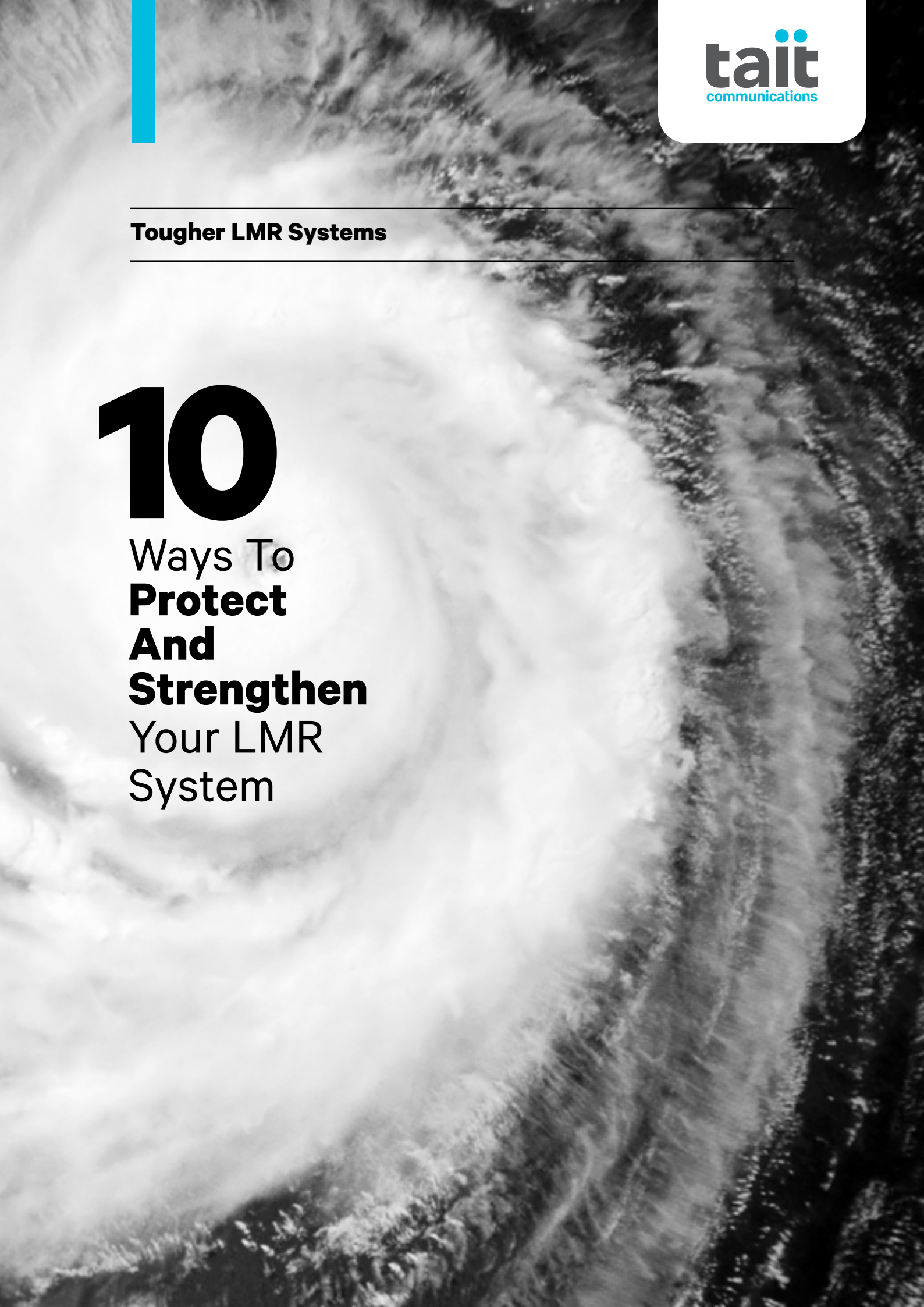


tait communications

Tougher LMR Systems

10 Ways To **Protect And Strengthen** Your LMR System

Ten essential attributes every radio system operator needs to understand, to boost the integrity of their new, or existing, LMR system.

contents

How do we qualify tougher LMR systems?

By the ability to maintain critical communications in the face of technical, physical, security or human challenges and threats.

This guide investigates every aspect of wireless communications, and considers how operators might make their LMR systems more resilient.

This is important because tougher, more robust communication supports your stakeholder expectations, protects your communities, reduces risk of costly communications outage and allows more efficient use of increasingly-constrained resources. And it gives your workers the confidence to perform their duties more effectively, knowing that support is at hand whenever they need it.

The advice and recommendations given here are not confined to a particular industry, a specific technology or manufacturer. Rather, this is a series of expert guidelines and ideas that LMR system operators might consider, weighing them up against the perceived risks they face, and the cost to implement.

Developing a deeper understanding of the technical challenges and the possibilities to improve creates more informed conversations with your consultant, vendor or local provider.

When upgrading to a new LMR platform, many decisions impacting on the toughness of your new system will be made at the design stage. However, there are still numerous cost-effective operational decisions that can positively influence your existing communications system.

Want to learn more?

Visit the P25 Best Practice website
www.p25bestpractice.com

See the case studies on the Tait website
www.taitradio.com/clients

Check out the latest articles in Connection magazine
www.taitconnection.com

1. Technology choice

A radio system is a considerable investment which may have a decades-long lifespan. Operators must ensure that their choices allow their communications to mature and adapt, as their needs and the available technologies evolve.

Open Standards

Genuine open standards bring real advantages to operators, guaranteeing choice, lowering costs and improving communications. Because they are non-proprietary, they are not under the control of any one vendor. And an increasing choice of certified vendors brings down prices, improves technical quality and avoids the risk of being locked in to a sole supplier.

Developed with the active participation of radio vendors, digital radio standards are dynamic and expanding, driven by evolving needs in sync with other digital technologies such as computer networks and VoIP.

For LMR system operators, this means:

- getting the best from your available radio spectrum,
- communicating more efficiently within your organization and with other networks ,
- a competitive market with many different manufacturers and vendors participating,
- technology platforms that are easy to use.

Interoperability

Interoperating securely with other organizations or agencies – sheriff, fire, hospitals, police – cannot be successfully achieved with analog equipment, without sacrificing security.

System level interoperability

Ideally, equipment designed and produced to a standard by one vendor will interoperate seamlessly with the same standard equipment from another vendor. However, there is often a difference in interpretation of a standard, and vendors may also add proprietary features not covered by the standard itself.

When choosing a vendor, look for standardized interoperability test procedures, and carefully scrutinize certification documents to avoid incompatibilities. For example, the P25 Compliance Assessment Program (CAP) provides independent compatibility testing that certifies standards compliance between equipment manufacturers.

Interoperability for mutual aid

Radio systems can operate with differing levels of interoperability, depending on priority and need. For example, Public Safety Task Forces will need the highest level, while routine operations require less interoperability - from sharing systems to simply swapping radios.

In a collective response to a catastrophic accident or disaster – wildfires, earthquakes, hurricanes, aircraft crashes – tactical communications between groups will be required at some level between public safety, utilities and local bodies and independent organizations.

Trunked or conventional?

One of the barriers to transitioning to a digital trunking platform is that they are often perceived as complex and expensive. As a consequence, some operators select the familiar, conventional technology when upgrading. Since there is a lower initial CAPEX investment, a conventional system's upfront cost may indeed be less. However this does not take account of the considerable long term financial and operational advantages of a trunked system.

