the ability to share skills and assess needs in advance and in real time. This shift from reactive communication to proactive situational awareness and planning is what transforms 6G from a faster network into a genuine foundation for preparedness that supports not only responders but the communities who must themselves be resilient when central infrastructure is under stress.

The robustness of that foundation will ultimately be tested in the worst conditions. True preparedness-by-design means that when power fails, towers are destroyed, and multiple agencies converge without shared training, the network continues to function. Meeting this standard requires natively combining energy-autonomous devices, satellite and aerial connectivity, and self-healing edge infrastructure that preserves mission-critical and emergency service levels regardless of the crisis at hand.

Trust is the condition on which all of this depends. As PPDR operations become increasingly cloud-native, cross-border, and dependent on automated decision-making, the foundations of trust must be built into the architecture itself through continuous verification, hardware-enforced security, and supply chain integrity that ensures critical components are not themselves sources of vulnerability. Documented accountability and responsibility chains are equally essential. Agencies will share data across boundaries and citizens will engage with emergency systems only when they have confidence in how those systems behave and who is answerable when they do not.

The full promise of this vision is only realised if its benefits reach everyone. Accessibility and affordability must be central design constraints, not secondary considerations, ensuring that the resilience 6G enables is not concentrated in well-resourced urban centres while rural areas, remote communities, and smaller agencies are left behind. This means attending to the full diversity of PPDR communication contexts, from permanent infrastructure extensions to rapidly deployable tactical systems that can be stood up instantly in a disaster zone, and treating equivalent capability across these contexts as a measure of success in its own right.

6.2. FROM RESEARCH TO IMPACT: WHAT NEEDS TO HAPPEN NEXT

The SNS portfolio has demonstrated that the technical building blocks of resilient, intelligent, pan-European PPDR communications are within reach. What the portfolio has also demonstrated through the challenges documented in Chapter 5 is that technical capability and operational deployability are not the same thing, and that closing the distance between them requires deliberate investment across six interconnected dimensions. Translating those foundations into the societal outcomes sought by the policy also requires deliberate, coordinated action across the research community, policymakers, practitioners, standardisation bodies, industry, and PPDR stakeholders.

Technical interoperability should continue to advance, including the protocols, interfaces, and architectures that allow systems to exchange data. This should, however, also ensure that the research community produces the **evidence base that makes operational interoperability possible**: **demonstrations that work across multiple agencies, multiple countries, and responders who have not trained together**, generating the technical proof points that cross-border governance frameworks, shared command protocols, and spectrum harmonisation processes need to move forward. Research that is designed from the outset to stress-test cross-border, cross-agency operation will produce outputs that are directly useful to the policy and standards processes shaping European PPDR

communications through 2040. Creating this requires validation scenarios that go well beyond single-agency or single-country testbeds, and technical and operational testing protocols drawn from the kind of crisis exercises that expose the hardest coordination challenges. This requires developing new forms of multi-national testing infrastructure paired with governance frameworks.

Resilience should be treated as a primary performance requirement. Energy autonomy, sustained operation under combined physical and cyber stress, and graceful degradation when infrastructure is partially destroyed should be baseline criteria against which all PPDR-relevant systems are measured. They should be evaluated alongside latency, throughput, and coverage as standard performance dimensions. The portfolio's strongest work already frames energy autonomy this way: a node that loses power in a disaster has failed regardless of its technical specification. It should treat the rest similarly.

Security is also key to resilience. The portfolio's security work is strong, and it should be sustained and extended. Resilience requirements include minimising attack surfaces as cloud-native architectures expand points of vulnerability, stress-testing protocols under the combined pressure of physical damage and active cyber threat, and establishing vulnerability disclosure and responsibility chains that function across multi-provider, multi-operator, cross-border environments.

