THE CASE FOR DEDICATED PUBLIC SAFETY NETWORKS

WHY COMMERCIAL NETWORKS ARE NOT AN OPTION FOR PS-LTE

Table of Contents

Introduction

Given the limited ability of today's public safety networks to offer modern data connectivity and the growing need among first responders for precisely such connectivity to effectively do their jobs, most governments are looking to upgrade their current narrow-band, voice-oriented systems to broadband alternatives. These governments, comprising more than 80% of countries around the world,[1] must address the question of how best to deploy PS-LTE solutions.

The fundamental choice in designing these future networks is to what extent they will either rely on an independent infrastructure or existing commercial networks, with various potential hybrid network models in between. This decision has far-reaching implications for the cost of operating the networks, as well as their reliability and performance.

In this paper, we explore the inherent issues and tradeoffs related to this decision, and the reasoning behind our contention that only dedicated networks can provide the reliability citizens should expect and the performance first responders deserve.

The document covers:

1. The fundamental **tradeoff between commercial and dedicated networks**
2. Specific **shortcomings of commercial RAN-based hybrid network designs**
3. Our vision **for a robust architecture of the future**

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

1 The tradeoff between dedicated and commercial network

When we consider the optimum public safety network, or PSN, much of the discussion centers on whether to use an existing commercial network, or invest in dedicated network build-out. We believe that the "mission critical" standard applied in the case of dedicated networks (defined below and required in the case of PSNs), fundamentally differs from the "business critical" standard that telcos and other players require of commercial networks.

Commercial networks are built under a working assumption that a business critical standard is sufficient – in other words, that such networks will be used by consumers who have reasonable access to radio frequencies. PSNs, by contrast, require a much higher "mission critical" standard, meaning that they need to work even in exceptionally congested or severe conditions. Especially in disasters, failure of a commercial network built under a business critical standard would at a maximum lead to substantial inconvenience for users; PSN failure can mean the loss of life [Exhibit 1]. PSN, therefore, requires much higher reliability than what can typically be supported by commercial networks.

In this section, we discuss why governments are nonetheless looking into using commercial networks for their PSNs and why we believe they should not.