» The increased spectral efficiency of current digital trunked systems creates a platform for dedicated digital channels, future-proofing communications as organizations become increasingly dependent on data transmission alongside their LMR voice systems.

» Multi-channel trunked radio sites provide inherent protection from channel failure; if a channel goes down, the remaining channels will automatically adjust to maintain normal trunked operation. Traffic handling capacity will be reduced, but radio users don't need to take any special action to maintain communication, as the channel controller always selects a channel from those available. Users will normally be unaware of the failure, so they can continue to carry out their duties without interruption.

Dispelling the complexity myth

Trunked radio systems are more technically advanced and therefore they may seem more complex. However, to the operator and the user, most of this complexity is concealed and automated by the trunking controller which controls the system. Once installed and configured, on a day-to-day basis a trunked system is demonstrably less complex, less demanding of your technical resource and more accessible to your workforce.

Traffic is managed and automated to ensure smooth allocation of channel resource, optimizing channel capacity, accommodating more users on fewer channels (compared to conventional systems). Private communications with talk groups, authorized system access and encryption options protect your communications from eavesdroppers.

Planning for the future

Every technology decision needs to prepare you for increasing data applications that will influence how you operate in the future.

Currently, the most basic application remains effective voice communication, but now mobile applications share information, video and text between the field and the back office, often simultaneously sharing different information with multiple operatives. A new generation of field workers demand the choice of durable, smart mobile devices to gain immediate access to this rich source of information.

This brings a new set of challenges for operators, including:

- the use of personal smartphones and tablets - Bring Your Own Device (BYOD),
- policies and SOPs that define and enforce mobile device use,
- vulnerabilities and security issues associated with mobile devices,
- finding, developing and using appropriate applications on mobile devices,
- managing data usage to avoid budget overruns,
- encouraging user adoption of applications and processes.

2. System design

Carefully considered and robust system design choices will protect your organization's communications on a daily basis, and prepare you to meet future communication needs.

Coverage

Coverage dictates the number and location of your radio sites. Together with frequency availability and traffic patterns, coverage decisions will determine where, when and how well your people can communicate, so they are fundamental to the strength and reliability of your system.

Defining coverage needs

For most systems, it is insufficient to define uniform coverage requirements across your entire service area. Typically, organizations have areas that require special consideration:

- critical use – key roads, prisons, courthouses, hospitals, refineries, critical infrastructure
- high population density - urban areas,
- challenging terrain – mountains, canyons, forests, shorelines
- challenging construction – significant buildings with "dead spots", urban canyons, tunnels

Map your entire geographical area to identify the locations with specific coverage level challenges or requirements.

In-building coverage

At the system design stage, you will identify where in-building coverage is needed. You can specify a uniform signal level in the most critical areas, assuming it will be sufficient in all buildings. Test signal strength from inside the buildings, using the signal from desired existing sites or temporary reference transmitters.

Alternatively, you can identify specific "must cover" buildings and place the burden of engineering on the vendors to provide this performance.

Measuring coverage

There are many ways to measure coverage performance. For example, Delivered Audio Quality (DAQ) is the most common signal quality measure, together with predicted reliability – the percentage of coverage area where the signal quality meets (or exceeds) the DAQ.

A widely-accepted coverage objective is DAQ 3.4 over the entire service area. This is defined as "speech understandable without repetition, some noise or distortion present". To specify a lower DAQ may require excessive speech repetition, while a higher value may require a prohibitively high level of infrastructure investment.

A common reliability standard is 95%. This means that you can expect a signal of DAQ 3.4, 95% of the time across 95% of your coverage area.

Coverage requirements and coverage acceptance test plans deserve great care and respect. The processes, tests, parameters and vocabulary are well defined in the TSB 88 standards, maintained and updated by Telecommunications Industry Association (TIA). Reference to this standard will minimize the risk of misinterpretation of either your RFP or vendors' responses.

Backhaul

The backhaul network interconnects your sites and control centers, and is the "big ticket item" on any communication system list. Include protection measures such as multi-path routing, ring structures and duplicate bearers to guarantee high system availability.

» Consider resilience in natural disasters. MiMo (multiple input, multiple output) linking is an alternative to wireless backhaul that has proven stability when microwave may be knocked out of alignment.

» If you are using your own microwave or fiber network, set up built-in monitoring to trigger alarms/ switchovers when transmission parameters are compromised.

» If your backhaul is provided by a third party, you need to include monitoring as part of your service agreement, with clearly identified performance parameters.

Paradoxically, even though backhaul service providers often use sophisticated technologies, they do not operate in a mission-critical environment, and backhaul failures commonly affect mission-critical radio systems, especially dispatch. Your regular LAN isn't mission-critical; you need dedicated links whether fibre or wireless.

Probably the best argument for a mixed topology solution - typically fiber and microwave – is to provide the redundancy that ensures the greatest LMR system resilience.

Redundancy

Redundancy refers to duplication of system components (or their functions) to strengthen the system in the face of failure or threat. It is an important aspect of system design, balancing your needs with a complex mix of geography, perceived threat, regulation, and budget.

Virtually any component of your LMR system can be duplicated, but here are two common examples.

1. Duplicated/decentralised control centre

Duplicating your control center function can protect against the loss of a dispatch facility due to fire, attack or a need to evacuate. You can specify a fully-redundant back-up center, or spread control between two (or more) centers in different locations. With good design, any centre can take up the load from a disabled central control center when needed.

2. High availability

Protection from server failure is critical, and will impact on the number and location of servers included in your system design.

Server redundancy in IP-based radio comms systems may involve basic main/ standby arrangements, but multiple servers in a geographically-diverse configuration can further protect your communications against failure or total loss of facilities. In this configuration all servers share the day-to-day handling of radio traffic.

If a server fails, or is isolated due to link loss, the remaining servers can step in to provide continuity of communications.

3. Major Events and Emergencies

This is when your system and your people must perform at their most effective, often at peak capacity and for extended periods of time. You need to invest enough to stay on air, ensuring power to your sites throughout.

Sizing your system for "The Big One"

A thorough risk analysis needs to be carried out periodically with a trusted consultant, vendor or advisor, but there are some guiding principles for planned events (such as sports events and political conventions), unexpected emergencies and natural disasters.

One simple rule is that your system capacity should be roughly three times your normal weekly "busy hour". Traffic statistics or data logging records will give you an indication of what that figure is.

However, a small rural organization is unlikely to need that much capacity regardless of circumstances – they may have few users and emergencies may be less complex, with potentially less impact. On the other hand, an urban area in an earthquake zone, with commercial centers, sports and education facilities and transport hubs may justify more than the "busy hour x 3" capacity rule.

Planning

Whatever sector or industry you operate in, planning for critical events on a daily basis is much better than figuring it out when you are under duress!

To predict emergency coverage and performance requirements, look first to local history – are you at risk from floods, hurricanes, forest fires, blizzards, or earthquakes? You also need to plan for unforeseeable events such as terrorist attack, plane crashes and civil unrest.

Here are ten points to consider.

- Disaster planning must limit access to critical users only. You will not have enough channels in extreme situations.
- Identify, protect and prioritize critical user groups in advance, and build them into your talkgroup structure.
- Define your interoperability needs – who needs to talk to whom?
- When will you use encryption? Can you communicate effectively with necessary agencies and groups?
- Estimate how long different disaster scenarios might leave you without power. You may have to be independent for 72 hours or more, without power, fuel or support.
- Consider investing in transportable systems that can be rapidly deployed.
- Prepare and maintain a cache of radios that your mutual aid partners can locate and use.
- Keep cached radios programmed, maintained and updated with the rest of your fleet – don't discover this has not happened under pressure.
- Train and practice simulated emergencies at least annually.
- Ensure all your procedures are thoroughly documented in electronic and hard copy formats, easy to follow and easy to find by everyone who might need them.

