MAKING THE WORLD A SAFER PLACE

THE ROAD TO PS-LTE

Table of Contents

1 Introduction

If the last years of progress in mobile networks have taught us anything, it is that **technology is evolving today faster than ever before**. Many features of daily life that we now take for granted could not have been imagined even a decade ago.

Yet, sadly, many of the **technological solutions supporting the world's emergency services today are far behind the latest technological capabilities**. Many current public safety networks cannot replicate functionalities that the most basic consumer mobile devices of today do with ease, such as distributing pictures or videos taken at a crime scene to other first-responders, or transmitting the geo-location of personnel in real-time to a central coordinator.

At the same time, we also see sophisticated solutions being deployed across the world that defy our previous conceptions of what is possible, such as street lights detecting and instantly reporting gunfire, not only with the location of the shot, but also with information about the specific model of gun used.[1]

We also see forward-thinking public safety authorities planning to use technological solutions that will forever **change the world of public safety**:

- Drones scanning mountains after avalanches to find survivors with infrared cameras;
- Video-cameras rotating on top of vehicles for first responders and continuously searching and running facial recognition to find suspects on the run;
- Augmented Reality (AR) helmets for firefighters giving real-time information in 3D about the surrounding temperatures and toxicity levels, as well as expected positions of survivors.

However astonishing these yet-to-be-built solutions may be, what excites us most about the future of public safety are the solutions yet to be imagined, and the **countless lives they will save**.

In this paper, we lay out what we believe public safety decision makers need to consider to be ready for this new reality. We do so by **studying recent incidents around public safety networks**, what we have learned in our numerous **dialogues with industry-leading thinkers,** and by concluding from these what we believe to be the **key elements that people in a position to influence** the future of public safety networks must take into consideration.

[1] Allison Barrie, "Incredible tech detects gunfire across America" *Fox News*, Mar 2, 2017, Foxnews.com.

2 Learnings from recent public safety network challenges around the globe

We live in a time when the **frequency, magnitude, and nature of the threats to public safety are changing**. Increasing global temperatures are driving a wave of natural disasters in some countries that are unprecedented in scale and severity. The rise of asymmetric warfare is pitching emergency services against more frequent acts of terrorism that are, by their very nature, designed to be difficult to react to.

Even though Land Mobile Radio (LMR) networks have been reliable voice communication tools for years, **current public safety networks (PSNs) have been put to the test** over the last couple of years. In some cases, the outcomes have been far from ideal, highlighting the shortcomings in today's solutions with painful clarity. There is, however, much to be learned from these situations – important lessons that will help design the next generation of PSNs.

In this paper we **specifically study four situations that highlight key issues**:

1. Missing basic **network capabilities**: Effective disaster response requires specific network capabilities different from the needs of day-to-day emergency management (e.g., warning systems, coordination);
2. Insufficient **traffic management**: Extreme events sometimes lead to extensive traffic for specific regions, resulting in network unavailability;
3. Lack of **broadband features**: The limits of voice-only communications become clearer in a world where even basic consumer devices are capable of a range of features that would be invaluable in disaster management;
4. A naive view of **cybersecurity**: Not only IT-systems, but the core communication networks, themselves, become targets for ever more sophisticated cyberattacks with the potential to disable critical public safety functions that are increasingly reliant on digital infrastructure.

2.1 Missing basic network capabilities

Post-mortem analysis of 2018's wildfires in a European country

In 2018, a **devastating series of wildfires** broke out in one European country, leaving more than 90 people dead and more than 150 injured. While some citizens, journalists, and analysts blame the tragedy on a combination of poor disaster management planning, climate change, and arson, had **the public safety network in operation that day been equipped with the capabilities shown below,** the impact of the event could have been lessened.

In three specific instances, solutions that are widely known could have been used to increase the effectiveness of the disaster response.

Situation: No warning alarms were sounded for citizens.

Problem: Residents were informed of evacuations via word-of-mouth.

Possible solution: **SMS-CB (cell broadcast)** used in Japan – broadcasts directly from cell towers to every phone in range, allowing for geo-based targeting with essentially unlimited capacity.

Situation: One of the helicopters that arrived did not have a wireless communication system to coordinate with ground forces.

Problem: Air-to-ground communication was poor.

Possible solution: **Device-to-device communication** or **satellite network.**

Situation: Issues arose in redirecting communication between agencies.

Problem: Communication between agencies such as fire service and police on the ground was delayed and inefficient (agencies tend to communicate through the high-ranking officers' personal mobile phones).

Possible solution: **Integrated systems** usable across agencies and regions.

While these wildfires bring the issues into sharp relief, the truth is that most current public safety networks across the world share the same challenges.

2.2 Networks not dimensioned for extreme events

Post-mortem analysis of 2017's forest fire in a European country

In 2017, a series of **deadly wildfires erupted in a European country,** resulted in at least 65 deaths and 204 injuries. The country's ruler called the disaster "the greatest tragedy… in recent years" and declared three days of national mourning.

During the disaster, more than **1,700 firefighters across the country were dispatched** to fight the fire, leading to a high density of traffic in an area with limited population. The **network had not been dimensioned with the capacity** to handle such a traffic load – the event was outside of the "range of reasonably expectable scenarios."

Situation: Emergency services were unable to communicate.

Problem: The network backhaul was incinerated in the fire.

Possible solution: **Build redundancy** into base station backhaul connections, such as secondary satellite links or portable base stations.

Situation: Real-time warning systems failed.

Problem: TETRA connectivity with commercial mobile networks is limited due to technological issues.

Possible solution: **SMS-CB (cell broadcast)** with no capacity limit using LTE.

This tragedy highlights the most important difference between designing public safety network systems and traditional commercial networks: **traditional networks are built to operate well within the parameters of 'normal' use, failing only in extreme cases**. Disasters that lead to large death tolls, however, are extreme cases by definition, falling outside the range of 'reasonably expectable' scenarios.