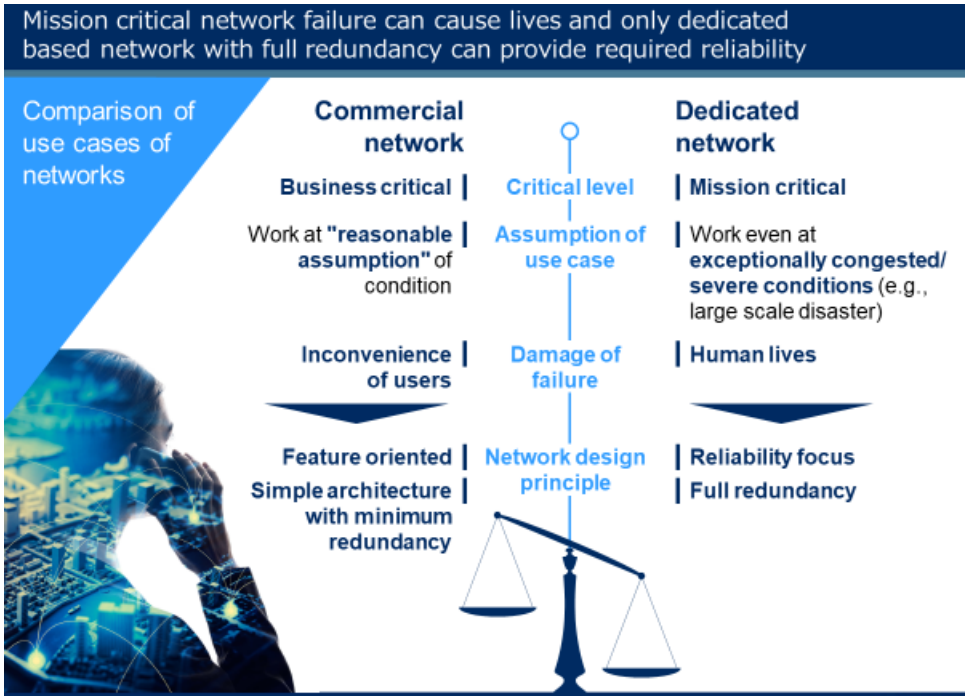

Exhibit 1: Fundamental differences between commercial and dedicated networks

The primary reason governments look to utilize existing commercial networks as a basis for their PSNs is the promise of **cost-efficiency**. PSNs leveraging commercial networks are inexpensive to establish compared to deploying a new dedicated network because they utilize infrastructure that is largely already in place. Also, by

pitting carriers against one another, the procurer can use competitive bidding to achieve the lowest possible expenditure. This savings, however, comes at the expense of reliability; **commercial networks** are far **less reliable** than dedicated networks.

Commercial networks are unreliable by design . . .

At best, commercial networks are built to live up to a **business critical** standard. The definition of business critical is very different from the **mission critical** standard in public safety; mission critical implies that the network never fails, especially when needed, while business critical suggests that the network is mainly reliable, but when it fails, it will likely do so precisely when the network is needed most.

This difference in reliability is built into the **fundamental design choices of the network**. From a commercial perspective, it makes no sense to build a network for business and consumer use that lives up to the definition of mission critical. The costs associated with it would be too high, and customers would be unwilling to pay for it, given that network failures are largely a matter of mere inconvenience. At worst, failures may lead to a marginal loss of customers (who, in many cases, are tied in by lengthy contracts anyway and will have forgotten about any failure by the time the contract is up for renewal). Furthermore, as all commercial networks tend to be similarly unreliable, the market impact is usually limited.

In a public safety network, however, the cost of failure can very well be immeasurable, as it is paid in human lives. Leveraging a commercial network for the PSN, therefore, is fraught with risk. They are historically unreliable, and time and time again, in country after country, they go down.

. . . and, consequently, often have unacceptable failures

One of the main arguments for countries to deploy dedicated networks for public safety is the reliability requirement. Commercial networks have repeatedly proven themselves to lack the required reliability. There are countless cases of failures and blackouts of commercial networks around the world, which can leave first responders without any communication whatsoever.

Just looking at some of the more populous countries in the developed world over the 12-month period from mid-2018 to mid-2019, we see a multitude of network failures that would have crippled effective emergency response, some of which are by operators that are proposed, or confirmed, to operate their nation's public safety communication on the same networks [Exhibit 2].

In just the past year, there are numerous outages of the operators in developed markets, some of which are even confirmed to run the public safety network.

Country	Operators	Time	Impact of the network outage
	orange	Jun-19	Internet network outage hit **Tours, Paris, Lyon and Nantes**
	TELSTRA	Jun-18	Disconnection lasted longer than **18 hours**
	OPTUS	May-19	Users across the country were unable to access streaming sites for more than **24 hours**
		May-19	Customers had no access to the Internet for **5 hours**
	O2	Dec-18	32 million O2 customers in UK were also hit by **25-hour outage** caused by Ericcson's software issue
	verizon	Sep-18	Outage knocks out service across US, including New York and Florida
	AT&T	Jun-19	Statewide outage in North Dakota
	CenturyLink	Dec-18	A nationwide outage knocked out **911 voice calls** in parts of the US for more than **24 hours**
	SoftBank	Dec-18	Experienced nationwide outage over 30 million subscribers for **5 hours** due to Ericsson's Core malfunction, which also occurred in other **telecom carriers across 11 countries**
	kt	Nov-18	Disruption to mobile and Internet service as well as the emergency services
	Singtel	Oct-18	Mobile service outage on 3G/4G network lasted for **3 hours**
	eir	Sep-18	Customers were unable to use 2G and 3G calls during the daytime
	kpn	Jun-19	**Knocked out the emergency number nation-wide** for ~4 hours
	TELE2	Jun-19	Network outage lasted for **2 days** impacted **emergency numbers**
	vodafone	Jun-19	Customers **across EU[1], India and Australia** were unable to access the internet
	3	Oct-19	Customers **lost internet and the ability to make calls for over 9 hours** caused while they were working in one of their data centers