Power at sites

One of the biggest risks to your communications is also one of the simplest. Statistically, the most common cause of communications failure is power at your radio sites. Backing up your power supplies with dual redundancy can prevent communications outages during weather events, particularly where towers are at elevation, remote or inaccessible during winter. Remember that a power outage may also mean your fuel supplier may not have power to pump fuel, so ensure backup supplies on site.

Performance

While your investment depends on location and risk assessment, there are some basic principles you should build in to your day-to-day planning to maintain communications in any event.

- Eliminate single points of failure at system design stage.
- You will lose power to your system – plan for it with dual redundancy (AC then battery then generator).
- Estimate how long different scenarios may leave you without power.
- Invest enough to stay on air through critical events, ensuring power to sites throughout.
- In a major disaster, telephone systems (especially cell phone systems) frequently fail.
- Plan for a scenario in which your computer systems are not available.

Site equipment

Even with the best planning, you may be without some sites in a disaster. Good planning and design can mitigate the effects of this on your communications.

Remember, a generator can take five to seven minutes to fire up, which may leave workers without communication at a critical time. If the power is out, utilities and propane companies may not have power to pump fuel.

Coverage and capacity

What will happen to your communication if you lose a site? Some systems use geographically-distributed back-up sites. Others over-provision the sites so that no important area of operations is covered by just one site. While this is highly recommended, it is expensive and creates its own technical challenges, especially in multicast systems, requiring finely-tuning roaming performance of subscriber units.

In every case, you need to limit traffic on your system to those who need to be involved. Emergency plans should include means to cut off "roamers" and anyone who does not need to participate. Allowing people to monitor activities while they are scanning may mean additional groups will load. This may choke your system.

Be prepared to completely isolate a site in emergency, especially on larger multisite systems as it will likely improve remaining capacity.

Interoperability

The only processes that will be effective in an emergency are those that are well known to your users. Expensive patching devices, ISSI (Inter-Sub-System Interfaces) and extra groups or channels will not help unless users understand how to take advantage of them.

Keep processes simple and make sure all your users are well trained. Avoid spending large sums of money on high tech devices - the best solutions may be operational.

Interoperating with other organizations

Planning for critical event interoperability with partners is a daily task, so that you are prepared for rapid deployment. You need to establish common process and technology with those you need to work with in a disaster.

- » Define the complexity of your interoperability needs - who will need to talk to whom.
- » Build critical user groups into your talkgroup structure.
- » Keep procedures as simple as possible as you may not have access to your full system in an emergency.
- » Protect capacity by prioritizing and limiting who will talk, in advance. Allow only critical groups to operate.
- » Identify the need for unencrypted interoperability channels for external agencies.
- » Use transportable systems and portable repeaters if possible.
- » Consider storing the configuration files for radio models used by your interoperability partners so you can interoperate at every level.

A recent addition to the P25 standard is ISSI (Inter Sub-System Interfaces). Implementing ISSI on your system allows you to connect your LMR system to other radio systems. This is invaluable for interoperability, but it does require close cooperation, so that all agencies concerned have the same expectations, processes and configurations.

Procedures and Training

It is very difficult to predict all emergency scenarios and prepare for every eventuality. However, being well prepared for the most obvious or most critical ones may be sufficient. Involving a large, cross-functional team in designing your emergency SOPs and then practicing the various scenarios regularly are important to your overall preparedness. Training for different scenarios should include procedures for reduced communication capacity.

Your users need to know how to interoperate with others in an event, so you should train with your interoperability partners. While this clearly includes your mutual aid partners and neighboring agencies, you may need to include transit, schools, municipal teams, Red Cross, National Guard and hospitals. Everyone needs to know how to interoperate before they need it.

Your people need to train with the equipment, so they know what to do in an emergency – including training them to stay off their radios, unless they urgently need to communicate.

A major benefit of training and regular drills is to identify weaknesses in your equipment, procedures or people, which you then have the opportunity to improve. Reviews and debriefs after training, drills and real events are invaluable and can save lives in the future.

While it can be difficult to justify the time and cost of extensive training programs, multi-agency, multi-discipline training has the advantage of shared funding, with each participating agency bringing their own training budget to the event.

- » Factor in the roles of other communication technologies during events.
- » Train everyone with the equipment they will use in an emergency. New or upgraded equipment requires fresh training.
- » Train your radio users to stay off their radios unless they need to communicate, and empower dispatchers to turn off non-priority talk groups during events.
- » Uncontrolled interoperability can consume valuable bandwidth - establish common process and train users in it.

Technical solutions

While your system design should provide a high degree of peace of mind, there are some event-specific approaches you can take to strengthen your communications in the event of a disaster.

COWs (Comms On Wheels)

Extreme weather events can indiscriminately put communication sites or their linking out of action. A COW (Communication on Wheels) trailer or truck with its own repeaters, antenna and linking capability can provide temporary communications in an affected area. Adding a small, rugged Private Broadband LTE system with a form factor can include high speed data.

Offsite control

IP-based console systems can manage your dispatch operation remotely, away from the normal control centers – wherever a network connection is available.