2.3 Lack of broadband features in outdated voice-only networks

Post-mortem analysis of 2017's terrorist attack in a European country

In 2017, a **terrorist attack occurred in a European country** where an individual drove a truck through the city's busiest shopping street, during peak hours, killing five and injuring 15.

While police officers were quick to react to the event as it happened, with the assistance of civilians and a well-functioning command center, there were **technological constraints which delayed the speed and effectiveness** of their ability to identify and apprehend the suspect.

This case shows **the limits of narrow-band voice-only systems**, even when they perform perfectly against their specifications. Such systems lack of features that might have seemed like science fiction when the networks were designed, but which are now available in even the most basic of consumer devices.

Event: Some police officers left their vehicles to take control of the situation on foot.

Problem: Geographic coordination had to be done via walkie-talkies because all central tracking of police officers' locations was based on the locations of their vehicles.

Possible solution: **Individual GPS tracking** of each police officer with real-time location sharing between officers.

Event: Civilians took pictures of the suspected terrorist as he left the truck and fled on foot.

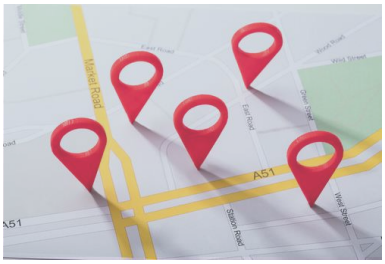
Problem: Police officers had no ability to share pictures with one another and resorted to describing the suspect verbally.

Possible solution: **Basic smartphone functionalities** to enable officers to share digital information

Event: A picture of the suspect found in the surveillance system of the transport authority was sent to the command center within approximately an hour.

Problem: Critical information was not shared in a timely manner between different agencies.

Possible solution: **Integration of systems** across agencies and regions.



Event: Command center agents received differing reports about the exact location of the suspect from civilians.

Problem: Large influx of reports of the suspect were received at two different locations, leading officers to misprioritize an incorrect location.

Possible solution: **Basic smartphone functionality for officers** – for video and image sharing.

One important lesson to be learned from this case is that authorities must not only act resolutely and **accelerate deployment of their planned PS-LTE system**, but **also invest in current systems** and workarounds to minimize issues while the next generation of networks is still under development.

2.4 Cyberattacks against the network itself

Cyberattacks have, over the last few decades, metamorphosed from being a marginal phenomenon directed at commercial entities to a core threat that goes to the very heart of a nation's infrastructure vulnerabilities. Whether the perpetrators are individuals or organized groups, well-organized attacks today could cripple and disable entire public safety systems.

Although authorities are clearly taking the issue very seriously, the design of the network tends to neglect security elements beyond conventional network security. In the shift towards broadband based public safety networks it is important to recognize that the end user devices and IoT systems themselves can be a target of attacks, and more focus **should be placed on end-to-end network security**.

Prevention in this new reality requires a complete end-to-end view of cybersecurity, including device authentication and securing the integrity of transmissions. Although, we have yet to see this being used as a factor in any actual attack, exploiting this vulnerability could give a hacker access to the network at a very deep level.

It is not farfetched to imagine a situation where cyberattacks target the network itself, and that could have dire consequences.

SCENARIO ONE

A criminal **steals an officer's communication device and gains access to confidential information** regarding the organization which helps him to plan attacks, e.g., location of principals.

SCENARIO TWO

A **terrorist triggers a gas leak alarm by generating false sensor warnings,** diverting emergency response resources to a false location in advance of an attack in another area. Response force redirection is a common technique utilized in terrorist attacks; one such event occurred in Europe in the early 2011.

SCENARIO THREE

A **criminal organization gains access to terminals, allowing it to edit or remove existing records** and information **regarding the perpetrators**.

SCENARIO FOUR

A **hacker auto-generates 1,000 simultaneous 911 calls to overload and disable the system;** one such event took place in North America in 2016.

SCENARIO FIVE

An attack is accompanied by activating a group of **false base stations or jamming devices that** disable the network around the area of the attack.

This tragedy highlights the most important difference between designing public safety network systems and commercial networks. **Traditional networks are built to operate well within the well-defined parameters of 'normal use', failing only in extreme cases**. However, disasters that lead to large death tolls, usually, by their very nature, fall outside the 'range of reasonably expectable scenarios.'

3 Public safety network imperatives – a new consensus emerging

When the notion of **moving from traditional narrowband to LTE-based public safety networks** was conceived, there were still many uncertainties and points of debate over how best to design and build these networks. Over the last couple of years these issues have been given serious attention by public safety authorities globally.

We have had the privilege of being part of many of these discussions, and **from these dialogues we have drawn the conclusion that there is a new consensus emerging** – a realization, shared by leaders in the field, that **four factors must be acknowledged** if broadband technologies are to become the new reality. Specifically:

1. ***Only dedicated networks*** can provide the **required reliability for mission critical usage**;
2. **Networks will sometimes be built using *nonstandard frequencies*** outside of normal commercial bands;
3. ***Migration from legacy networks must be the focus,*** with an emphasis on temporary coexistence;
4. An ***integrated view of solutions, in anticipation of future applications*** yet to be imagined, is imperative.

3.1 The need for dedicated networks

One of the most fundamental debates with regard to PSNs has been whether they are best built as separate networks (as the current TETRA/TETRAPOL networks) or if the public is better served when they operate on top of existing commercial networks. The **arguments in favor of commercial networks** have been three:

1. Not having to build a new network leads to substantial ***cost savings***;
2. Commercial networks enable increased ***speed of build***, with coverage across the nation from day one;
3. ***Traffic prioritization*** and targeted geographic network reinforcements can solve capacity issues

The benefits of this choice, in terms of cost-savings and time of implementation, are indisputable, but the **issue of reliability** has raised such a degree of concern that today, **81% of the countries nearest to deploying a PS-LTE network** are planning to do so based on a **fully or partially dedicated network.**[2] There are four justifications:

81%

Of countries plan to fully or partially deploy dedicated PS-LTE networks

1. Commercial networks are generally designed for a lower level of reliability

It **makes no commercial sense to build networks that 'never fail.'** The costs of doing so would far outweigh the benefits in the eyes of commercial consumers. This principle affects design choices throughout the network, from capacity dimensioning and transmission aggregation ratios to electricity backup resilience and level of redundancy in equipment and backhaul. This is why network failures in commercial networks are so commonplace, e.g., the two nationwide mobile outages experienced in an APAC country in 2018, one of which lasted seven hours and even affected the connection to the national emergency number.

