Why choose Private Digital PMR Networks over Public Networks?

DMR Association

Introduction

Public safety, utilities, public transportation, and industrial production have unique requirements for the functionality and reliability of their communication services. This white paper will assist the management decision process in choosing between private digital professional mobile radio (pmr) networks and public mobile networks.

The digital pmr technologies discussed in this white paper are trunked radio and conventional technologies. From a structural point of view, private and public networks seem to be similar. However, fundamental differences are seen when considering the unique requirements of mission or business critical applications, like public safety, utilities, public transportation, and industrial production supervision.

General Differences between Public and Private Mobile Networks

Public Mobile Network Operators (MNO) drive their business under competitive conditions with licenses granted by National Regulatory Authorities (NRA), furnished with a certain amount of spectrum allocated for 20 years on average and purchased at high-priced auctions. Usually, there is more than one public mobile network in a country.

The license conditions require the MNOs to deploy their networks within a given period of time to cover a pre-defined percentage of the national population. In the beginning, the goal of the MNOs normally is to fulfill the license conditions by first deploying mobile service in regions of dense population to maximize market share. Later they focus on revenues and are profit-driven - i.e., they try to maximize Average Revenue Per User (ARPU) and minimize cost of operation, thus commercially optimizing their businesses. Of course, this approach has a strong impact on service availability as far as location and communication capacity are concerned.

Private digital PMR networks, on the other hand, are purpose-built. They deal with severe situations within a given coverage area with defined quality properties. Their coverage is not defined in terms of population but in terms of size and shape of a required service area and expected worst case situations. PMR networks offer a functionality that fits the needs of their users and is of outstanding resilience. They provide service availability and enough communication capacity to meet the requirements under all circumstances, even during peak traffic situations. As such, private digital PMR networks are under full control of their owners and are not operated under any competitive condition.

Public Access Mobile Radio (PAMR) networks are midway between PMR and MNO, as they are based on operators which offer air-time with PMR features to private organizations. Even if they are more similar to MNO networks in terms of availability and integrity, they are much more similar to PMR networks, as they can provide all the PMR features. For this reason PAMR networks will be assimilated in this paper to PMR networks.

Mission and Business Critical Communications

Modern society depends on public safety agencies to immediately respond, utilities to securely provide electricity/gas/ water, public transportation systems to be reliable, and production companies to operate securely, especially when dealing with hazardous substances. Common to all these sectors is that failures could jeopardize human lives or put at risk assets whose impairment or loss would significantly harm society or the economy - thus all are considered to be critical. This is why utilities and public transport are also designated as critical infrastructures. In particular, e.g. Liquefied Petroleum Gas (LPG) depots, high-voltage electricity lines, and nuclear power plants (along with their fuel/waste cycle) are critical infrastructures.

Traditionally, each sector had its own dedicated radio communication network, often with exclusive spectrum allocations laid down in the frequency plan of the respective licensing authority. These communication systems are of paramount importance to the operation of a nation's public safety and critical infrastructure services and are therefore required to have particular and adequate built-in functionality, availability, resilience, and security.

Public Safety Requirements

Public safety usually comprises police, fire fighters, ambulances, and rescue services making use of mobile communications in a voice-centric manner with an increasing demand for data applications.

It is important to understand that public safety users generally work in teams, which mostly results in communication as a "talk group" sharing radio channels to update all group members simultaneously, providing a common communication platform for the entire team. Defining and redefining talk groups quickly is crucial for effective teamwork; thus it is a major requirement for public safety users.

Talk group communications may be monitored on-site in case of a major incident or by a control center which may be some distance away (dispatch mode). The control center may also record or log the conversation.

Immediate access to the communication network is initiated by using the Push-to-Talk (PTT) button addressing a particular individual or talk group with a call set-up time of less than half a second. Every communication initiated by PTT event is accompanied by an automatic identification disclosing the identity of the speaker.

Different priority levels may be assigned to mobile users or talk groups, with highest priority that can be configured to be pre-emptive Highest priority is with the emergency alert function using an alarm button at the mobile radio to indicate that immediate communication is needed.

Automatic location discovery, navigation assistance, and tracking of mobile users and response vehicles are essential for speedy dispatch and supervision by control centers.

Speech intelligibility is a key issue of audio quality. In case of fire fighters this is made difficult by respiratory equipment and noisy environments.