1 Incl. Ireland, Italy, Germany, UK, Netherlands, Spain
SOURCE: Press search

Exhibit 2: List of network outages in developed markets from mid-2018 to mid-2019

An additional risk involves the conflicts that commercial operators face in terms of priorities, as they are primarily accountable to their shareholders, not the public. This conflict was thrown into sharp relief in the past year when an operator in North America made a commercial decision at the expense of public safety.

Situation: In August 2018, a series of deadly wildfires erupted in North America, the largest fires on record in that region, resulting in over 100 fatalities (including six firefighters) and 1.9 billion acres of land ravaged by fire.

Complication: The commercial operator truncated the firefighters' "unlimited" data plan to 1/200 of its original speed during the disaster. The constraint was lifted only after the local fire department subscribed to a new, more expensive plan.

Commercial networks particularly fail during extreme events

During disasters, the public's use of communications networks tends to skyrocket. For example, during Japan's earthquake, tsunami, and nuclear plant disasters of March 2011, the number of call attempts increased by a factor of 60 within minutes. Such networks are typically designed to handle peak spikes of just 2-3 times the predicted load [Exhibit 3].

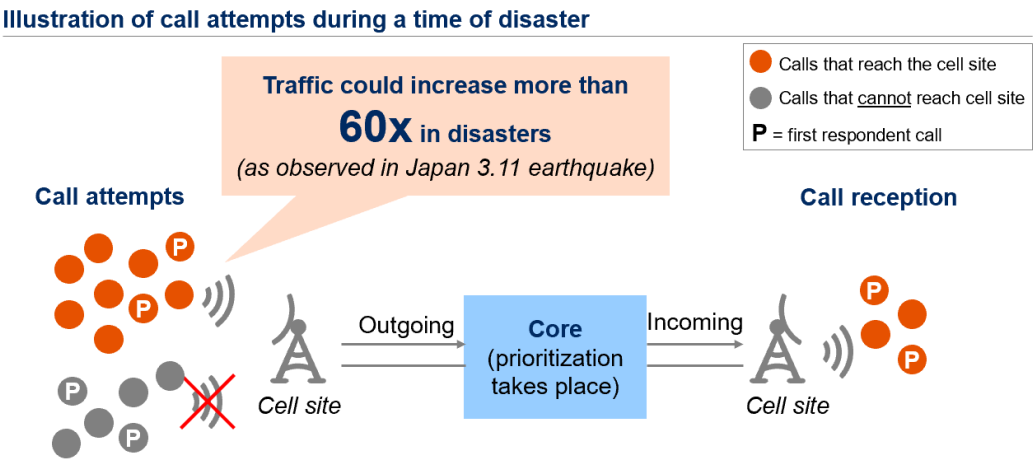

Exhibit 3: Illustration of call attempts during a time of disaster

It is a commonly held misconception that "Access Control" features of the 3GPP standard will allow operators to prioritize traffic in such a way that first responder communication would not be affected by a sudden spike in non-essential traffic. In reality, features of this nature prioritize across calls that come into the prioritization engine itself, i.e., that have reached the cell-site and been assigned a priority by the radio access network (RAN). In situations with *extreme* levels of call density, therefore, the majority of the calls fail *before* they are even able to establish a connection with the RAN. A crude but accurate analogy from the physical world would be the uselessness of priority boarding rights at the airport when you are stuck in traffic on the way there.