2. Disasters are extreme events – the situations that commercial networks are least well-equipped to handle are exactly the situations where public safety networks are most needed

Commercial networks are optimized for operating under 'reasonable assumptions of conditions.' A situation where a plane crashes in the center of a city is the opposite of that. Yet such moments are exactly when the need for a public safety network to operate flawlessly is at its greatest. Commercial networks degrade or fail, almost without exception, during disasters.

Yet during many of the same disasters the dedicated networks of emergency services have continued to operate uninterrupted (the aforementioned terrorist attack in a

[2] Based on NEC's customer research survey conducted among PSN decision makers in 43 developed and developing markets globally, April 2018.

European country is a good example where, despite commercial networks crumbling under pressure, the dedicated public safety system experienced no problems).

3. Commercial networks optimize deployment around where people live, while such disasters strike in all kinds of places

The notion of commercial networks having national coverage is not entirely accurate in the context of disaster response. Commercial networks generally measure coverage by population, not geography. Also, capacity dimensioning is based on where the population normally uses the service. This issue is best illustrated by the recent forest fires in Europe. In few events is it more critical that communications work than when isolated teams of firefighters are deployed in the middle of a burning forest. Yet these are often the locations where barely anyone lives. If the commercial networks have coverage at all, they are **not dimensioned to deal with the stress of the traffic generated** by a nation's firefighters being deployed to such a remote area.

4. Prioritization alone is not enough to guarantee reliability

The idea that traffic prioritization can increase the reliability of a commercial network service to the level of a dedicated or hybrid network is mistaken. First, such prioritization only works if the network is running in the first place. Second, the extreme conditions associated with disasters can drive traffic to levels where the prioritization engine, itself, cannot handle the load. Finally, the commercial networks in some areas simply cannot handle the required load, even at full capacity.

The future technologies of 5G, such as network slicing, offer a new, more robust version of quality-of-service prioritization. Yet, few decision makers seem willing to bet on this, choosing instead to take the "NASA" approach, whereby no technology can be considered reliable until it has been proven 10 years in the field (4G-LTE) is about to reach this threshold, but 5G still has a long way to go).

3.2 No escaping nonstandard frequencies

Countries opting to **build dedicated or hybrid public safety networks** will often face a situation where they **need to deploy outside of the standard (3GPP) band of commercial deployments**, requiring both network and device customization of equipment.

To build new nationwide networks at anything that resembles acceptable cost would have to be done on low bands. The physics of propagation are such that **lower frequencies allow for a ubiquitous network at a fraction of the cost** of frequencies above 1500MHz. This is why current narrowband networks, usually operating at sub-400MHz frequencies, could be built at relatively low cost.

Many countries are looking at the 700MHz band as the band of choice for dedicated public safety networks. Although it is a natural choice, given the frequency characteristics and the fact that it remains unoccupied in many countries, **it also presents complications**. The 700MHz band plays an important part in the development of commercial networks, and there is a tension against other national interests when it comes to allocating a third (usually) of the usable spectrum (i.e., 2x10MHz) considering the lost auction revenues for the government and the socio-economic impact of the reduced 4G/5G coverage.

Lower bands in the 450MHz (or even less common bands) have fewer of these problems as they rarely have a role in commercial networks and also have better coverage economics for public safety networks. **This band range has already been the choice of several successful early deployments**, most notably Brazil, where the frequency was not yet standardized when it was deployed.[3]

The **problem with these lower bands** is that they are, for historical reasons, not as uniform as the bands normally deployed for commercial use. Many slots in the sub-600 band have only recently been standardized by 3GPP and some have yet to be so. In some cases, the available allocations are a near but not perfect match to standardized areas of the band; in some countries they are entirely different.

> *"...many future deployments will need equipment customized for specific frequencies and not necessarily off-the-shelf commercial networks"*

Hence, **many future deployments will need equipment customized** for specific frequencies and not necessarily off-the-shelf commercial networks from suppliers. Yet oftentimes the **cost reductions associated with lower bands** outweigh the inconvenience of deploying the types of equipment required to utilize them.

[3] André Rocha, Juliano João Bazzo, Luís Cláudio Pereira, João Paulo Miranda & Fabrício Lira Figueiredo, "LTE 450 MHz technology for broadband services in rural and remote areas. Case study of Brazil", *ITU News*, Nº 10 2013, ITUnews.itu.int.