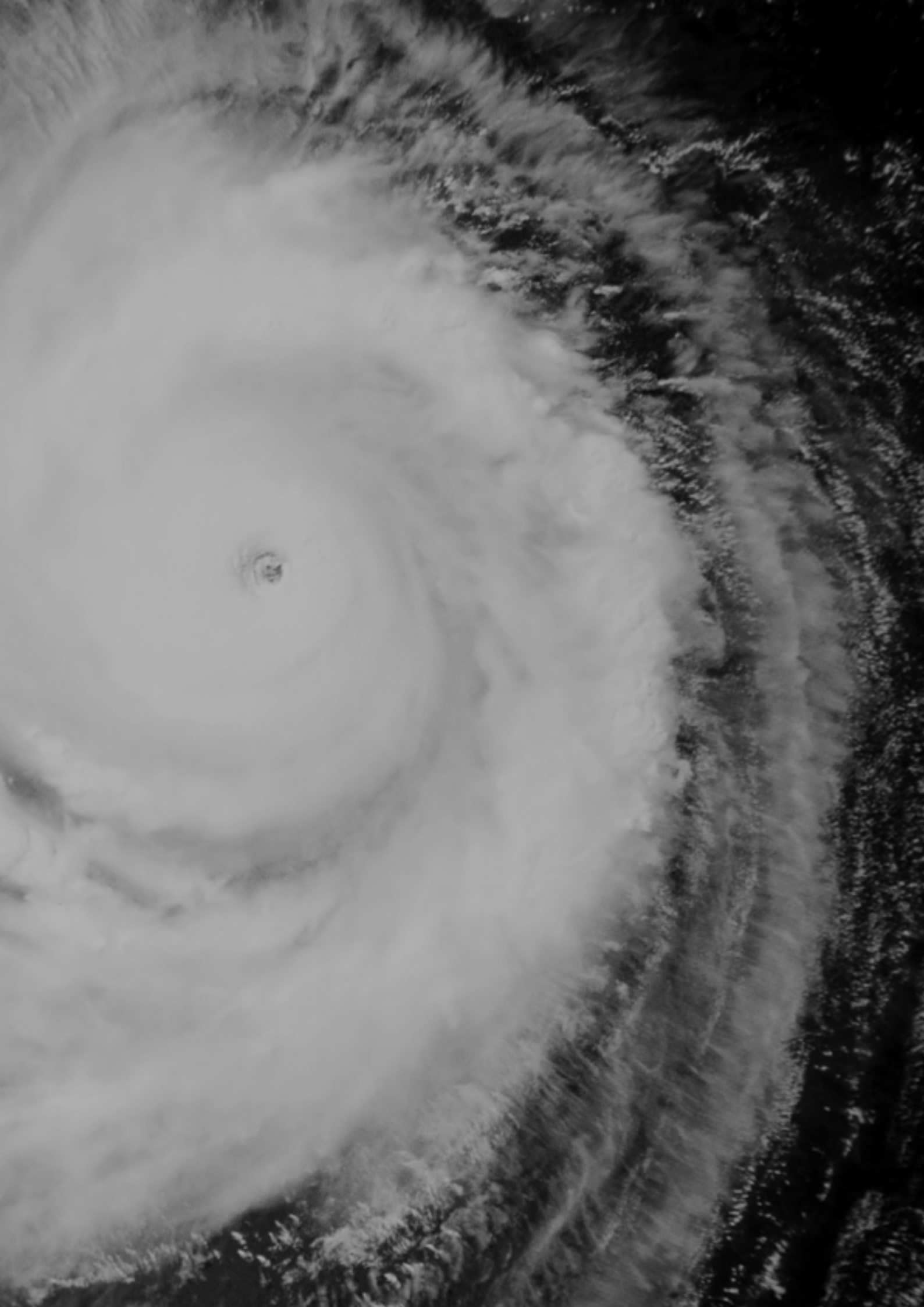
Power at sites

Backing up your power supplies with dual – even triple – redundancy can prevent communications outage, particularly where towers are at elevation, remote or inaccessible during winter.

Training

The greatest barrier to effective response in an emergency is low levels of preparedness – lack of training, and being unfamiliar with emergency SOPs. Technical issues come second. Section *8: The Human Factor* has more information on training and procedures.

Invest enough to stay on air through critical events, ensuring power to sites throughout.



4. Hardware: selecting, maintaining and upgrading

The equipment your workers use, how it is maintained and when it is upgraded, will determine the degree of communications confidence your organization can have, and the return on your communications investment.

Selecting the right hardware

If you consider some high-level failure scenarios, you can determine how durable your hardware will need to be. Common hardware solutions that increase the strength of your system are:

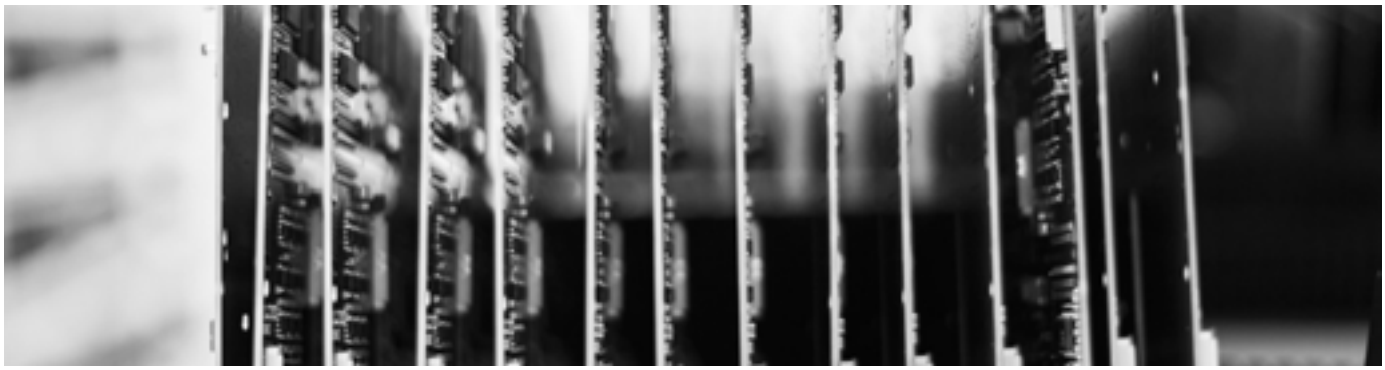
- back-up power source/s generators and batteries,
- duplication of site equipment so that no single site failure has significant impact on your coverage or capacity,
- microwave or fiber network architecture (star, ring, hybrid, hot standby), Specify seamless switchover during failure – ring architecture for backhaul system.
- antenna system engineering, using multiple antennas, combiners and multicouplers at large sites,
- redundant controllers, including geographically distributed ones,
- emergency radio cache, maintained and programmed for mutual aid,
- transportable repeaters that can extend current coverage or set up dedicated communications within minutes.

Remote sites need the best equipment you can purchase, to reduce failure and minimize callouts during winter.

Prioritizing

Often, low-risk system equipment gets the attention and funding, while crucial equipment is overlooked. When you are prioritizing your purchases, keep in mind what breaks most often. These are:

- power (poor quality unprotected mains, un-maintained UPS or DC battery banks, un-tested generators, generators with insufficient fuel supplies),
- antenna systems (bad lightning protection, poor grounding, poor design),
- backhaul (operator/technician errors).



Repairs, upgrades and checks

Increasing system complexity has changed the role of system technicians. The key skills for techs are now troubleshooting, diagnosing and resolving system failure - antenna system problems, power problems, backbone issues and system configuration errors.

Repairs

Virtually all electronic boards are now unserviceable except in highly-specialized settings, so field repairs are largely limited to replacing antennas, knobs, switches, display boards, speakers, and microphones. For all other problems, radios need to be returned for factory-based repairs. At system level, field repair is now limited to swapping faulty boards or even entire devices.

The ability for technicians to perform component level repairs is no longer important, except to maintain legacy equipment.

Upgrading hardware and software

Every aspect of your system is software-dependent, so it is important that you understand the implications of upgrading (or not upgrading):

- interoperability with other organizations,
- compatibility with system components,
- costs of falling behind on upgrades (typically more expensive than keeping up),
- impact of operating system obsolescence on your upgrade plans,
- taking advantage of useful new features and functions.

Before it is rolled out, test software on a dummy system, to avoid having to roll back – this can have huge implications for your system, and leave your communications vulnerable. Nevertheless, it is wise to have a rollback plan for worst-case scenarios.

Routine Maintenance

Cost, 24/7 availability or warranty/liability will often dictate whether you use your own technicians or a third party. Whatever the decision, responsibility for day-to-day maintenance must be clearly defined.

Schedule thorough maintenance checks at least annually - as your system ages, you need to schedule checks more frequently.

» Test your microwave system regularly. Links can be checked on site, so technician can measure and record parameters such as signal strength and BER.

» Alternatively, MiMo (multiple-input and multiple-output) linking can save on maintenance, as its alignment needn't be so precise.

» Periodically simulate failure conditions to test switchover functions for backhaul networks designed for automatic switchover.

» Electronic hardware is becoming ever more reliable. Systems with appropriate environmental (temperature and humidity) control can manage with annual checks, but systems working at high capacity or in difficult environments should be checked more often.

» Base station maintenance should include thorough examination of the receiver, transmitter and, above all, antenna system.

Scheduled site maintenance

Site inspections should be scheduled more often in regions with challenging weather or geography. Inspections should include:

- generators, including batteries, propane tank levels,
- fencing,
- cameras,
- security measures,
- on-site spares.

Spring and autumn equipment checks are particularly important in mountain regions. Make sure crews have all necessary spares and tools with them – returning to base to pick up forgotten items is costly.