PPDR communications have historically been designed for professional responders, and the current portfolio reflects this. But the policy ambition is broader. Preparedness is now explicitly **a whole-of-society responsibility**, encompassing schools, hospitals, businesses, and individual citizens alongside emergency services. 6G research has a role in this wider frame working towards public-facing connectivity tools. European policy has also set a specific target that any citizen should be able to be self-sufficient for 72 hours in a crisis. **6G research should help meet the technical specifications that support a community that has lost central infrastructure, power, and first responder support for three days.** Answering this concretely, perhaps in terms of local mesh connectivity, energy-autonomous devices, community alert and coordination tools could support the whole-of-society resilience ambition of policy.

Projects should validate under operational stress as standard practice. The most consistent finding across the portfolio is the gap between what performs well in a laboratory and what can be trusted in the field. Closing this gap requires a shift in research methodology. Validation against operationally representative stress conditions should be a standard expectation; that includes damaged infrastructure, spectrum contention, multi-agency convergence, unpredictable human behaviour. This means developing shared operationally realistic datasets as a collective community resource; designing evaluation frameworks that include operational metrics alongside network KPIs; and treating digital twins and sandbox environments as supplements to, rather than substitutes for, validation that reflects the conditions of real incidents. Projects that have linked technical performance to operational outcomes have consistently found it strengthened both the realism of their work and the case for adoption.

6G's contribution should be further extended across the full crisis lifecycle. The portfolio is strongest in the response and preparedness-for-response phases. Recovery, organisational learning, and community resilience represent the next research frontier. 6G can provide the data continuity, post-incident forensics, and analytical infrastructure that allows agencies to understand what happened, adapt their processes, and prepare more effectively for the next event. Connecting 6G research to the whole-of-society resilience should include tools for joint simulation and training across agencies, community-level resilience support, early warning systems, and the local communication capabilities that allow communities to self-organise when central infrastructure is under stress.

Digital literacy and public trust are conditions that determine whether technically capable systems produce the outcomes they are designed for. Research that attends to how systems are understood and used, not just how they perform in labs, will produce outputs that are more robust, more transferable, and more likely to be adopted. This should consider the full diversity of responders, different training levels, languages, and organisational cultures, and the public in the moments when they most need to act on what a system tells them. PPDR community engagement and co-design should be a methodological standards rather than optional enrichment.

As AI-native control becomes central to managing 6G complexity, the research community has an opportunity to shape **what responsible and accountable deployment looks like before the systems reach operational scale**. This means developing interpretable AI, documented decision logic, and auditable responsibility chains as core research outputs alongside technical performance metrics. Research that proactively produces these properties by design will be more trustworthy, more adoptable by PPDR agencies, and better positioned to inform the accountability frameworks that deployment at scale will require.

European strategic autonomy in PPDR communications depends not only on what 6G systems can do, but on what they are made of and where those components come from. The research community can contribute directly to this by treating provenance, auditability, and long-term supportability as design requirements alongside performance. This would involve engaging with the supply chain implications of architectural choices from the outset

Ensure that advanced capability reaches everyone. A system that works for well-resourced urban agencies but is unaffordable or impractical for smaller agencies, rural forces, or cross-border volunteer networks has not fulfilled its purpose. Affordability, ease of rapid deployment by non-specialists, low-bandwidth resilience, and equivalent capability across urban, rural, and remote environments should be explicit research design constraints and part of how problems are framed, solutions are tested, and success is measured.

The research and innovation community cannot resolve this alone. One of the most consequential contributions the programme can make is to encourage activities to actively engage with the bodies and processes that will determine whether research outputs are ever deployed at scale. The processes shaping how PPDR communications will evolve across Europe all need the technical evidence and operational insight that SNS-JU research and innovation is generating. That evidence should be made available in forms that policy and standardisation audiences can use.