Handheld radios for fire fighters must be usable with gloves and should be certified IEC IP67 resistant to dust and water. Intrinsically safe radio equipment is needed when there is a risk of accidentally igniting explosive gases which have contaminated the site of the mission.

In contrast to police requirements, encrypting fire communication channels is rarely necessary.

Public safety's effectiveness is constrained by network downtime, especially in emergencies. Hence, there is a requirement for constant availability - communication services should be available at least 99.99% of the time. The networks must offer defined fallback modes in case certain elements or parts of the network become unavailable during longer crisis situations. Apart from outdoor coverage, this also comprises service availability inside buildings and tunnels, including subways. Thus, the communication service must be adequate for both voice and data independent of location of mobile users with sufficient capacity for peak loads in times and places of crisis (not just a certain minimum signal strength).

Requirements of Utilities

For reasons of simplification, the emphasis is on the requirements of electric utilities since electricity generation and distribution are the utility sector’s primary users of radio. Gas and water require a very similar but limited overall functionality.

Mobile communication for utilities likewise is voice-centric. It is the communication means for the day-to-day business of the mobile work force and is, most important during power outages, the means to facilitate fast repair missions. Reliable and resilient connectivity to PABX and PSTN is essential. Furthermore, many utilities are accustomed to duplex mode for voice communication because PABX users communicate regularly with radio users.

However, data communication for the control of supply systems is becoming more and more important. Recently in the context of Smart Grids, mobile data communication emerges for telecontrol and telemetry of electricity generation and distribution. This application is also known as Supervisory Control and Data Acquisition (SCADA) and requires low data volumes at comparably low transfer rates and high availability. SCADA as a radio service demands exceptional efforts to secure confidentiality, integrity and availability of communication.

The service territory of a utility and specific remote areas where essential infrastructures and supply sources are located determine the required radio coverage. Often, these areas are outside densely populated areas and offer low attractiveness for public networks.

Utilities want network separation to avoid having their operational communications disrupted or blocked by other users in a crisis. Thus, they prefer to own dedicated communication networks for their operations because service disruptions generate legal and commercial liabilities, especially in case of a major utility supply failure and its high impact on the economy. They require continuity of communication service with resilient communication networks of very high availability with low latency for data communication.

Requirements of Public Transportation

The diversity of public transportation applications is greater than the diversity of public safety and utility applications. Public transportation includes buses, tram, light rail, metros, railways, sea and airports, road maintenance services, and various assemblies of sensors and actuators. A well known example for the latter is the traffic light as an urban traffic management tool, regulating the

road traffic with the option of prioritizing certain vehicle classes (e.g. police cars, fire engines, ambulances, buses). For all this, mobile communication serves as an enabling technology.

Within public transportation, voice and data communication are of equal importance, although in some applications data is used more often. This includes location data and important status information of vehicles that helps mass transportation operators to manage their schedules. Subsequently, derived from this, Real Time Passenger Information (RTPI) is provided to indicate bus, tram, or train arrival times. Most current data applications for public transportation are characterized by low data volumes and low speed requirements. However, they represent a strong portion in exploiting the capacity of the mobile communication network.

A mobile communication network must be able to assign functional dial numbers to vehicles, so that they may be called based on their organizational numbering scheme. This assignment ensures independence of vehicles and mobile equipment in use and is also independent from deployment of staff.

This applies also for the return path to a control center - a call to the dispatcher in charge is always routed to the right person, no matter where the vehicle currently is located. The same approach is found at airports when teams around an airplane are called based on the flight number and a suffix describing the working team, e.g. catering, cleaning, and fueling. This is known as object-oriented calling.

The mobile communication network must facilitate a voice group call to all mobile users in a certain area. Secure talk group services are needed similar to those of public safety users. Mobile users and control centers must be able to broadcast messages throughout the service area.

The network must permit different priority and pre-emption rights, up to an emergency call with fast access to the communication network.

So what is Common among Public Safety, Utilities and Public Transportation?

As could be seen from the discussion above, the functionality in use throughout all three sectors is more or less identical. It is more in some applications where they differ and in the share of voice and data exploiting the capacity of the mobile communication network.