The cost advantages of using commercial networks are overstated

Building new networks, such as dedicated or reinforced hybrids, naturally incurs costs, but the difference with the typical costs involved in leveraging commercial networks is often exaggerated. While not an apples-to-apples comparison, the average coverage and capacity costs for commercial networks are much higher for several reasons:

A. Commercial networks, on average, operate on **higher frequency bands**. PSNs built on frequencies of 700 or below require far fewer base stations than the average density typical of commercial deployments. For instance, covering a geographical area with 700MHz compared to 2600MHz requires somewhere between the square root and the fourth root of the number of cell sites depending on the topography. With frequencies in the 400MHz range now being considered by many countries, the comparison becomes even more stark, and it is perfectly viable to cover large geographical areas with a fraction of the base station count of commercial networks.
B. Dedicated networks require **less densification** as, in most geographical areas, even under full deployment the user count is much lower than the general population or the commercial user base.
C. There are also strong **lock-in effects**. Switching the underlying network

supplier at the end of the contract is not straightforward. PSNs require the integration of specific features in the network core, radio planning has to be reviewed and confirmed, and the risk of service disruption during the switch is real.

In addition to the above, the introduction of commercial networks for PSN does not always go smoothly. One of the lighthouse cases for using commercial networks for PS-LTE in Europe has shown that the cost-efficiency of this type of solution may not always be as high as first estimated:

Situation: In 2015, a European country started a project to replace its current TETRA network with a PS-LTE network run on top of one of the commercial operators. An important part of the economic calculus was the cost-efficiency, especially factoring in the replacement, and shutdown, of the existing TETRA network.

Complications:

- As of today, the **project budget has increased by about 50%,** and the breakeven point of replacing the TETRA network with LTE has been delayed by seven years to 2029.
- Authorities have considered revisiting the approach altogether as the program has faced substantial technical and commercial risks with suppliers.
- Concerns have been raised by end users as to whether the **coverage and resilience of the commercial network will really match the current TETRA solution they depend on for their lifeline.**

Service level agreements, or SLAs, present an additional cost hurdle in using commercial networks. Existing commercial networks usually lack the quality to provide a mission critical level of reliability. As such, even when governments decide to use commercial networks for their PSN, regulators tend to ask commercial operators to agree to a higher SLA. Imposing a higher SLA, however, does not solve the problem: as the cost of upgrading the network to reach mission critical reliability is typically too high to justify for commercial use, operators tend to simply pay the fine for violating the SLA. This may increase regulator income but does nothing to enhance the service quality.

2 Design shortcomings of commercial RAN-based hybrid networks

Despite having established the clear reliability issues with commercial networks, even countries that decide to rely primarily on a dedicated network often consider augmenting it for cost-efficiency reasons by utilizing an existing commercial network in a type of **commercial RAN-based hybrid network solution (hereafter in this section, hybrid network)**.

The concept bears investigation, as it can blend the best of both worlds. But reaching this outcome depends on specific design choices; some configurations that have been put forward would lead to an even worse outcome than relying purely on a commercial network.

Hybrid networks done right can build cost efficient network

Augmenting a robust and reliable dedicated PSN by utilizing the existing commercial infrastructure makes a lot of sense in principle, given the low costs for increasing marginal capacity. It is imperative, however, to factor in the known shortcomings of commercial networks. The assumption *must* be that in the case of a severe disaster all critical communications can be handled *without any* reliance on the augmentation.

Luckily, not all first responder communication needs are equally critical, nor do they have the same bandwidth requirements. For instance, running camera feeds to facial recognition to detect criminals under warrant is bandwidth-heavy, but first responders could work without such a feature when responding to, say, a major plane crash in a city center.

To reap the greatest benefit from hybrid network solutions, we believe decision makers should:

A. Focus use of the non-dedicated network towards high-bandwidth features (for capacity relief) that are not part of the mission critical systems.
B. Ensure the technical implementation does not bring unnecessary complexity to the system as a whole, which could undermine the effectiveness of the dedicated network.

