P25
BEST PRACTICE

MANAGING YOUR P25 SYSTEM

tait communications

Who should read these guides?

If you are a Public Safety official who is responsible for, or involved in, procuring a new communication system, this guide (and the others in the series) is written for you. You may be new to the position, or focused on other disciplines, such as IT. Or you may be new to P25. We assume that you have an understanding of Land Mobile Radio, but not necessarily in-depth knowledge.

We also assume that your interest is pragmatic; you want to make sure you procure and/or manage your radio system to meet the needs of your first responders and public service providers in a fiscally-responsible way. Becoming an expert on all related topics is not your objective.

We hope these guides will benefit you and your wider Public Safety Communications community by presenting you with a range of P25 topics so you can more effectively engage in the process.

The decision to adopt the digital open standards-based P25 platform offers Public Safety agencies many benefits, but it also raises a lot of questions. There are many common questions and there are many agencies who have already tackled them, who are happy to share their experiences.

Tait is sponsoring an on-going project, to discuss these topics and put forward some answers.

Over a series of intensive round-table sessions, our participants discussed their own experiences and challenges, generously sharing their frustrations and triumphs. Together with Tait expert advice, these guides include their many valuable insights, based on their hands-on experience working through typical P25 project challenges.

Learn more and subscribe to future guides at
www.p25bestpractice.com

MANAGING YOUR P25 SYSTEM

- What are your options for managing your network?
- What should you be monitoring?
- How do you prepare for major events?

Managing a P25 network requires significant, up-to-date experience and knowledge, as the complexity of Public Safety networks continues to increase. The primary responsibility for system management rests with the system owner, usually a government agency, assisted by equipment vendors and local technical support providers.

The objective of this guide and its companion volumes is to provide high level information to assist Public Safety professionals responsible for a P25 communications system.

These are not hard and fast rules. These recommendations are based on Tait experience and the informed opinions of industry players who have attended our round-table workshops and shared their best advice, based on hands-on experience working through typical P25 network challenges.