For the sake of completeness the functional requirements as described above are summarized and presented in the following table:

Voice Communication	
Group Call	The method of voice communications that provides communications from one-to-many members of a group or team. Theoretically, the number of members of a group is unlimited.
Individual Call	The individual call permits communication between two parties and is thus a point-to-point connection. Parties may be mobile stations, dispatchers in control centers, and telephone extensions.
Dispatch Mode	The dispatcher in a control center manages and supervises the mobile user community via a mobile communication network.
Push-to-Talk (PTT)	The fastest way of voice communications - the speaker pushes a button on the radio and transmits a voice message addressing a particular individual or a talk group. On release of the Push-to-Talk button the radio returns to listen mode.

Emergency Alert/Call	An alarm button when pushed indicates that the user is in an emergency and requires immediate access to the communication system. It is therefore given the highest level of priority. It may also be pre-emptive.
Fast Call Set-up	The call set-up time must be less than half a second.
Late Entry	For mobile users who were out of reach during call set-up, or missed it because of other reasons, this function facilitates attending the group call.
Direct or Talk Around	This mode of communications provides mobile users with the ability to communicate unit-to-unit when out of range of a wireless network. Also known as Direct Mode Operation (DMO).
Full Duplex Communication	A simultaneous two-way transmission in both directions, i.e. both parties may talk at the same time. This is the preferred use for communication of mobile users with Private Automatic Branch Exchange (PABX) extensions and interconnections to the Public Switched Telephone Network (PSTN).
Talker Identification	This provides the ability for a user to identify who is speaking at any given time (e.g. showing who has pushed the PTT) and could be equated to caller ID available on most commercial cellular systems today.
Audio Quality	This is a vital ingredient for mission critical voice. Voice normally must be understood without repetition (speech intelligibility) and the talker should be identified by the listener.
Encryption	Encryption serves to secure information against eavesdropping and unauthorized talkers, thus safeguarding privacy of voice communication.
Data Communication	
Status Code Messages	Status codes are pre-coded text messages which replace routine voice messages (e.g. "arrived at scene").
Short Data Messages	These are messages of arbitrary content, usually not longer than 100 characters.
GPS Locationing	Geo information is periodically submitted about location and status of mobile users in the field. Also known as Automatic Vehicle Locationing (AVL).
Database Queries	Retrieving information about license plate numbers and hazardous materials transportation are both examples for database queries.
Miscellaneous Communication Functions	
DGNA	Dynamic Group Number Assignment, one or more talkgroup numbers may be assigned dynamically to a mobile station.
Functional Dial Numbers (Object-oriented)	Dynamic assignment of a functional dial number to a physical address of a mobile radio. May address a bus, a train or a functional team at an airport (to name a few). When used to address a person results in calling this individual independent from using a certain mobile radio.
Talkgroup Subscription / Attachment	A mobile station may request the site under which it is working to be subscribed or attached to a particular group of interest.

Apart from these functional requirements, there are some features or properties mobile communication networks must fulfill for critical communications of all three sectors.

Most important is the availability of service that is rated to range between 99.9 to 99.999%. "Five nines" stipulate extremely high reliability and resilience of a mobile communication network and allits auxiliary equipment, i.e. switches, base stations, power supplies, interconnection links, antennas, feeders etc.

Furthermore, it is a must that integrity of communication regarding interconnection and radio links is not jeopardized. Otherwise voice and data communication would be faulty, with possibly severe impact, especially as far as data communication is concerned.

Finally, confidentiality of communication is a major requirement throughout all three sectors.

Availability of service, integrity, and confidentiality of communication thus are key essential requirements of mission and business critical communications.

Vulnerability and Threats

Disruption of availability may occur caused by power outage, hardware failure and line disconnection or, for example, by interference directly affecting a microwave link. The reason for that may be a technical failure, but as well may be found in negligent behavior of technical personnel or even in intentional damage by others.

Hurricane Katrina:

The majority of service outages were due to a lack of power and connectivity to the wireless switch. It took one week to restore 80% of the cell sites of public networks (Source: FCC).

We all know about natural and man-made disasters affecting and challenging availability of mobile communication services. There are natural disasters like earthquakes, tsunamis, winter storms, hurricanes and floods, and man-made disasters like airplane crashes and railway accidents, terror attacks and acts of sabotage.

All these situations can result in heavy congestion in public networks when many people try to make calls at the same time at the same spot. However, congestion can already be observed during major sport events, traffic jams and other occasions where a huge number of people come together at a small area.