Back up power – generators and UPSs - are often overlooked. Make sure UPS and DC-bank batteries are maintained to manufacturer recommendations and back-up generators are periodically exercised so they start easily, and have sufficient fuel for extended emergencies.

Subscriber equipment

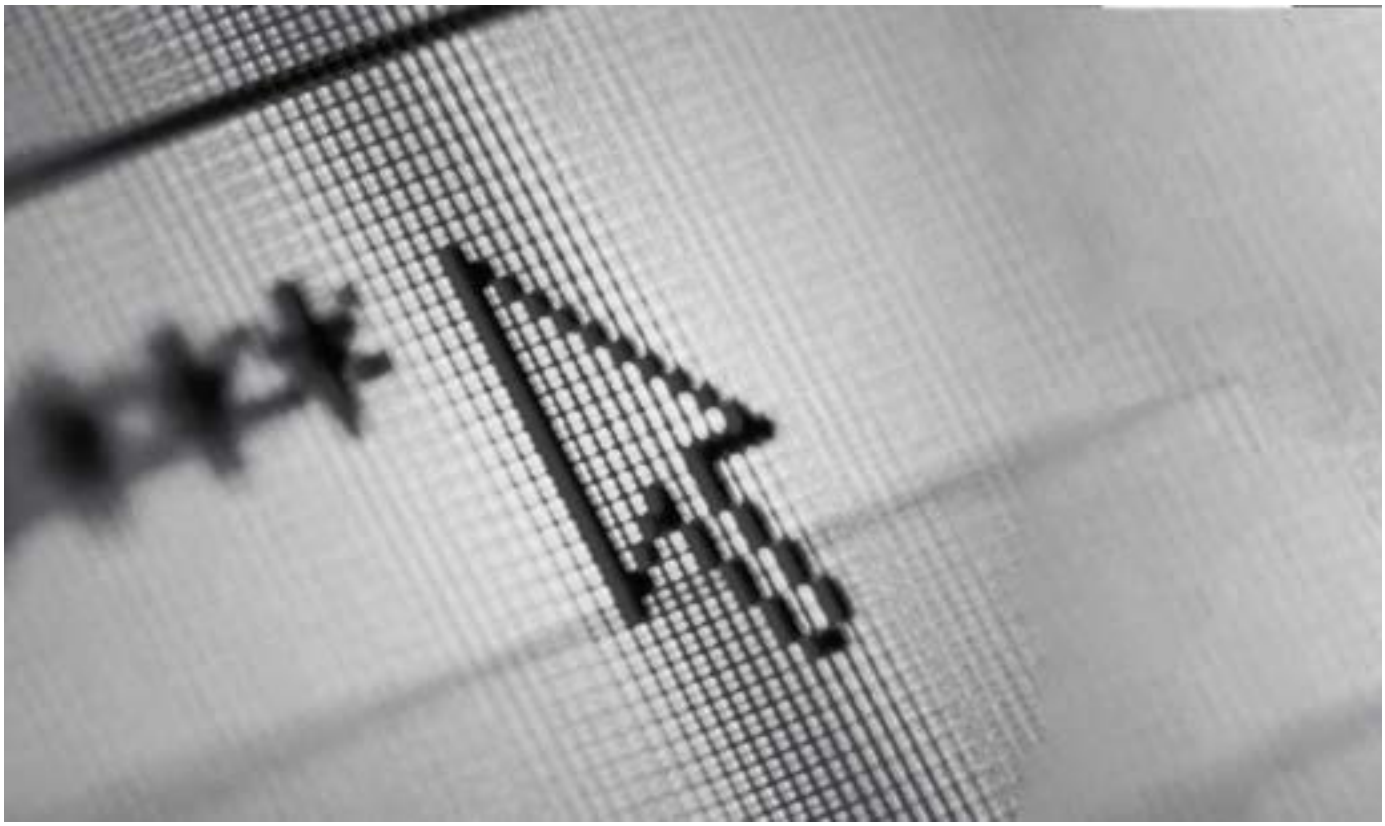
As digital radios become more reliable, routine tune-ups become less common. Instead, radios are usually tested whenever they come in for reprogramming or repair. Ideally this will be supplemented by remote monitoring.

Every radio needs to return to base regularly, especially your portable radio fleet, which are subject to physical damage as well as malfunction. Check portables whenever they are in the shop, and update your records. Asset Management software makes this task simple and quick.

It is more difficult to check on your mobile fleet – a wide area system might only see mobiles every seven or ten years. You can implement a program of radio maintenance alongside the vehicle maintenance schedule.

5. System configuration and optimization

Regularly reviewing and optimizing your system can identify incompatibilities and allow you to take advantage of new features and functions that make your communications more effective.



Optimization

Optimization was previously relatively uncommon in radio communications systems, which were often fine-tuned at implementation and then left alone for their entire useful lives.

Technology

Failure to upgrade software or respond to obsolescence issues can prevent you from accessing useful new features and functions, or worse, create compatibility issues within your LMR system.

Is your hardware and software up to date? Are any of your system elements facing obsolescence? Would upgrading some elements - for example base stations or servers - yield better performance or lower costs?

Functional performance

Functional performance should be monitored, verified and improved as often as practical.

» Keep a formal log of users' complaints. This will shed light on emerging issues such as changes in coverage performance due to urban construction or forest growth.

» Analyze traffic reports to identify changes and anomalies in system use, sites with capacity problems. Use this information to add channels or sites proactively.

» Keep up with market development and pay attention to your vendor's software upgrade release note. They can provide you with enhanced operational or security functions.

System configuration

Where configuration changes are infrequent, the system is built, configured with assistance from the vendor, and seldom changed without external help. Whenever sites, channels or dispatch positions are added, or backhaul network altered, the vendor is likely to be involved. This can result in system operators lacking system configuration knowledge and experience.

But radio systems are changing. Instead of a set of hardware coming from a single vendor, systems are much more software-driven, standards-based and likely to include interdependent sub-systems from multiple vendors. These evolving changes make configuration skills and related processes paramount.

Every operator should have at least one person fully versed in LMR system configuration, but, due to the increased complexity of digital communications, it may be safer to contract support from vendors for any major changes.

6. Monitoring: a preventative, proactive approach

Operators who routinely monitor their systems can detect issues and take remedial action before failure can occur. In the worst case scenario, a point of failure can be more quickly identified and remedied sooner.

Even the simplest radio communications are much more complex than their predecessors and therefore much more vulnerable. While operators may recognize this, it is not always reflected in their system monitoring practices.

We know how to monitor for intrusion and theft, environmental factors, equipment malfunctions, antenna system problems, power problems and many more. Where monitoring often falls short is the human resource; the actual monitoring personnel.

Few organizations can afford the ideal - their own, dedicated, system monitoring resource. But just because the ideal is not achievable, every modern radio system should be monitored in some way. There are technical and logistical solutions to fit any size and any budget. So it cannot be justified to simply rely on users' complaints to alert you when your system goes down.

Large systems

Large trunked systems with thousands of users should be monitored 24/7, which may require some ingenuity.

» You can add your system monitoring to an existing larger system.

» You can pool your resources with other LMR system operators.

» You can work with your equipment vendor, local service provider or seek a specialized service provider.

Smaller systems

For systems of less than a thousand users, finances are likely to be constrained and you may have to apply a combination of approaches. For example, you might rely on your own staff during working hours and dispatch personnel and/or third parties after hours.

Depending on dispatch personnel to monitor your system detracts from their core duties. If that is your only option, you need to establish very clear operating procedures, easy-to-interpret alarms and regular training.