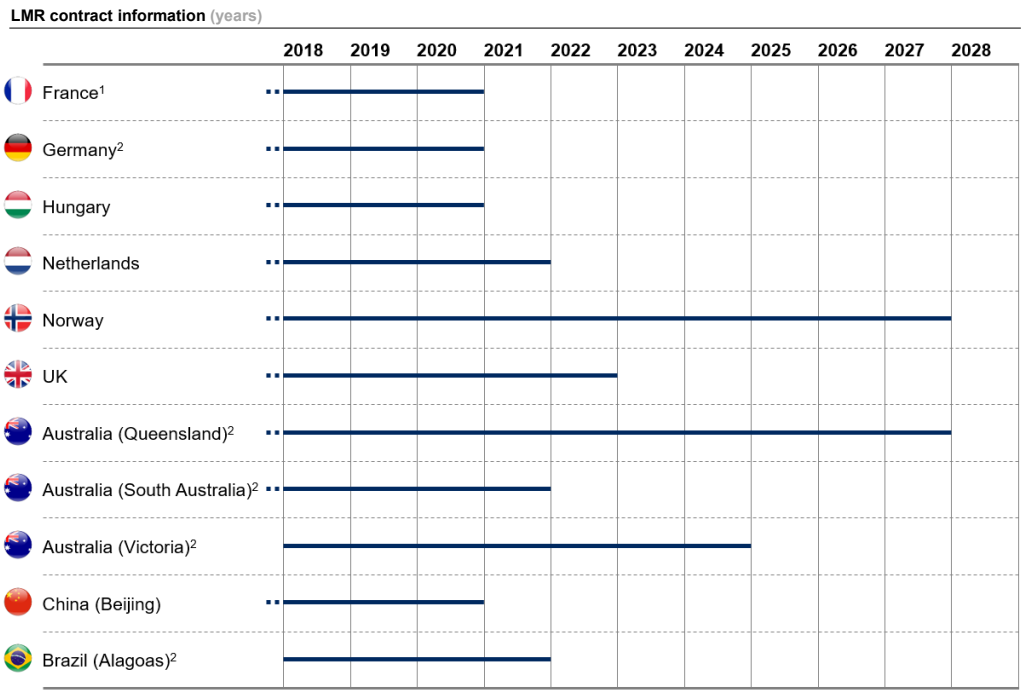
3.3 Migrating from legacy networks

Despite their lack of modern broadband based applications, there can be little doubt that the **existing narrowband networks have served the public safety needs well** for years. In many countries they have provided reliable voice-based emergency service communications in the face of situations driving traffic well beyond what commercial networks could withstand (e.g., 9/11). It is important to recognize that these networks will be with us for a long time. In many countries, existing service contracts run several years into the future and, in others, new TETRA/TETRAPOL investments have recently been made. That said, there is **currently no path for gradually upgrading** these networks to broadband applications within the frameworks of their specifications.

Any deployments of PS-LTE will have to factor this in, either by **integrating with existing narrowband networks or finding a solution for seamless migration**; a migration that delivers the benefits of broadband based applications as soon as possible to emergency service staff, while maximizing use of existing voice-based networks for their reliability and prevalence.

In fact, dealing with this issue of temporary coexistence is one of the primary concerns we have identified in our dialogue with PSN decision makers. There has been significant progress in 3GPP in terms of standardizing TETRA/PS-LTE interoperability. However, as of today there have been no full-scale deployments incorporating all features, and there are other options that need to be evaluated.

Figure 1: TETRA contracts remain for many years



1 Airbus will cease to maintain network in 2035, and in 2020 in some areas including Paris
2 Start dates of the TETRA contracts for some of the countries has been assumed to be the public announcement of the contract

3.4 Taking an integrated view in anticipation of the future

Many **use cases we now expect future public safety networks to be able to handle** (e.g., automatic facial recognition built into rotating cameras on vehicles for first responders) would have been thought science fiction when the current networks were first constructed. Further, **every year we find new applications proposed** that would have not been considered possible just years earlier (e.g., an armada of coordinated drones with heat-seeking cameras deployed over a mountain after an avalanche to find survivors under the snow).

> *"...every year we find new applications proposed that would not have been considered possible just years earlier."*

This rapidly increasing pace of technological development poses a **problem when planning for deployment of a network** that is supposed to operate for at least a decade. Consequently, the most advanced thinking in this realm today includes planning, not only for technologies we know of and desire, but **for applications we cannot yet imagine being deployed**.

In light of this, we see **decision makers** taking a more **integrated view of deployment,** anticipating that future innovations could be more complicated than simple applications on top of broadband networks, and that incorporating network elements (e.g., mobile edge computing) integrated directly with, for instance, command center software. Hence, increasingly there is a premium placed on solutions that will be able to take an end-to-end view of the entire system in terms of application development as opposed to just providing individual components.

4 Five key requirements for successful networks

Recent cases of network failure as described earlier, and the emerging imperatives gleaned through our discussions with industry thought leaders, lead us to conclude that there are five main areas of concern for **every procurer of a PS-LTE network**:

1. Reliability: The availability of a network supported by redundant architecture, quick recovery, and durable equipment;
2. Applications and network features: Network compatibility with the applications and key features of today (e.g., facial recognition solutions, biometric authentication, MCPTT) as well as robustness to support applications of the future;
3. Cybersecurity: Looking at cybersecurity as an end-to-end issue, recognizing that many of the most important vulnerabilities must be addressed in the network layer itself;
4. Customization: The degree of customization required to make the solution work in the local context, be it nonstandard frequencies, resilience in the face of local climate conditions, or physical dimensions of network units;
5. Land mobile radio (LMR) migration: Dealing with the migration from LMR to PS-LTE to get as many benefits as possible from the new networks while optimizing legacy network usage to minimize costs and leverage proven reliability.

In the following sections, we discuss these concerns in further detail to shed light on the technical requirements decision makers should consider when building robust, future-proof networks.

4.1 Reliability

When asked **what matters most for their communication equipment**, any first responder will give the same answer: reliability. Relative to other uses, reliability is foremost a convenience, but in the case emergency response, reliability can be a matter of life and death.

To ensure the network meets first responders' extreme requirements of dependability, **decision makers need to strive to maximize** five parameters:

1. Level of network dedication: Although hybrid networks utilizing commercial infrastructure have many benefits, at the end of the day the last line of defense will be the elements of the network that are dedicated; dedicated not only in the sense that they operate on separate frequencies of separate equipment, but that the network as a whole has been designed from the ground up to ensure reliability in every component of the network.
2. Durability: All elements of the network need to be considered in terms of end-to-end durability, from devices to eNodeBs, core, and backhaul. Durability needs to be measured across multiple dimensions: mean time between failures (MTBF), climate fluctuations (temperature, humidity), margins of error in extreme circumstances (flooding, sand storms), considering not only the core parameters of the equipment but the guardrails that come with it (e.g., placement on the tower).
3. Track record: No piece of equipment can truly be considered reliable until proven in actual field conditions. Assessments of average lifetime for newly produced equipment is an estimate from a lab. Quantified results from real-life deployments is something else. Newly invented technology can be extremely thoroughly tested, with errors only discovered after wide-scale use (e.g., INTEL Pentium FDIV bug, 1994).[4]
4. Layers of backup: Even equipment meticulously designed solely for reliability will eventually fail under some circumstances. The only guarantee of continued operation in these situations is a multilayered, redundant architecture with standby units ready to activate and replace failed components. Also, the design must be optimized for autonomous operation, i.e., the ability to continue functioning even when the surrounding environment experiences failure.
5. Recovery time: Backup solutions are no more useful than the time they take to activate. The aspiration should always be for as near to instantaneous recovery as possible.