Complete congestion at a company's event:

There was a complete loss of wireless data connectivity at Microsoft's annual company meeting at Safeco Field in Seattle when tens of thousands of highly connected employees gathered together in a single place (Source: ENISA).

It even may lead right up to a complete loss of service availability in case of a catastrophic event with subsequent power outage of few minutes up to one or more hours.

If technical failures in transmission or radio links occur, voice communication may become unintelligible and, for data communication, control information or measured values may be compromised.

When using plain, i.e. non-encrypted transmission, data contents and address information may be identified and understood. Therefore, a plain transmission link may favor an intentional manipulation.

Private Digital PMR Networks vs. Public Mobile Communication Networks

So far, general terms were used describing mission and business critical communications. Here now a distinction with regard to functions and features between private digital PMR networks, hence dedicated PMR networks, and public mobile communication networks (including PAMR) is investigated. The result of this comparison is illustrated in the following table.

It should be noted that voice communication in public networks is telephony-like communication. That is, individual call and duplex is included but no fast call set-up and no group call. Group calls can only be simulated by a conference call which again is in contradiction with fast call set-up and very limited in the number of members. This applies also to the PTT and the late entry function. Additionally, mobile terminals in public networks always need the network to establish a communication link, thus there is no DMO.

Function & Feature	PMR Network	Public Network
Group Call		
Individual Call		
Dispatch Mode		
Push-to-Talk (PTT)		
Emergency Alert		2
Fast Call Set-up		
Late Entry		
Direct or Talk Around (DMO)	1	
Full Duplex Communication		
Talker Identification		
Audio Quality		
Status Code Messages		
Short Data Messages		7
Data Applications		3
DGNA		
Functional Dial Numbers (Object-oriented)	6	
Talkgroup Subscription / Attachment		
High Availability		
Integrity		4
Confidentiality (Encryption)		5

	Function or feature is available
	Function or feature is not available
	Function or feature is only implemented to a limited extent

	For these function and features full control over the network is required, in terms of back-up power, redundancy, capacity, encryption and applications

Furthermore, the numbers given in the table require some explanation:

1. DMO is a special mode of operation and requires setting up a mobile radio accordingly, i.e. to manually switch to this mode of operation.
2. Emergency calls in public mobile networks address only the usual national emergency dial number, e.g. 911 or 112. In PMR networks, however, a mobile user must have a choice of different dial numbers depending upon the severity and the needs of the organization.
3. Data applications, although basically feasible in a public network, are constrained because of confidentiality reasons. Routing of data is done via the Internet.
4. Integrity cannot be maintained, e.g. in case of a failure in a transmission link. This requires redundant interconnection for another transmission link to take over which in public networks normally is avoided because of cost reasons.
5. Although there is an air interface encryption at base stations of public networks, this does not secure end-to-end confidentiality.
6. Functional dial numbering as a kind of indirect addressing requires access to the subscriber database of a network. This usually is not accepted by MNOs.
7. SMS feature works with store & forward and there is no guarantee for immediate reception.

High availability for mission critical communications, i.e. the "four or five nines", can only be achieved when users can influence the architecture and implementation of the mobile communication network. Thus, they need to be network owner to have full control over all properties that determine availability. This is best achieved by a dedicated, private digital PMR network.

Essential for high availability is power back-up with a duration of up to 72h. This is in line with redundancy measures, e.g. redundant switching subsystems (hot stand-by) and redundant transmission links between switches and base stations. In case of failures, service is taken over automatically by the spare subsystem and by the alternate transmission paths, respectively.

Capacity and radio coverage of a dedicated PMR network can be planned to avoid congestion and to ensure communication service where it is needed.

Considering the functions and features as presented and compared in the table above, only private digital PMR networks can fully meet the requirements of mission and business critical sectors, such as public safety, utilities/industry and public transportation.

Digital Standards in PMR

Major digital PMR standards with global spread and good market penetration are TETRA, P25, and DMR, all of which are public standards created and published either in Europe or North America.

The standardization bodies are the European Telecommunication Standards Institute (ETSI) and the Telecommunications Industry Association (TIA). The process of writing a standard is driven by the industry and interested user groups or organizations, like public safety, utilities, and public transportation. This is an excellent prerequisite for these standards to be suitable to communication needs of critical infrastructures. In this way Terrestrial Trunked Radio (TETRA), Digital Mobile Radio (DMR) and Project 25 (P25) were created.