Even very small systems should still be monitored. While active 24/7 monitoring may be impossible to fund, you can install all the necessary alarms and bring them to a central terminal with logging and messaging capabilities. Determine which alarms warrant immediate notification and which can be cleared the next working day. For example, you do not want to be woken every time a site's voltage drops below 105 V, but if your main repeater loses power, you do not want to wait till the morning.

What should be monitored?

For secure communications, the main elements to monitor are:

- power,
- environmental conditions (temperature, humidity),
- backhaul interruptions,
- integrity of antenna systems,
- intrusion.

Your system should have selectable, automatic notifications with pre-defined thresholds for minor, major and critical alarms, via SMS or paging, set up so that the correct notifications go to the right people at the right time. For example, you do not want every alarm (back-up generator kicking in for a couple of minutes due to a power brown-out) to trigger pagers in the middle of the night. But significant problems (TX power drop in a base station) should be reported immediately.

Typical performance reports will include:

- busy periods,
- call duration,
- number of "busies",
- calls per hour.

7. Back office: managing assets, fleets and subscribers

Operators can efficiently track and identify assets and people, then reconfigure or quickly disable units to prevent them falling into the wrong hands.

Asset tracking

The risk of theft and deliberate misuse highlights the importance of asset tracking and diligent record-keeping. However, few operators currently maintain up-to-date documentation with detailed information about hardware and software versions, ownership and repairs. As devices become more interconnected and product lifecycles get shorter, accurate documentation becomes increasingly important.

Keeping track of repairs is essential for identifying chronically-faulty equipment or abusive operators. A spreadsheet may be sufficient, although a specialized and sophisticated asset tracker application can control work in the shop, ownership, maintenance schedules, programming upgrades, inventory checks, installation and structural maintenance. You can set up asset management reporting, and make departments responsible for their own assets and control access.

Tracking devices and subsystems

Most radio system owners rely on their vendors, which can work well as long as your relationship is good. Standards-based systems with equipment from different vendors may require you to create and maintain a centralized, unified database.

Tracking subscriber equipment

Maintaining user information is important for day-to-day operations and for future planning, so it is easy to justify the cost of asset tracking tools. However, few systems have formal asset tracking processes, which is hard to understand, given that radios are expensive, and those who have implemented asset tracking tools are enthusiastic about their value. RFID tagging of equipment can help automate asset

tracking and has been adopted increasingly to improve the management of all assets and to enhance security.

Of course any system relies on accurate input, and it is common for record keeping to deteriorate over time. For the best results, you should purchase the best tool you can afford, and use it consistently, but even a basic spreadsheet or database is better than nothing at all.

Here are some guidelines to give you solid information when upgrading or replacing your system.

- » Delegate responsibility for keeping track of information to one person.
- » Use maintenance records to track assets, and to assess equipment reliability for replacement.
- » Control access for accountability.
- » Outsourcing maintenance services can compromise recording – establish clear, common asset management processes and tools with support partners.
- » Workers must report losses immediately, so radios can be disabled.

If your communications are publicly-funded, you may need to track any item worth more than $100. Good processes will mean fewer unpleasant surprises at audit.

Administration

Large LMR systems demand significant active administration, but even smaller systems require meticulous set-up and active management.

Subscriber management

While LMR system configuration changes are relatively infrequent, adding or removing subscribers, changing status or access can be a daily event. Inter-system interoperability means the skills necessary to successfully manage subscribers are growing in complexity and importance.

At the same time, programming is becoming increasingly complex, due to greater functionality and the fact that many systems have radios from multiple vendors.

Subscriber programming is not yet standardized, so although vendors may provide system keys (or advanced system keys) to prevent unauthorized cloning, programming or access, these will vary between vendors. Becoming proficient in programming different radio models is challenging and time-consuming, so you need to factor in the cost of this, if you choose to have different vendors' radios on your system.

Modern radio equipment may offer Over The Air Programming (OTAP) as a means of remotely updating radio software and changing a radio's features by transmitting the updates directly to the radios.

This replaces the process of bringing radios into a workshop where a technician physically installs the updates. If your radio fleet is large, then OTAP can save time and money. The type of updates that can be transmitted over the air range from basic services, such as changing channel plans and talkgroups, to more advanced services, such as altering individual user profiles or modifying applications on the radio.

Dispatchers and consoles

Regardless of your maintenance arrangements or the industry you operate in, at the heart of your day-to-day communications are your dispatch consoles. This is the major function for any system operator – directing traffic, allocating tasks, identifying technical or safety issues.

Your dispatchers are the eyes and ears of your system. They may identify problems with the system itself, or at the user end – unhappy users are quick to let them know there is a problem.

Development of digital CSSI (Console Sub System Interfaces) standards has helped to define console interconnection to the system. Time spent learning about your console options will result in better, future-proof decisions.

8. The Human Factor: training for safety and efficiency

Well-trained individuals and teams have clarity around their day to day responsibilities, and clear expectations from colleagues and mutual aid partners when disasters happen.

Not all your solutions are strictly technical. Because communication is an essential service, you are most likely already bound by regulation and compliance. How you manage this aspect of your operation is a vital part of your reliability picture. Developing and enforcing robust processes, assigning clear responsibilities, and logical, well-understood procedures will reduce outage risk and support swift, decisive response to events.

Whether they are dispatching, monitoring, maintaining or simply communicating, your people's competence and efficiency contribute significantly to the strength and reliability of your LMR system and the return on your communications investment.

People

Well-trained, consulted and engaged users, technicians and administrators, and robust SOPs are vital to getting the most out of the communications you have invested in.

It is not uncommon to see organizations fail to take full advantage of system features or upgrades. Resistance to technology can be linked to a lack of buy-in, when decisions are imposed without discussion, consultation or training.

Conversely, users who participate in decisions and changes are more likely to promote new solutions across the organization, adapting to and adopting the technology faster. Even those who are initially reluctant, by involving them early have time to accept the change well before it is implemented.

Training

It doesn't matter how much you spend, and how advanced your technology, any communications system is only as good as the people who use it every day. It can be tempting to save on staff training, to rely on training on the job, self-training, or internal courses. Unfortunately, this will most likely result in unforeseen future expenditure, in callout fees, higher maintenance overheads and users unable to communicate when they most need to. Better training means better technical judgement to manage risks and ultimately, safer workers.

A well-resourced training plan will retain organizational skills, get new workers up to speed quickly and support existing staff to continually refresh and update their knowledge. It should include hands-on experience for all users, together with scheduled repeats and refresher courses.

The best starting point is to scope the potential training requirements and plan what is needed by when. You need to identify who is responsible for that training, whether it is formal or informal, and whether you will involve trainers from outside your own organization.

Processes

Your Standard Operating Procedures (SOPs) determine the best way to perform the multitude of tasks your people carry out on a daily basis. With the focus on efficiency, effectiveness and safety, the SOPs relating to communications impact directly on the strength of your LMR system.

Clearly, a new communications system will trigger substantial changes in communications SOPs, for both your back office and front line staff. But even without those changes, your processes should have regular, scheduled reviews. Ask these questions:

- » Is your system used the best way it can be?
- » Are all the right people involved in standard communications procedures?
- » Are some people involved but should not be?
- » Do some procedures put an unnecessary burden on users or slow down the exchange of information?
- » Will changes to SOPs impact on interoperability with other organizations?

Once the task of producing and reviewing SOPs is completed, it is easy to assume

that the job is done. However, while SOPs make excellent training resources, they should never replace the training itself. SOP changes should trigger refresher training to keep everyone up to speed and working efficiently.