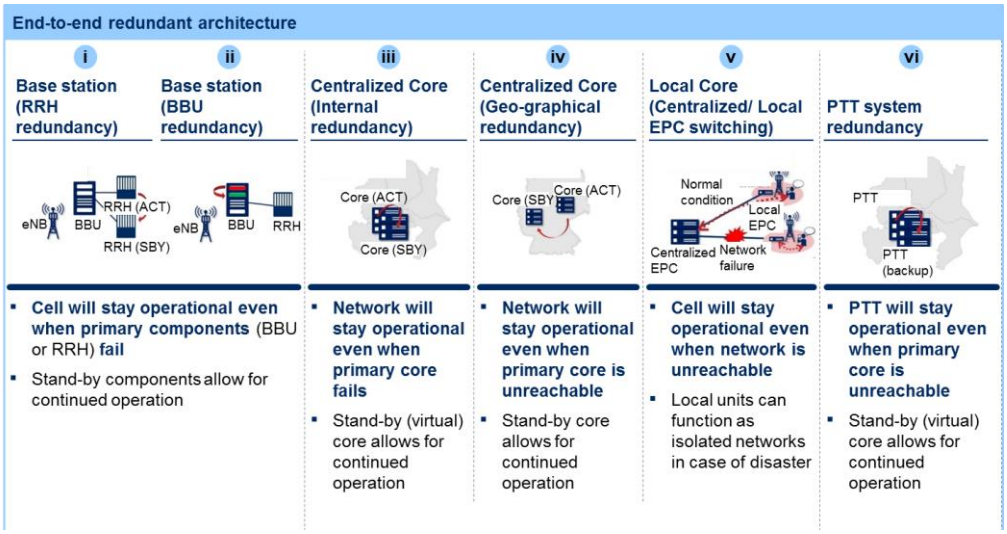
At NEC, we believe that what is **required from network architecture** is:

- Redundancy at every level of equipment: Board-level, component-by-component redundancy in RAN with the ability to seamlessly switch to a backup unit.
- Geographic redundancy: Multiple autonomous cores and MCPTT servers able to operate even in cases of a backhaul disconnection.

[4] John Markoff, "COMPANY NEWS; Flaw Undermines Accuracy of Pentium Chips", *The New York Times*, Nytimes.com.

- Isolated cell operation: Sufficient core capabilities adjacent to each base band unit (BBU) to be able to handle local traffic (including new units coming in to the coverage zone) even in cases of complete disconnection from the network.
- Track-record: All elements of the network having a track record of operations in the field, preferably withstanding shocks from natural disasters.
- Rapid recovery: Minimized time to recover.

Figure 2: Network technology with six layers of redundancy



4.2 Applications and network features

When making decisions about future public safety networks, it is **important to not exclusively focus on the technical details** of the network itself. The networks are, after all, built to support the applications that run on them. These applications are currently developing at a pace unimagined a couple of years ago, facial recognition software being a case in point.

"...applications are currently developing at a pace unimagined a couple of years ago, facial recognition software being a case in point."

This introduces a problem for critical communications and disaster management decision makers: although we do not yet have visibility on the technologies we will require 24–36 months out, the networks we build today will stand for 10–15 years. So how do we **ensure that the infrastructure choices we make will be compatible with future innovations**?

There are no perfect answers, but **we know some things with relative certainty**:

1. **New use cases** are emerging with the introduction of cutting-edge solutions such as facial recognition software for border control and surveillance.
2. Many of the **next generation applications will be AI based**. Understanding how AI platforms can be most effectively integrated into the network design matters.
3. **Core features of current LMR networks**, such as trunked communications and calling groups, **will also be required** going forward and future networks must be prepared to deal with them.
4. **Specific-purpose networks allow for integrating applications** deeper into the network layers than commercial networks that are built to maximize benefits for OTT applications. There are already technologies on the horizon (e.g., mobile edge computing) which the most advanced next-generation public safety networks are likely to utilize.

For decision makers, we at NEC believe this challenge necessitates:

- **Prioritizing mission-critical solutions with high accuracy,** which is critical for minimizing analysis and reporting times. It is important to note the high capability gap that exists between providers of advanced technologies which can be seen by the difference in error rates of facial recognition solutions, shown in Figure 3.
- **Evaluating peripheral applications** carefully. As shown in Figure 4, there are many applications for PS-LTE and we should choose suitable solutions based on the requirements of the country. These solutions not only include biometric recognition but also analytics solutions, such as behavior analysis and customer profile estimation.

- **Planning for AI** by enriching an understanding of which generalized AI platforms can serve as a basis for multiple applications, how they do it, and how they relate to the network.
- **Anticipating integrated applications** by discussing with suppliers that take an end-to-end view of the network as a whole to understand how future applications will require coordinated R&D across these network elements.