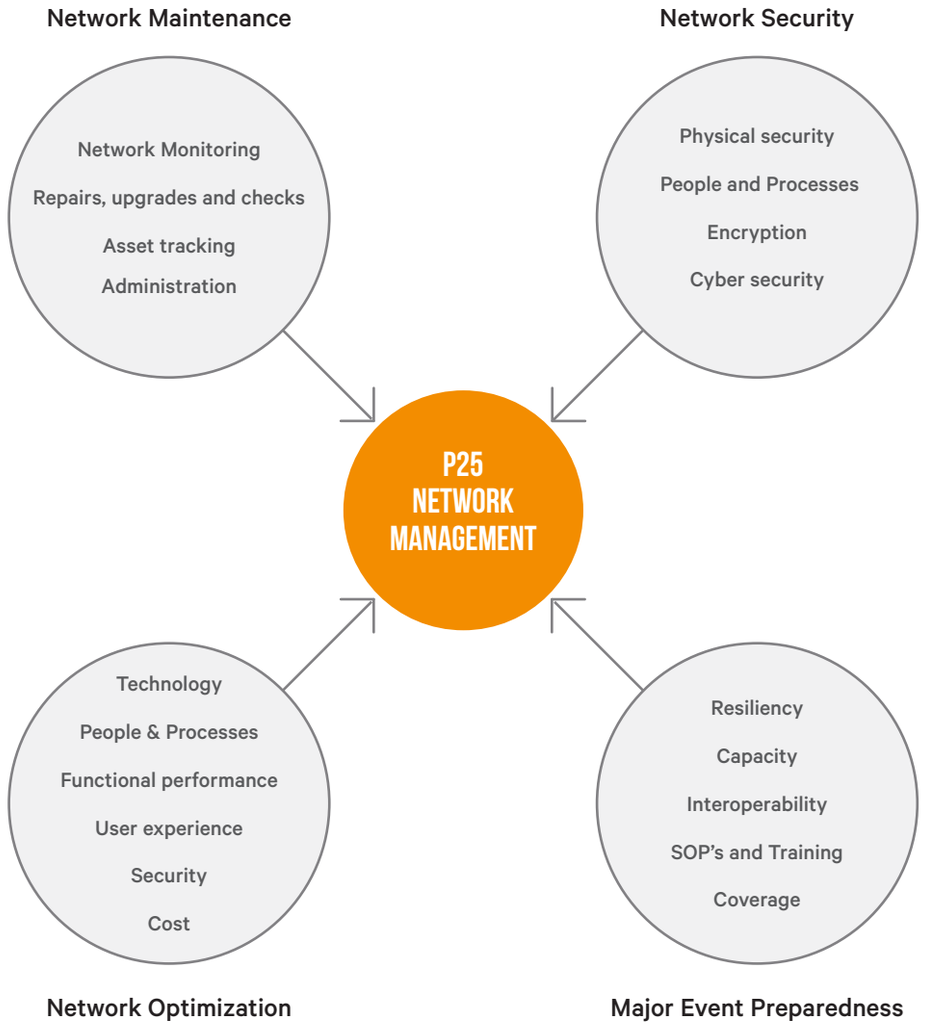
CONTENTS

This Best Practice guide for managing P25 systems uses a simplified, non-chronological approach. The organization of topics is loosely based on standards in related industries (IT) as there are currently no known, well-established standards for managing Public Safety radio systems (2021).

The cornerstones of P25 network management are:

- Network maintenance – maintaining operations of your system at the expected level
- Network optimization – making your network operate better
- Major event preparedness – being prepared for emergencies and events
- Network security – protecting your network from physical or cyber attack

More on these topics can be found in the guide "**10 Ways to Protect and Strengthen Your LMR System**"



Managing a P25 digital radio system is very different from managing your old analog system. The demand for sophisticated network management techniques and processes among Public Safety organizations is only beginning to emerge.

This area of Public Safety operations will have to change significantly within the next few years. The old static, hardware-based systems of yesterday that run without a problem (as long as there was no physical damage) are no longer the norm.

Public Safety networks are increasing in complexity as software components become more significant. The interdependence between various system components, often coming from different vendors, with different (and continuously shortening) life cycles is turning a very static system into a highly dynamic network requiring new processes, methods of care and new sets of skills.

However, while tools to simplify network management abound, they should not define it. It is more important to understand what needs to be managed and to provide practices, people, and resources to manage your network effectively.

"THE NEXT GENERATION OF TECHNICAL PERSONNEL WILL BE MORE COMFORTABLE WITH DIGITAL COMPLEXITY, BUT THEY ARE NOT AT MANAGEMENT LEVEL YET.

EVENTUALLY ALL SMALL NETWORKS WILL MIGRATE TO LARGE, AND ALL WILL BE MANAGED. BIG SYSTEM OWNERS NEED TO ACCEPT MORE USERS."

NETWORK MAINTENANCE

This section focuses on maintaining the technical integrity of your system for routine operations.