One critical aspect of communications SOPs is how you will interoperate with others during planned or unplanned events and disasters. This requires cooperation with all the other parties you have mutual aid agreements with, or will need to support, to ensure that everyone's SOPs align and are well understood.

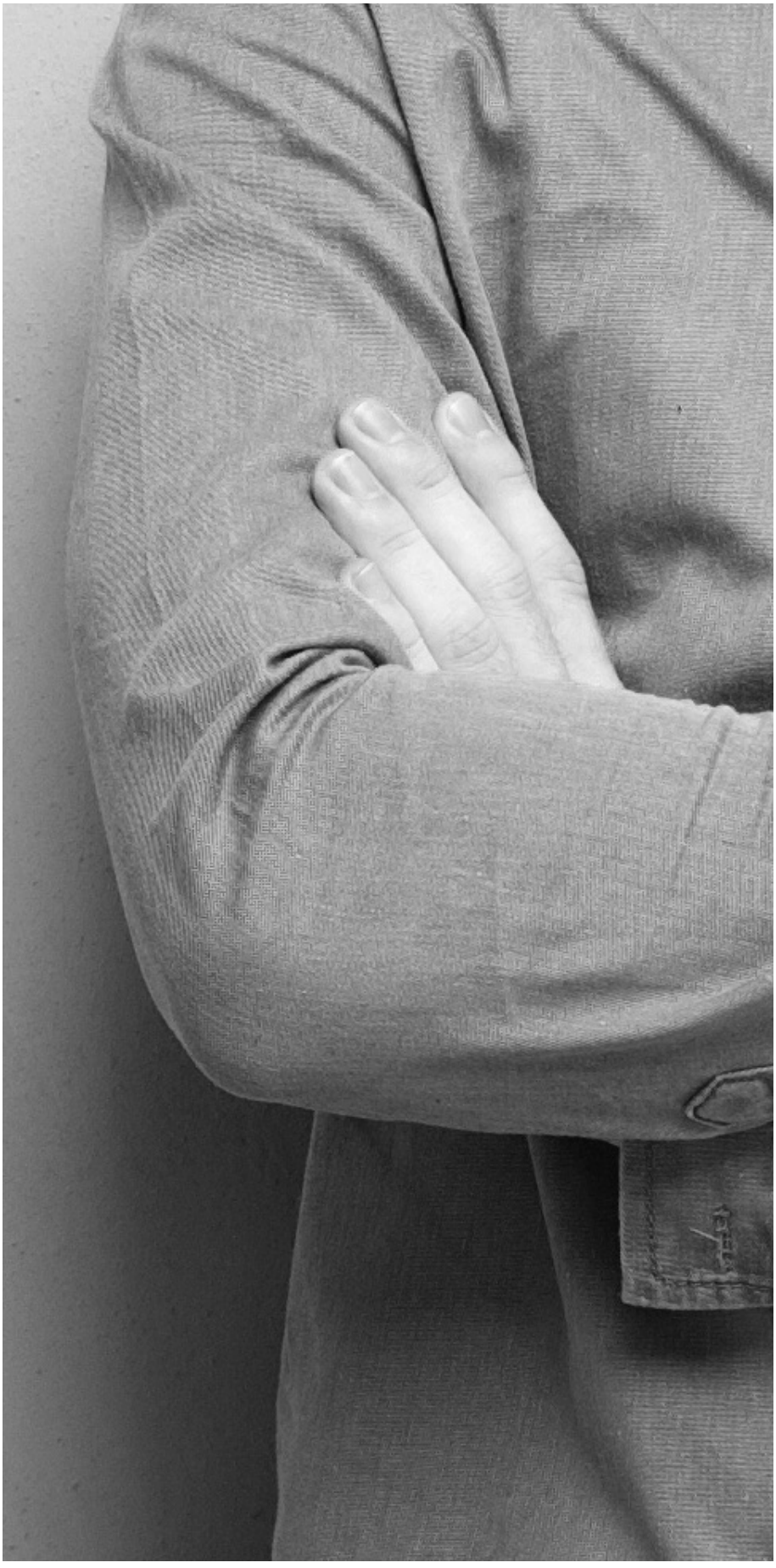
- » Allow access to sites and groups as-needed only.
- » Limit monitoring/scanning.
- » Limit groups on the system.
- » Enforce incident discipline of communications.
- » Train your people to ensure they understand what is required of them.

Users as stakeholders

At any decision making point, user opinions must be represented, to ensure the communications meet their needs. They need to be consulted and informed so that they can embrace the technology you have invested in, and embrace change when necessary. Typical internal stakeholders should include:

- radio users,
- dispatchers,
- system administrators,
- technical personnel.

A simple way to keep these stakeholders engaged is user satisfaction surveys. Conducting simple surveys may generate ideas to improve your SOPs, or identify training needs. The opinions of users are well worth listening to.



9. Security

Critical communications require robust protection from physical or cyber attack, eavesdropping and equipment failure.

Physical security – protecting your sites

Ideally, your site equipment is housed in your own building, surrounded by secure fencing which only your organization can access. However, that is not the reality for most system operators, who must choose a combination of cameras, fencing, controlled access, monitoring and inspection, while sharing sites with other organizations.

Site access

Restricting and protecting access to sites will reduce the risk of accidental or deliberate damage to your equipment. Here are some guidelines.

» Within the fenced compound, your own building should be double-locked and alarmed.

» Provide unique access and security of compound and gate locks.

» If sites and enclosures must be shared, provide locked cabinets and shelters, and gated equipment cells.

» Equipment room doors, air-conditioning and grounding must be monitored 24/7.

» Site equipment access should be limited to key personnel only.

Theft and vandalism

For some organizations, this is a greater risk than cybersecurity. Air conditioning units are frequent targets - monitor them by camera, and protect them with secure fencing and access control.

Copper from grounding and lightning protection is also targeted. Innovative deterrents include concealing the copper by painting it, or enclosing it in plastic pipe.

Cyber Security

Connectivity between your radio communications and the outside world is perceived as a threat by some, but it has become inevitable, with devices such as smart phones now used in the field. Anything beyond your firewall is open to a breach.

How do you assess your security needs? It is difficult to find a formal process, and the decision is a management one rather than a technical one. But it is crucial that RF and IT engineers need to understand the implications of their own, and each other's disciplines.

Communications security largely depends on the integrity of your backbone, switch and backhaul. Most secure is all microwave, with fibre for routing and fibre backup.

You will most likely need to consult with a security expert on the subject, but the following approaches could be considered:

» Factor in risk associated with remote access – for your people, vendors and contractors.

» Vendor equipment may require higher security.

» Remote monitoring via IP is dependent on the internet and remote servers.

» Equipment brought in by visitors (cell phones, portable memory devices, laptops, cameras etc) can compromise security.

Encrypting communications

While encryption is an essential item on most organizations' security list, it is expensive to purchase and expensive to manage. However, you should resist the temptation to accept cheaper, non-standard (proprietary) encryption. As well as reliability issues, you will seriously compromise your ability to interoperate with partners, and limit your radio purchasing options in the future.

Encryption can also be resource hungry, and you may need to factor in degradation on your system. However, these costs are offset against the very real benefits of being able to communicate securely, keeping your workers safe and vital information protected.

Common approaches to encryption include:

- encrypting channels rather than users, so long as everyone can access the encrypted channel,
- a single encryption key for users,
- no interoperable channels encrypted to avoid communication issues,
- emergency-only encryption, with a clear, well understood code of practice.

Who needs encryption?