Figure 3: Performance variability in facial recognition solutions

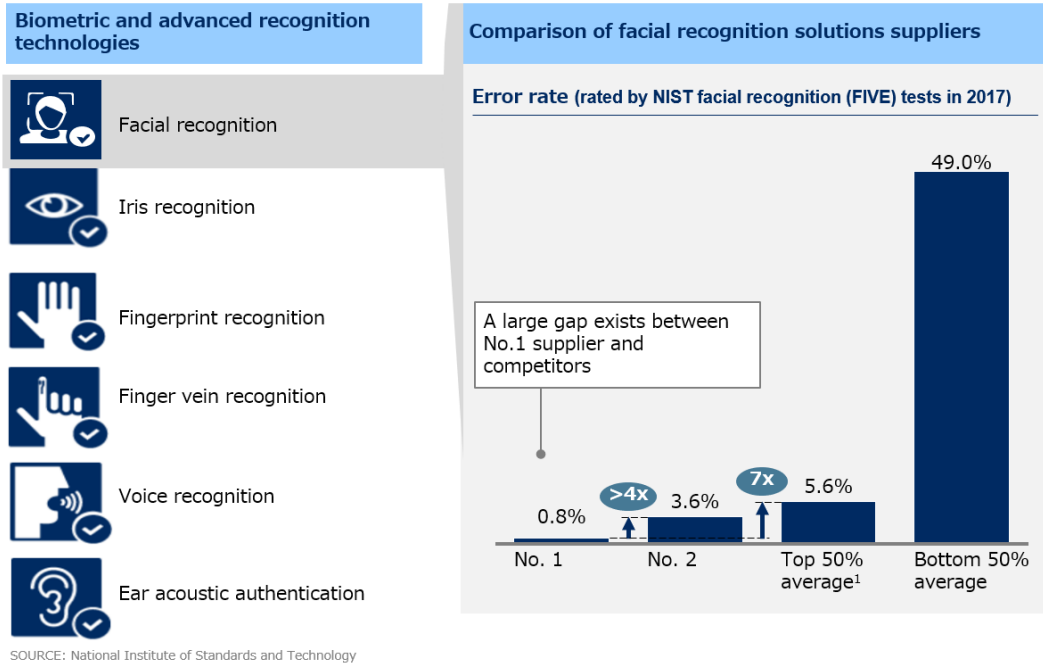
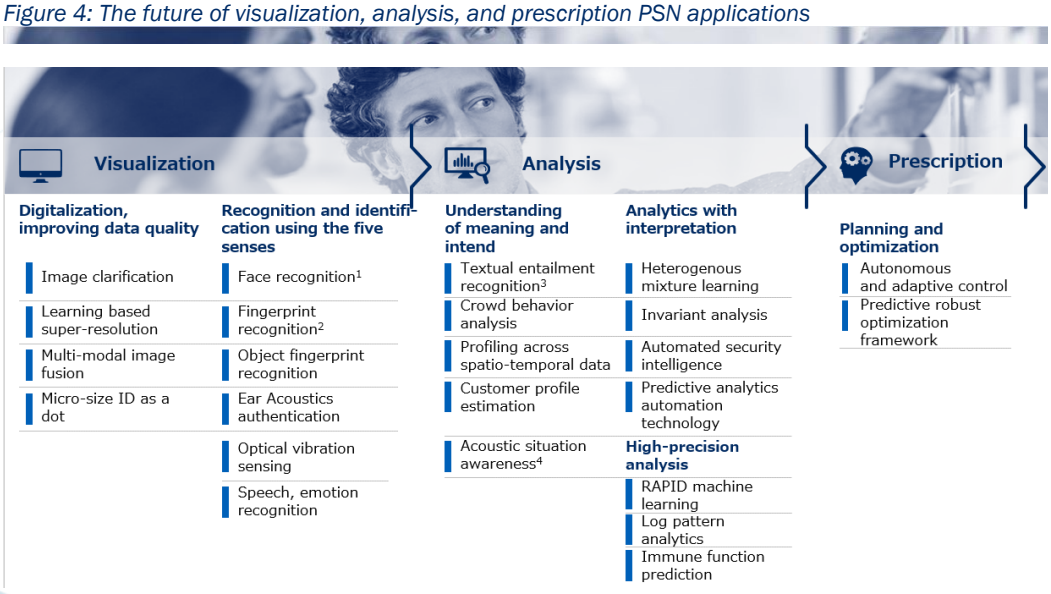


Figure 4: The future of visualization, analysis, and prescription PSN applications



4.3 Cybersecurity

In section 2.4 “Cyberattacks against the network itself,” we mentioned four main threats common to public safety networks: **confidentiality, data integrity, network availability, and unauthorized network access**.

The **security concerns of users and procurers** of public safety networks are usually centered around IT security as well as encrypted communications. However, because communication and collaboration involve an increasing number of devices (computers, handsets, and sensors) for some of which authentication is different in nature than for traditional IT-system endpoints, there is the **need to employ a broader range of security solutions** than today. **Procurers of public safety networks need to ensure that security solutions are end-to-end**, across IT systems, network communications, and end-point devices.

4 threats

to network safety

1. Confidentiality
2. Data integrity
3. Availability
4. Unauthorized access

Specifically, as outlined in Figure 5, **firewall solutions** should block suspicious traffic before any damage to the systems occur. They should do so by using **a dynamic signaling firewall software** and all IoT devices used on the network should be encrypted. **Anti-malware solutions** should reliably prevent malware attacks against servers, network devices, and user devices to ensure the integrity of the data stored and transmitted. **Network defense solutions** should be multilayered and protect against blended network attacks, without slowing down connections. **All devices** that are used on the network should be **protected using biometric authentication**. The **authentication information** of network users and especially network administrators should be **encrypted,** and changes thereof should be controlled.