REFERENCES

[1] PSCE (2023). What Connectivity to Improve PPDR? https://www.psc-europe.eu/wp-content/uploads/2023/11/PSCE-Connectivity-infographics_V26.09.pdf

[2] European Commission. (2025). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the European Preparedness Union Strategy. JOIN/2025/130 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025JC0130&qid=1743598660031

[3] EPRS [European Parliamentary Research Service]. (2025). EU preparedness: From concept to strategy? (Briefing PE 772.898). https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772898/EPRS_BRI(2025)772898_EN.pdf

[4] Niinistö, S. (2024). Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness. Report by Special Adviser to the President of the European Commission. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

[5] European Commission (2024). The Draghi Report: The future of European competitiveness, Part A: A competitiveness strategy for Europe. Report by Mario Draghi. doi:10.2872/9356120

[6] European Commission (2025). Communication: A competitiveness compass for the EU. COM(2025) 30 final. https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en

[7] European Commission. (2024). White Paper: How to master Europe's digital infrastructure needs? COM(2024) 81 final. https://ec.europa.eu/newsroom/dae/redirection/document/102533

[8] European Parliament Think Tank. (2025). Digital networks act. [Briefing]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772864/EPRS_BRI(2025)772864_EN.pdf

[9] Radio Spectrum Policy Group (RSPG). (2025). 6G Strategic vision: RSPG Report (RSPG25-006 FINAL). https://radio-spectrum-policy-group.ec.europa.eu/document/download/89457260-ab6b-495a-9a10-437711cbe831_en?filename=RSPG25-006final-RSPG_Report_on_6G_strategic_vision.pdf

[10] Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code. https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng

[11] European Parliament Think Tank. (2024b). A future-proof network for the EU: Full fibre and 5G. [Briefing]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762298/EPRS_BRI(2024)762298_EN.pdf

[12] European Emergency Number Association (EENA). (2025). Applying the NG112 Framework to support European legislative requirements (Version 1.0). https://eena.org/wp-content/uploads/2025/11/EU-legislation-and-NG112.pdf

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

PE/51/2022/REV/1. http://data.europa.eu/eli/dir/2022/2557/oj

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). PE/32/2022/REV/2. http://data.europa.eu/eli/dir/2022/2555/oj

[15] Collaborative Coalition for International Public Safety (CC:IPS). (2024). Public Safety Mission Critical Communication: Is this Critical Infrastructure? https://www.bapco.org.uk/_userfiles/pages/files/ccips_public_safety_mission_critical_communication_is_this_critical_infrastruc_hvnajfd.pdf

[16] KPMG. (2025). Critical Entities Resilience Directive: Compliance insights on ensuring resilience for critical infrastructure. Whitepaper. https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/services/cer-whitepaper-may-2025.pdf

[17] National Cyber Security Centre (NCSC). (2025). NIS 2 A Quick Reference Guide. https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

[18] Council of the European Union (2025). Council Recommendation on an EU blueprint for cyber crisis management. 2025/0036 (NLE). https://ec.europa.eu/newsroom/dae/redirection/document/116563

[19] ENISA (2025). Ready, United, Secure, the EU is Cyber Prepared. https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA_Cybersecurity_Bluprint.pdf

[20] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). http://data.europa.eu/eli/reg/2025/38/oj

[21] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). (2024). Official Journal of the European Union, L 2024/2847. http://data.europa.eu/eli/reg/2024/2847/oj

[22] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). (2019). Official Journal of the European Union, L 151/15. http://data.europa.eu/eli/reg/2019/881/oj

[23] European Parliament. (2026). Cybersecurity Act review: What to expect. EPRS | European Parliamentary Research Service. https://epthinktank.eu/2026/01/05/cybersecurity-act-review-what-to-expect/

[24] European Union. (2025). EU Cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[25] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC). (2024). Official Journal of the European Union, L 482. http://data.europa.eu/eli/reg_impl/2024/482/oj

[26] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). http://data.europa.eu/eli/reg/2024/1689/oj

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/oj

[28] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

[29] 6G4Society and PSCE (2025). PPDR Values and KVI Reference Toolkit. https://6g4society.eu/wp-content/uploads/2025/11/6g4society_KVI-PPDR-Workshop_Report_V1.0.pdf

CONTACTS

SNS JU TB chair:

Kostas Trichias, 6G Industry Association

Kostas.trichias@6g-ia.eu

Paper Main Editors:

Katrina Petersen, Public Safety Communication Europe (PSCE)

k.petersen@psc-europe.eu

David Lund, Public Safety Communication Europe (PSCE)

david.lund@psc-europe.eu

Paper Reviewers:

Pedro Tomás, OneSource

Xavier Masip Bruin, UPC

Tomaso de Cola, DLR

Nikos Dimitriou, NCSR Demokritos

SNS JU:

https://smart-networks.europa.eu/

LIST OF EDITORS

Name	Company / Institute / University	Country	Project
Katrina Petersen	PSCE	BE	FIDAL, 6G4Society
David Lund	PSCE	BE	FIDAL
Stylianos Trevlakis	InnoCube	GR	NANCY
Ana Pereira	Ubiwhere	PT	IMAGINE-B5G
Konstantinos Maliatsos	University of the Aegean	GR	iSEE-6G
Tanya Politi	University of Patras	GR	AMAZING-6G
Panagiotis Papaioannou	University of Patras	GR	FIDAL, AMAZING-6G

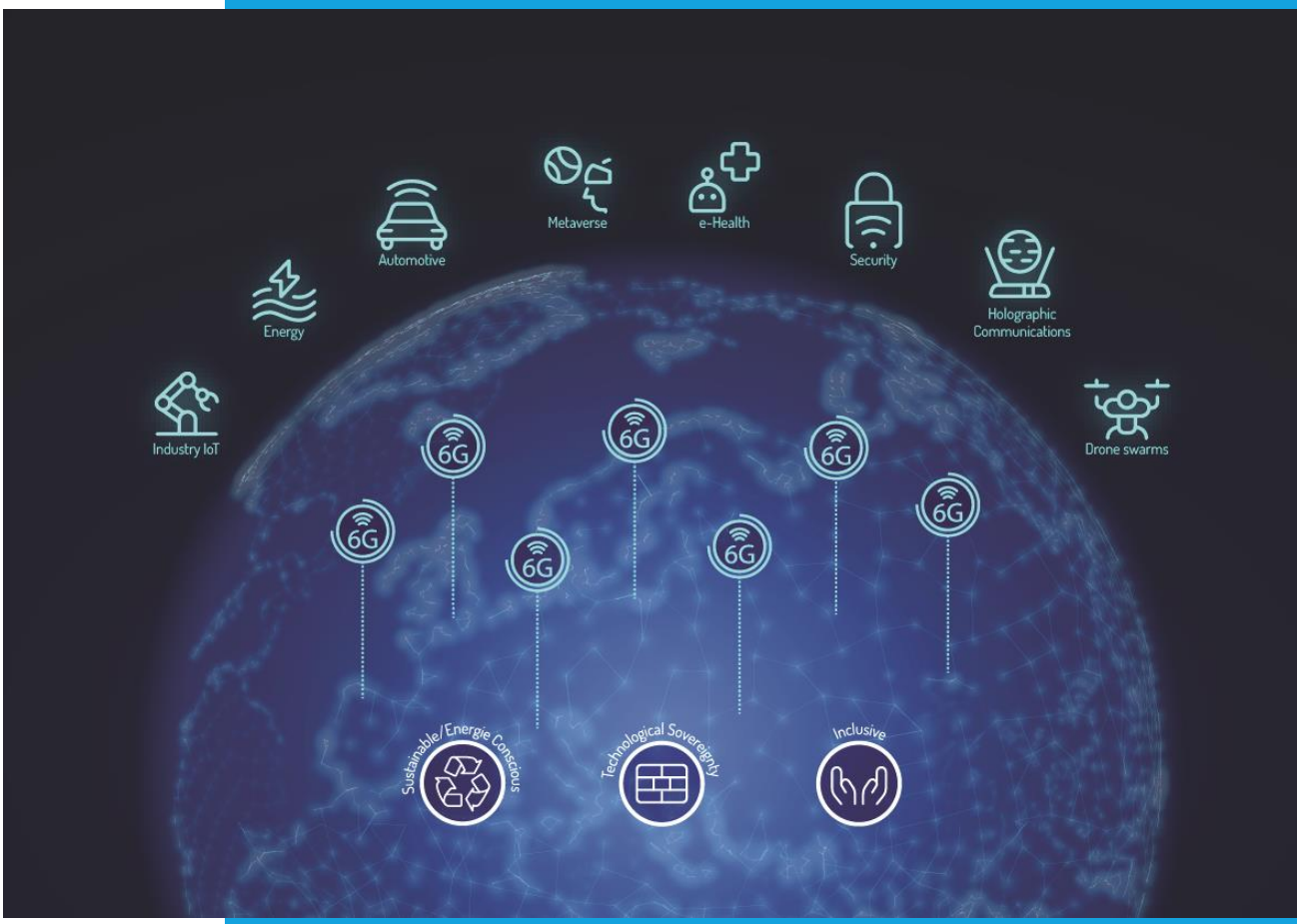
LIST OF CONTRIBUTORS

Contributors	SNS JU Projects
Admela Jukan, TU Braunschweig	MARE
Alexandre Moron, Airbus	6G-PATH, iSEE-6G
Ana Pereira, Ubiwhere	IMAGINE-B5G
Antonios Lalas, CERTH	NATWORK
Benjamin Barth, DLR	5G-STARDUST
Carlos Martins Marques, Altice Labs	IMAGINE-B5G
Christos Tranoris, P-net	AMAZING-6G
Clara Lee, DFRC	FOR-5G
Cristian Petrache, Orange	TrialsNet, AMAZING-6G, iSEE-6G
Daniel Alcaraz Mora, RedZinc	Project Critical
David Jia, Thales	6G-Cloud
David Lund, PSCE	FIDAL
Dimitrios Pliatsios, UOWM	NANCY
Erel Rosenberg, Correlation Systems	FOR-5G
Eva Rodriguez, UPC	MARE