Encryption was designed for high risk situations, rather than business-as-usual, so most conversations don't require encryption. It is probably not necessary

for all radios to be encrypted, but the most critical factor is ongoing dialog with partners that you share communications with. You need to agree on approach, access and purpose to develop a fully transparent process. Don't underestimate the training required to have everyone up to speed. Without this, encryption can actually inhibit communications for mutual aid.

Encryption-related SOPs benefit from periodic reviews. For example, your system may have started with everyone using it, but two years later, some groups barely use it, others have never changed the key, and new groups need encryption but do not know how to manage it.

Managing encryption keys

Maintaining encryption keys is a major challenge, but it is essential to encryption management. When keys are compromised, your system integrity is challenged, and once a breach or loss is identified, you must change the entire group. A single lost radio means new keys for everyone.

Plan to change all keys regularly. How frequently you change keys depends upon how much security is required by the various groups in your organization. Groups that need high security should change keys more frequently. Keys that are never changed will compromise your security and provide an opportunity for unauthorized parties to access your communications.

Over-the-air rekeying (OTAR) will reduce the overhead of key management considerably. Current offerings are proprietary, but including OTAR in LMR standards will simplify programming, especially for operators of mixed-vendor fleets.

Alternative access

Alternative access for dispatchers is critical, when there is disruption at the control centre, such as a forced evacuation due to a fire alarm or bomb alert. Radio-based access, via portables or control station mobiles, is a cost-effective and reliable way to maintain communications with workers in the field.

Control station mobiles may have a handset and in some cases a reduced-feature console. Mobiles with extended remote control heads - and even dual remote control heads - can be installed in buildings to position the radio body and antenna in the least vulnerable place, while still providing a full mobile user interface inside an office or control center.

You can also use the control stations for off-air monitoring.

10. The future

No single system will deliver all the information types required to achieve efficiency and effectiveness gains in the dynamic environment of modern communications.

Simple physics and economics mean that, in the future, operators will need to deploy multiple communication bearers to access rich data sources. Future-proofing your communications involves recognizing that the convergence of wireless communications, voice over IP, data networks, and smart devices is already well underway. However, this will need to be achieved without jeopardizing or conflicting with their critical voice communication.

One solution is to integrate multiple bearers, to create seamless communications that will link the field to the back office. By investing in open standard IP-based technologies and utilizing only open standard interfaces you can position your LMR system to take advantage of the profound changes in communication that taking place now.

The Internet of Things

The concept of an Internet of Things builds upon this convergence by interconnecting embedded computing devices, each with a unique identity (an IP address), within an Internet-style network. These devices are inside sensors, actuators, and a variety of software-driven controllers. They can collect data, monitor their environment, and communicate directly with each other – machine to machine – without human intervention. This advanced connectivity enables faster, smarter, more automated control of a system that is better able to optimize services, business operations, and reliability.

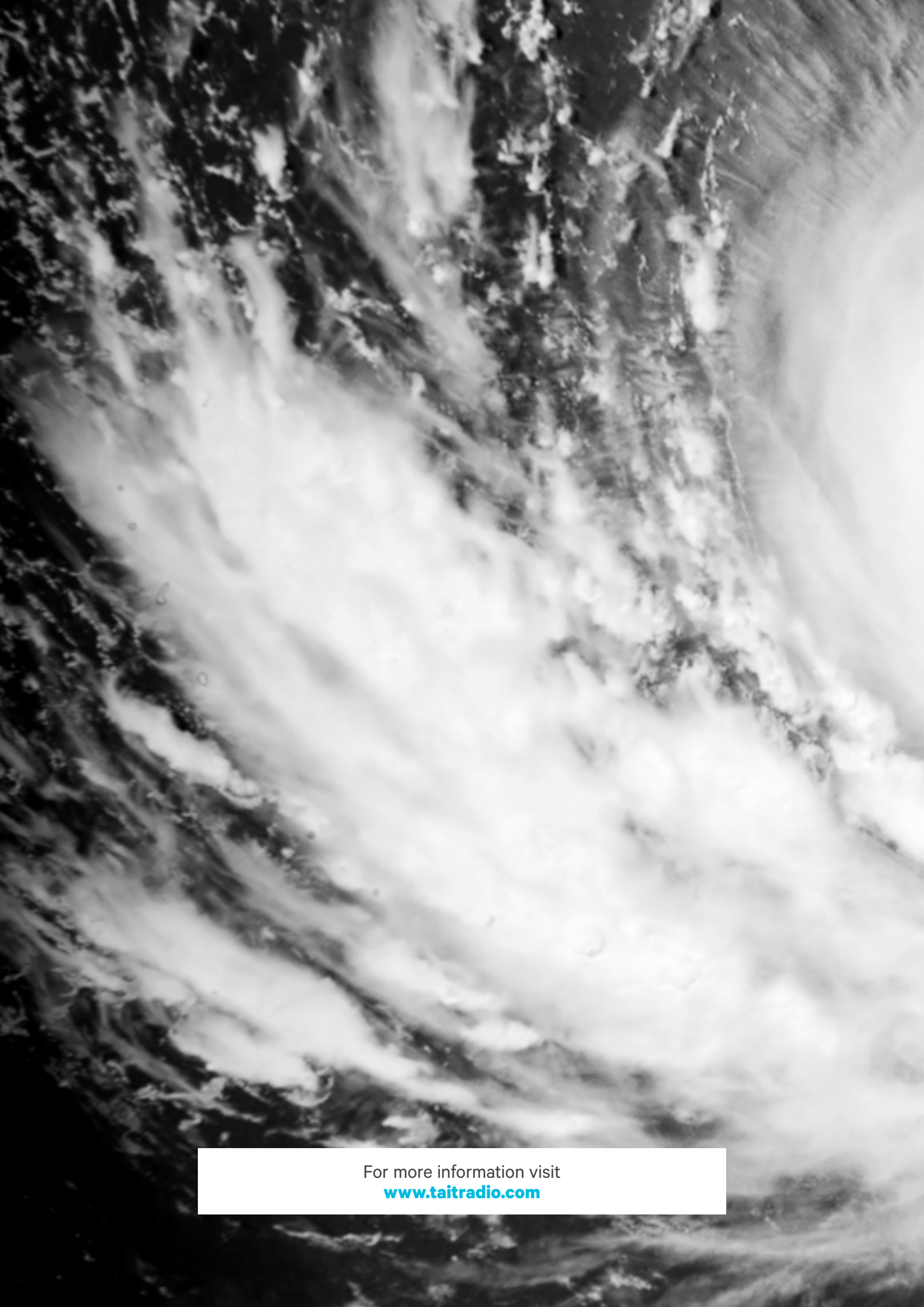
Far from being a distant vision, this concept is already being applied in a variety of industries:

- utilities – the Smart Grid,
- oil and gas – the Digital Oil Field,
- fire control – smart field operation devices,
- mining – mine site automation,
- manufacturing – the Connected Factory,
- transportation – Intelligent Transportation Management and driverless vehicles,
- public safety – automated video monitoring and data security analytics.

Importantly, the concept of unified critical communications is compatible with The Internet of Things; multiple communications bearers integrated into a single IP-based network create new opportunities for smart services and applications.

With remote monitoring, automated notification, and self-correcting components comes improved communications system availability. Individual components will use whatever communications technology is most available and most appropriate to connect into the communications network. Applications designed to process the vast quantities of data generated by smart, interconnected devices can develop a more detailed and dynamic picture of an organization's business operations.

Integrating multiple communications bearers into a single IP-based network creates new opportunities for smart services and applications.



For more information visit
www.taitradio.com