Figure 5: Network and IT security solutions

✓ Eliminates threat

	Solution Name (Product)	Threats			
		Confidentiality breaches	Threat on data integrity	Network unavailability	Unauthorized Network Access
NW Security & Authentication	1. Signaling Protection	✓	✓		
	2. DoS/DDoS[1] Defender			✓	
	3. Biometric Authentication				✓
IT and IoT Security	4.. ID/Key Management				✓
	5. ID/Password Management				✓
	6. IoT Device Security Manager				✓
	7. Light-weight encryption development kit	✓	✓		
	8. Anti-Malware Software	✓	✓	✓	✓

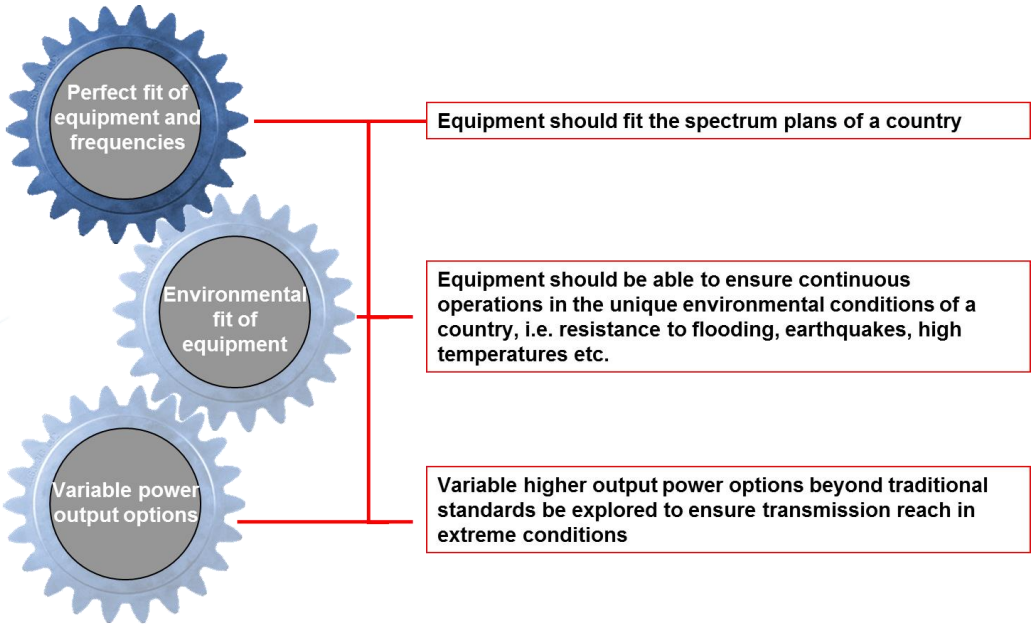
4.4 Customization

For public safety networks to meet functionality and reliability expectations in **many countries, customized solutions will be needed**. This may happen for several reasons, such as available frequency bands being outside of the 3GPP standardization, environmental considerations, or simply form factors.

Specifically, we believe that **procurers should not limit their requirements** (see Figure 6) to the specifications that are readily available for commercial equipment but rather, they should **require:**

- Manufacturers to provide **equipment that fits the frequency plans of the country** rather than having the frequency plans of a country adapt to commercial standards.
- **Equipment that meets the potentially higher environmental conditions** required for continuous operation rather than abiding only by what commercial equipment can allow, be it resistance to flooding, earthquakes, sandstorms, or simply temperatures outside the normal range.
- **Higher variable output power options** beyond traditional standards to be explored to ensure transmissions can be received in extreme conditions.

Figure 6: Customization demands



4.5 Land mobile radio (LMR) migration

Despite the broadly shared ambition to move from the narrowband solutions of today to broadband based networks, **current communication systems will remain with us for quite some time**. Many countries have recently invested in the continuation of TETRA/TETRAPOL systems, while more countries still have many years to go on existing contracts (Figure 1). The TETRA/TETRAPOL networks will be with us for many years to come, not least because emergency service personnel have come to trust them, which inevitably leads to the **question of how best to make use of the period when legacy systems coexist alongside LTE networks**.

There are **multiple options** and, as of yet, no agreed common practice. Systems can be integrated (through gateways or other means), co-exist with dual devices, or a multitude of options in between.

Whatever the exact choice of solution, the **objectives of migration** are clear:

- **Maximize the utility** of existing LMR investments;
- Provide the **new functionalities enabled by PS-LTE** to staff in the field as rapidly as possible;
- **Minimize any interventions** in the current systems that could threaten the integrity of operations;
- **Keep LMR systems operational** in migration while the reliability of PS-LTE solutions is being field tested;
- **Minimize additional costs** related to temporary solutions.

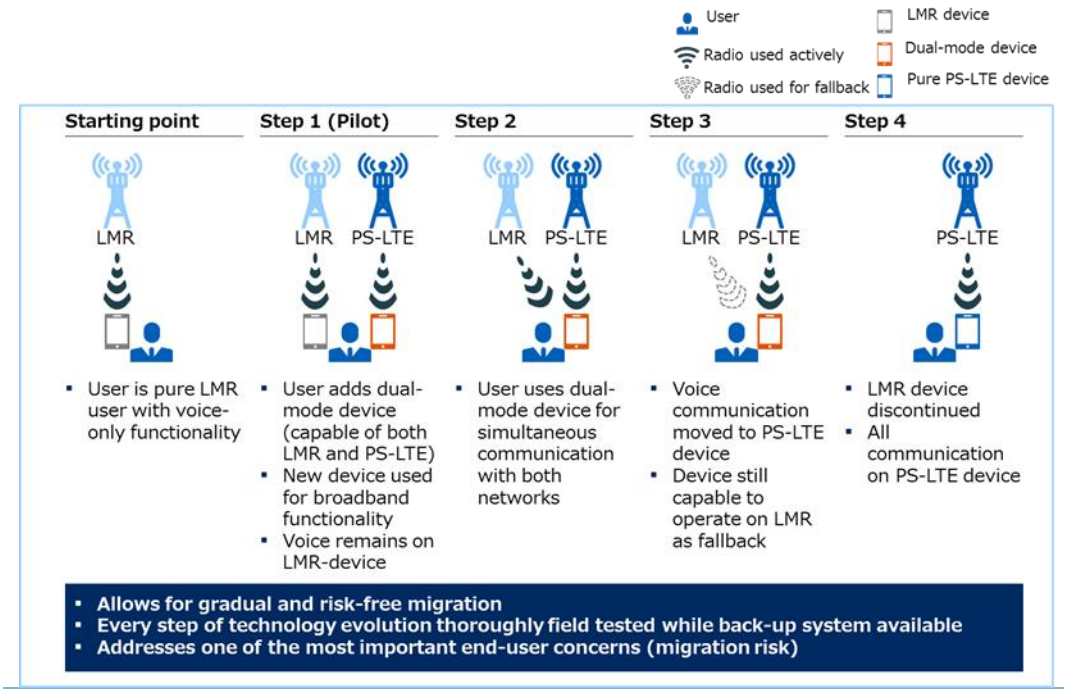
There are several potential technical options to handle the period of migration. We recommend solving it on the device side, specifically by

- **Introducing dual-mode devices** that simultaneously transmit to LMR and PS-LTE networks;
- **Employing broadband-based devices** that can utilize the PS-LTE channel while narrowband voice can remain on the LMR network initially;
- **Integrating functionalities** at the application level of the device.