Hybrid networks done wrong can weaken a PSN by giving users a false sense of security or causing a decline in actual performance

From a technical perspective, there are many ways to create a hybrid network. Some approaches make more sense than others, but none are perfect. Specifically, there are three types of commercial RAN-based hybrid networks for which we would urge caution before pursuing [Exhibit4]:

a) Multi-commercial operator arrangements (MVNO solutions)
b) Active network-sharing arrangements (e.g., MORAN)
c) Spectrum-sharing arrangements (e.g., MOCN)

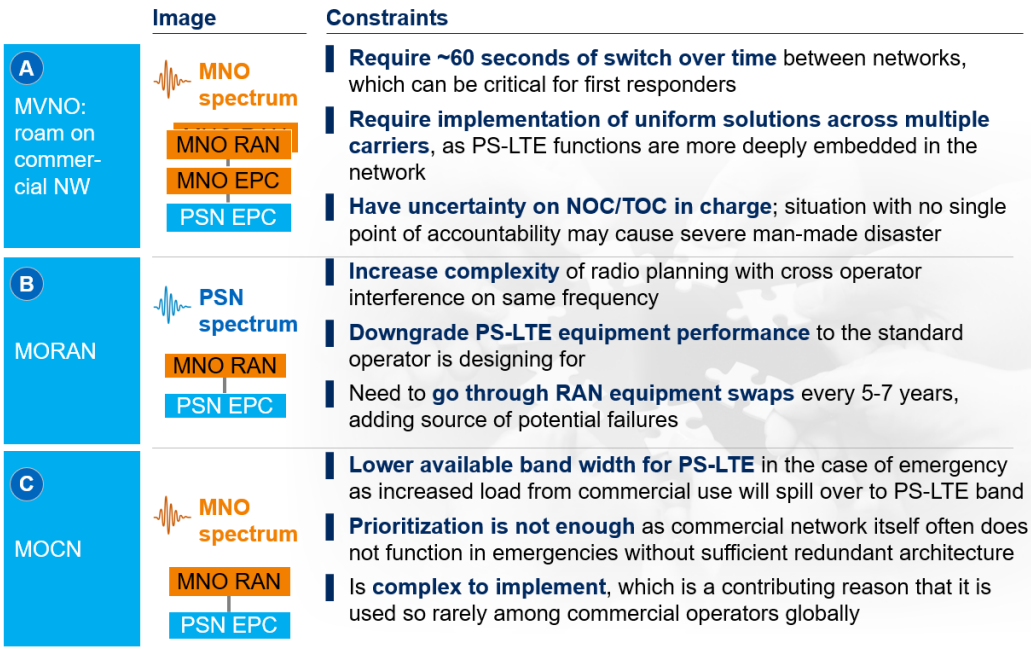

Exhibit 4: Fundamental differences between commercial and dedicated networks

A) Multi-commercial operator arrangements (MVNO solutions)

It has been argued that if adding one commercial operator to augment a dedicated network creates cost advantages, then adding more operators should increase the benefits even further. Technically, all these solutions tend to boil down to some form of MVNO solution dependent on domestic roaming.

On the face of it, a multi-carrier MVNO solution has a certain appeal. In theory, it should allow for emergency services to use whichever of the commercial networks are best performing in their physical location at a given moment. In practice, however, roaming, as a technical solution, is not especially robust. The primary issue with roaming is the **switchover time between networks**. When the device seeks to attach to a new network, the signaling to establish a connection takes time. These times vary but delays of up to **60 seconds** are not uncommon, and under particularly bad conditions it can take as much as five minutes. During this switchover time the user has no network connection whatsoever.

Switchovers are **not entirely predictable**. Temporary small dips in the main network can trigger a switchover, even though remaining on the base carrier would have resulted in only a short service disruption.