Faheem Awan, Telenor	IMAGINE-B5G

Francisco Fontes, Altice Labs	IMAGINE-B5G
Frédéric Feresin, Azuria	5G-FIRE
Giancarlo Caratti	TrialsNet
Ignacio Ingerto, Digital Aeronautics	Airway
Josep Maria Fabrega, CTTC	6G-EWOC
Jilane el Khouly, Azuria	5G-FIRE
Joan Meseguer Llopis, Valencia Airport	ADAPT-6G, RESCUE-5G
Joao Fernandes, OneSource	6G-Path
Jose Miguel Higon, Valencia Airport	ADAPT-6G, RESCUE-5G
José Ricardo Guimarães, OneSource	RIGOUROUS
Katrina Petersen, PSCE	FIDAL, 6G4Society
Konstantinos Maliatsos, University of the Aegean	iSEE-6G
Luis Cordeiro, OneSource	6G-PATH
Maria Kounalaki, WINGS	TrialsNet
Natalia Polushkina, Rinisoft	FOR-5G
Nikolaos Nomikos, Four dot Infinity	6G-LEADER, MARE
Nikos Dimitriou, NCSR Demokritos	6G-Cloud
Oumaima el Moumen, Azuria	5G-FIRE
Panagiotis Demestichas, WINGS	TrialsNet

Panagiotis Papaioannou, University of Patras	AMAZING-6G
Panos Trakadas, Four dot Infinity	6G-LEADER
Pedro Tomás, OneSource	RIGOUROUS
Pelayo Zemborain, UTEK	ABYSS-5G
Ronald Legallais, Airbus	FIDAL, FIRESCAN
Sokratis Barmpounakis, WINGS	Hexa-X-II, ISEE-6G
Stylianos Trevlakis, Innocube	NANCY
Tanya Politi, University of Patras	AMAZING-6G
Tao Chen, VTT	6G-CLOUD
Tomaso de Cola, DLR	5G-STARDUST, 6G-NTN, UNITY-6G
Xavi Masip, UPC	MARE

Smart Networks and Services Joint Undertaking (SNS JU)
Technology Board (TB)



Website: https://smart-networks.europa.eu/