By this method users can gradually migrate in a way that ensures full field testing before switchover.

- No need to tamper with currently operable networks, ensuring stability
- Costs are kept at a minimum as a device-level development is cheaper than integration in the network layer

Figure 7: Dual-mode migration approach



5 Conclusion

If there is one thing we can learn from the recent challenges facing public safety networks across the globe, it is that we must a **move to broadband based networks as soon as possible to reap the functionality benefits** that they provide. When doing so, we must **raise the bar for reliability**, whether in the face of traffic load or environmental conditions. We must make sure that the networks are robust in the face of new emerging cyber threats. And, we must also, **build networks that can sustain and support the next wave of innovation in applications**.

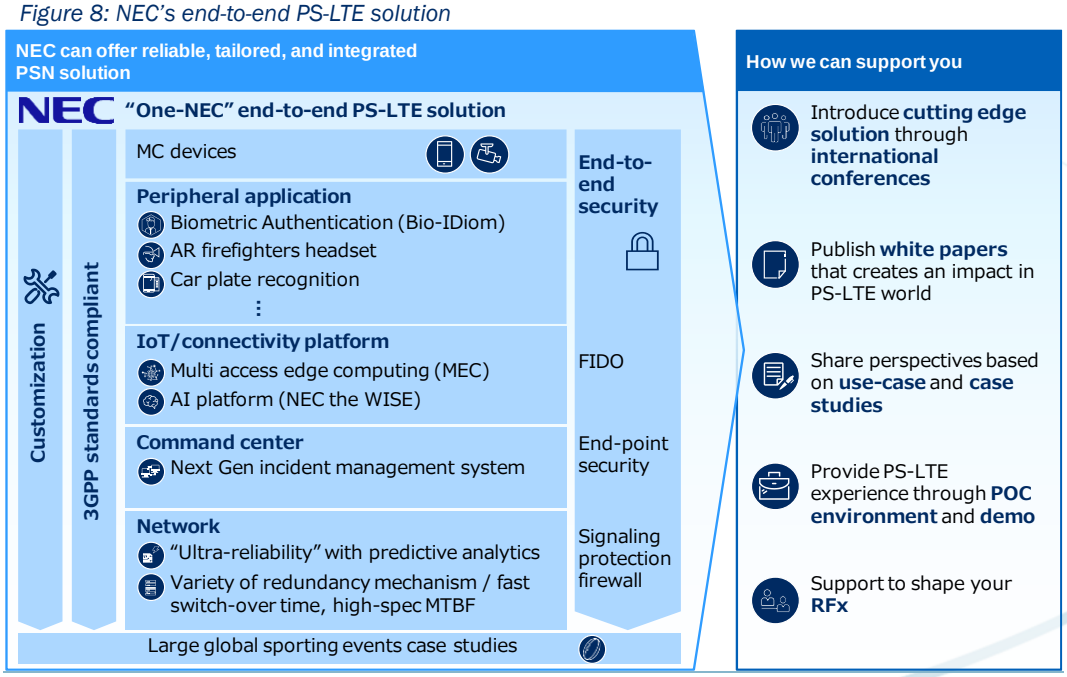
We cannot be certain about what these new innovations will look like, but we do know that there are **technology developments on the horizon**, where the network, itself, can play an important role in future applications (enabled by the way PTT is implemented as opposed to OTT applications). We also know that **capturing the full benefit of these developments will require coordinated R&D across layers that are now separate**, i.e., devices, applications, and networks.

■ ■ ■

In conclusion, we must avoid the pitfalls of the past by designing and building an infrastructure that is outdated even before it is deployed. **We must take a more holistic view of public safety networks in the context of next generation technologies**. We must look at all elements in an integrated fashion.

AT NEC – WE DO.

Figure 8: NEC's end-to-end PS-LTE solution



For more information, contact us at NEC Japan:

Email address: info-pslte@fccp.jp.nec.com

Glossary

3GPP	3rd Generation Partnership Project, the organization that defines the telecommunications standards
4G	Fourth Generation mobile communications standard
5G	Fifth Generation mobile communications standard
ACT	Active
AI	Artificial intelligence
AR	Augmented Reality
BBU	Base band unit
DoS	Denial of Service
DDoS	Distributed denial of service
EIM	Enterprise Identify Manager
EPC	Evolved Packet Core
FIDO	Global alliance for authentication standard to reduce over-reliance on passwords
GPS	Global positioning System
IT	Information Technology
IoT	Internet of Things
LMR	Land mobile radio
LTE	Long term evolution
MCPTT	Mission-critical push-to-talk over LTE
MEC	Multi access edge computing
MTBF	Mean time between failure
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OTT	Over the top
PMR	Professional mobile radio
POC	Proof of concept
PS-LTE	Public Safety – Long Term Evolution (the 4th generation mobile communications standard)
PSN	Public safety network
PTT	Push to talk
RAN	Radio access network
RRH	Remote radio head
SBY	Standby
SMS	Short message service
SMS-CB	short message service - cell broadcast
TETRA	Newer standard than Tetrapol, adopted by the European Telecommunications Standardization Institute (ETSI) as the European public safety standard.
TETRAPOL	A digital, purpose-built professional mobile radio technology for mission-critical public safety users.