There are three additional issues, the first of which is that PS-LTE use cases differ from normal commercial use cases. Elements of functionality are more **deeply embedded in the network**, for instance MCPTT, requiring the implementation of *uniform* solutions across multiple carriers, possibly with cores from different equipment vendors. It is also important to underscore that use of these embedded services *crossing multiple commercial networks is, to date, untested in live situations.*

The second issue is the question of **who is in charge**? In other words, which network operation center (NOC) should the tactical operations center (TOC) turn to in a case of

network failure? How does the TOC know which carrier emergency services it should rely on in a certain area, and who has a service disruption that needs to be corrected? *There is no single point of accountability.*

The third issue is that the sense of security provided by having multiple operators to rely on in a crisis is fictitious. The spikes in network load associated with a disaster experienced by one operator will be experienced by all at the same time. Load and other factors that would cause one network to go down during a disaster would likely cause all others to go down as well.

For a country of large geographical area, where different commercial operators have significantly different quality of network coverage in different regions, this solution still has some undeniable benefits, at least in theory. There are few such countries, however, and we know of none that are exploring national PSN implementation.

In short, introducing more operators introduces more complexity. In telecommunications engineering, needless complexity is the mother of all preventable faults.

B) Active network-sharing arrangements (e.g., MORAN)

RAN or active sharing (MORAN) is the shared use of radio equipment between a dedicated PS-LTE element and one of the existing operators. Multi-operator active sharing, with the public safety network, binds the radio-planning of the public safety network inseparably from one commercial partner.

Although active sharing does lower costs, as BBUs and RRUs can be utilized for both networks, it also comes with problems.

1) It **downgrades** equipment performance **in the PS-LTE frequencies** to whatever standards the operator is designing for, usually considerably lower than ideal in terms of redundancy and switchover times.
2) **Equipment swaps**, which are common every five to seven years, represent a completely unnecessary but real source of potential failure while also introducing the risk that the operator will **further downgrade** the reliability of future equipment for LTE as they move customers towards 5G. Public safety networks are built to stand for decades, as has been the case with TETRA networks of the last generation, and do not require such swaps.

C) Spectrum-sharing arrangements (e.g., MOCN)

MOCN is another technological solution that is occasionally put forth for discussion. MOCN increases load tolerance somewhat as it utilizes the available spectrum more efficiently. It will not do so during a disaster, however, as the increased load from commercial use will almost undoubtedly consume the commercial frequencies and load will **'spill over'** into the PS-LTE bands, effectively lowering the available bandwidth. Actual cases proving this bandwidth shrinkage exist.

It has been suggested that **traffic prioritization** can prevent this issue, but it relies on the 3GPP notion of "access control" which, as outlined above, has its own drawbacks.

Furthermore, MOCN is **complex to implement**, which partly explains why it is used so rarely among commercial operators globally. Only a few network sharing arrangements rely on it.

3 A proposal for a dedicated network with more robust architecture

Equipment vendors that are present among commercial carriers tend to argue for the solution that suits them best, that is, the solution that maximizes their sales, their penetration among and stickiness within the commercial operators, and their utilization of off the shelf equipment. They are optimizing, in short, not primarily in the best interest of the PSN, but in their own best interest across all the networks they operate in the country. Just as the reliability of their solution tends to be exaggerated, so are the costs of the alternatives.

Our view is that the dedicated network [Exhibit 5] is the only type of network that can provide enough reliability to support PSN. While the commercial network does have its merits that they are cost-effective and already have large coverage over the land.