Actually, all digital PMR standards meet the required functions and features as presented above. Except TETRA, they are specified for both trunked and conventional radio systems with distinct spectrum requirements. The following table illustrates the differences of general properties of the respective digital PMR standards.

	TETRA	P25	DMR
Standardization body	ETSI	TIA	ETSI
Trunked system	yes	yes	yes
Conventional system	no	yes	yes
Direct Mode (DMO)	yes	yes	yes
Channel access	TDMA (4-slot)	FDMA, TDMA (2-slot)	TDMA (2-slot)
Frequency ranges	380-450/800MHz	150 - 800MHz	70 - 900MHz
Radio channel bandwidth	25kHz	12.5kHz	12.5kHz
Effective (equivalent) communication channel bandwidth	6.25kHz	12.5/6.25kHz	6.25kHz
Power efficiency	low	high	high
Physical footprint at sites	high	medium	low
Possible traffic density	high	low, medium	low, medium
Ease of migration from analog, equipment re-use	low	very high	very high
Simulcast capability	no	yes	yes
Price level of systems	high	very high	low, medium
Price level of radio units	low	high	low

Cost Considerations

At an early stage of the planning process to implement a private digital PMR network, you have to decide which technology to deploy. The discussion so far has not revealed a substantial difference in functionality among TETRA, P25, and DMR as required by the three sectors.

Obviously, other factors with a direct impact on Capital Expenditures (CAPEX) and Operational Expenditures (OPEX) are better suited to take a decision.

When migrating from an existing analog to a new digital PMR system, very often the allocated frequencies may be retained or new channels are within the same band in close spectral vicinity of previously used frequencies. Thus radio coverage is expected to be the same or nearly the same with the new digital system, i.e. sites may be re-used as well as a lot of expensive equipment like

combiners, antennas, RF cabling etc. Also the number and associated cost of the radio links to interconnect radio basestation has to be carefully taken into account when migrating from analog.

Since P25 and DMR terminals are available in a wider range of frequency bands, chances are high that initial investment can be smaller due to repurposing above mentioned equipment.

P25 and DMR also have the advantage that, when migrating from an existing analog simulcast to a new digital PMR system, the same simulcast system architecture can be maintained, without the need of finding out and managing new different frequencies.

Frequency allocation determines the number of base stations needed to provide radio service for a certain region. In general, lower frequencies up to 150MHz are better suited than higher frequencies to cover larger areas with fewer transmitters. This again favors P25 and DMR.

Finally, it is the general price level that affects the decision for a digital PMR technology. This, together with a favorable frequency allocation, makes DMR the PMR technology of choice, offering lowest capital expenditures.

Looking at cost of operation, there are spectrum license fees, electricity expenses, air conditioning and physical footprint at sites, and recurring maintenance efforts, to name the most important cost factors. While license fees and maintenance efforts do not differ significantly, site rental and electricity expenses including air conditioning may drive cost differently. DMR here again is well suited because of its low physical footprint and its high power efficiency.

Conclusion

Private digital PMR networks for mission critical communications are purpose-built to deal with severe situations within a given service area under defined quality properties. Thus they are designed for high available ("four to five nines") utilizing power back-up and redundancy measures. Integrity and confidentiality of communication is of significant importance, especially for data applications like SCADA. All these features are under full control of an operator or owner of a private digital PMR network.

Special emphasis regarding their functionality is on group communication and fast call set-up with Push-to-Talk service. Emergency alerts are calls of highest priority and instantaneous access to the communication network. Furthermore, some useful and required applications exploit direct access to internal data bases of the PMR network.

As discussed above, in contrast to private digital PMR networks, public mobile networks cannot provide the features and functions which are suitable for mission and business critical communications of public safety, utilities/industry and public transportation.

Cost considerations including CAPEX and OPEX vary when comparing the dominant PMR technologies, TETRA, P25 and DMR. Under certain conditions, it is advantageous to make DMR the technology of choice for deploying a private digital PMR network.

About the DMR Association

The DMR Association is focused on making DMR the most widely supported 21st Century digital radio standard for the business world. Through a combination of interoperability testing, certification, education, and awareness, the Association seeks to ensure that business buyers of today's digital radio technology gain ongoing value through the competition and choice derived from an open, multi-vendor value chain.

DMR
DIGITAL MOBILE RADIO ASSOCIATION

www.dmrassociation.org