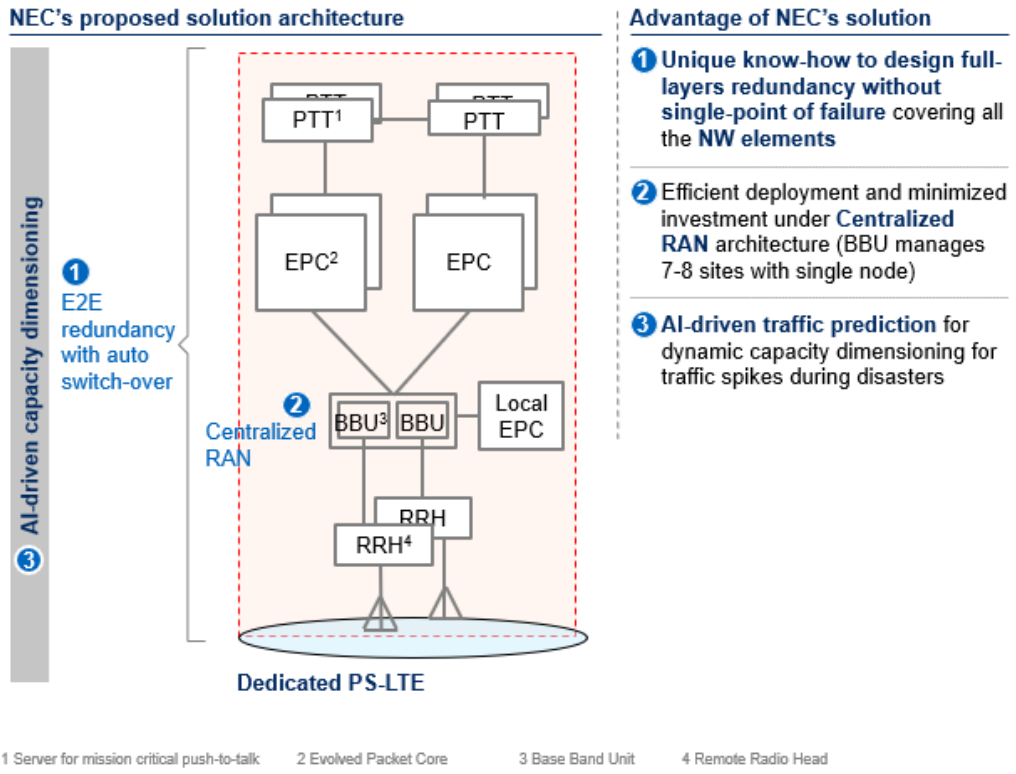

Exhibit 5: Robust dedicated network architecture

To this point, we have been discussing network types, but implementation approaches also vary. Based on our experience in building one of the world's most reliable PS-LTE networks, we have learned lessons about enhancing network reliability, and how to do so while meeting a range of conditions. For example, in cases where there are budget constraints or network coverage conditions, a PS-LTE network can potentially be supported by an existing network during the transition process. NEC can deliver a range of solutions to support these and other situation-specific needs and can be a discussion partner in supporting the process.

4 Conclusion

For any PSN to be reliable, it must primarily rely on a dedicated network with dedicated frequencies. Augmenting this network with the support of an existing commercial network can, if done right, further support the implementation process.

In summary,

1) PSNs require a **mission critical standard of reliability with a redundancy focus** as they need to function even in extreme cases where lives are at stake.
2) **Commercial networks** are designed under the lower threshold of a business critical standard; they are intrinsically **unreliable** and experience frequent crashes – even more so in disastrous situations where calls are concentrated (as in the March 2011 disasters in Japan noted earlier) and the PSN is most needed.
3) Some commercial RAN-based hybrid network options (MVNO, MORAN, MOCN) are inherently risky, as they **introduce additional unnecessary complexities** and **additional points of failure** without significantly, if at all, improving performance.

For the above reasons, critical communication should be supported through a **dedicated network**.

NEC has extensive experience in PSN development and can provide end-to-end support in migrating existing LMR systems (e.g., TETRA, P25) to next-generation PS-LTE design, including transitional phases where both networks are co-excitingly operative, which is a common concern for many of our customers. We can help develop insights by sharing global trends and serving as a discussion partner on topics ranging from optimal network models and frequency bands to LMR-LTE interoperability and network security requirements; we can deliver PoC demonstrations to showcase the promise and potential of next-generation PS-LTE; finally, we can deploy dedicated, reliable networks with cutting-edge technologies and a robust product portfolio, from backend to frontend, along with applications and security.

NEC - CAN

For more information, contact us at NEC Japan:

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


Orchestrating a brighter world
NEC