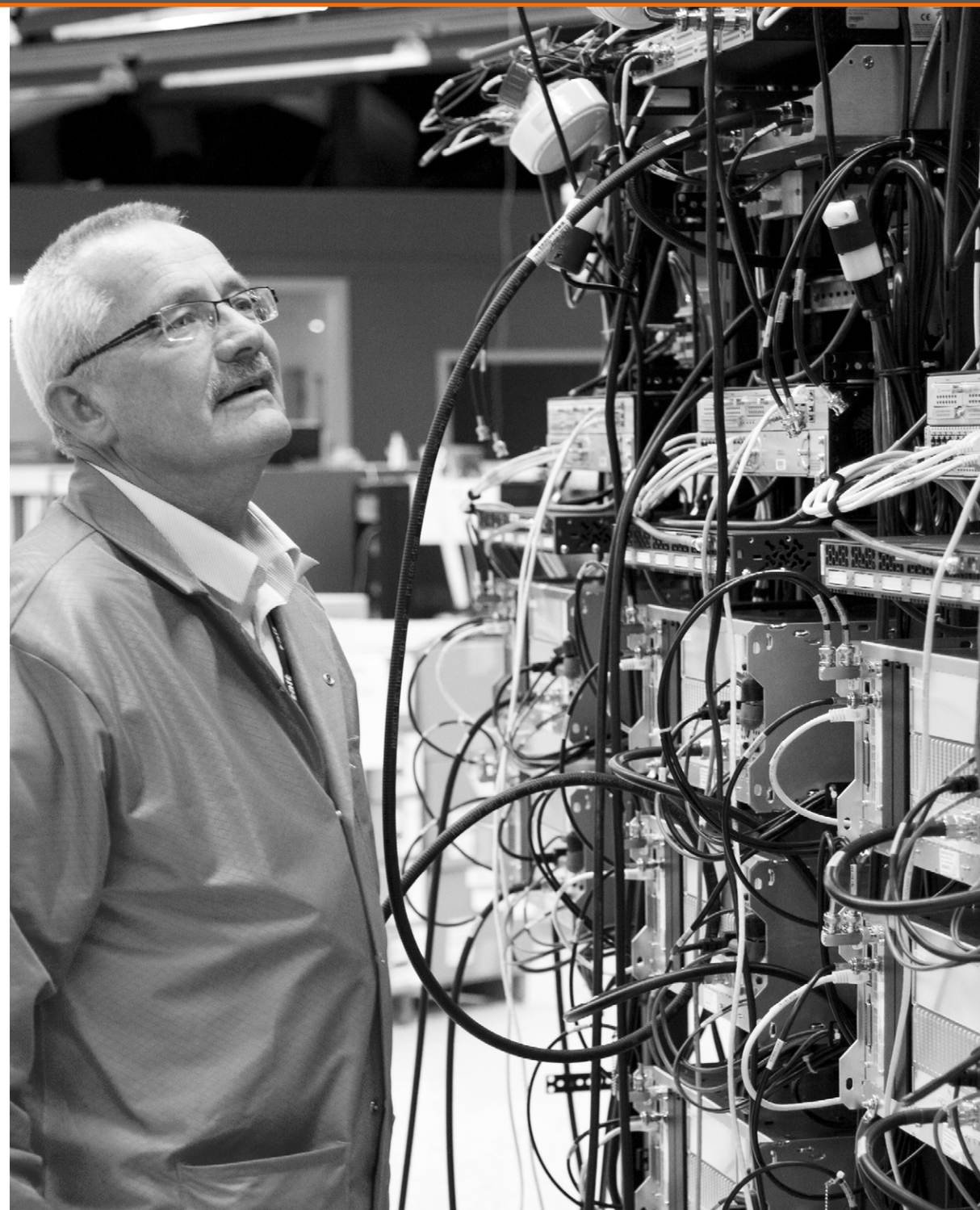
Monitoring a P25 radio system is very different from monitoring an analog system. The P25 radio network is made up of numerous components, which must communicate with each other. To successfully manage them, you need to understand their use and how they communicate.

Broadly, the components can be classified in three tiers:

- system-level components (e.g. network controllers),
- site-level components (e.g. base stations),
- subscriber-level components (e.g. portable and mobile radios).

In contrast to analog systems which often contain proprietary equipment and interfaces, open-standard P25 communication networks are generally IP-based. They utilize components (such as switches and routers) that make use of standard transport protocols (such as TCP/IP), and also include built-in IP monitoring that conforms to the standard Simple Network Management Protocol (SNMP).

A variety of SNMP-based tools, from the simplest to the most sophisticated network management applications, can monitor all the components of your P25 network.



NETWORK MONITORING

Even among the largest state-wide systems, network monitoring practices vary from strict, structured 24/7 internal operations to a reactive approach – responding only to complaints from system users.

Why are relatively few Public Safety systems proactively monitored? Back in the days of software-free radio systems, not much could go wrong. As long as there was power at the sites, power amplifiers did not burn, and antennas were not damaged by lightning, your system was probably in good shape. Should anything go wrong, your subscribers would quickly tell you that their channel was not working. As a result, many people in charge of digital radio systems do not give monitoring a sufficiently high priority.

Dedicated 24/7 resource can be expensive, but your network should be monitored, regardless of size, using the approaches matching your needs and capabilities. Alternative methods to 24/7 Network Operations Centers (NOCs) include:

- system monitoring terminals at dispatch centers,
- automatic page or text messages to technical or administrative personnel in case of an alarm,
- ad hoc monitoring by local service providers (internal or external).

You shouldn't rely on your subscribers to tell you when there is a problem with the network.

So while you don't need 24/7 staffing if you have a good alternative system in place, simply maintaining the status quo for the many under-monitored systems is no longer viable. Software-dependent digital networks are subject to glitches, viruses and compatibility issues. They are heavily dependent on correct operation of complex subsystems such as fiber backhaul (often provided by a telco), and are subject to frequent software upgrades. So they are much more vulnerable than analog systems.

As networks become more complex and interconnected, a virus brought into a dispatch console (perhaps doubling as a gaming PC during the slow hours) can cause serious issues for your entire network.

Your P25 network should be monitored regardless of its size, with management methods and resources that match your organization's needs and capabilities.

Techs who are on the system every day will pick up problems before they are reported. They are constantly talking and listening.

Risk factors

At RF sites/equipment rooms:

- Copper theft,
- Power loss,
- Intrusion
- Antenna system failures
- Environmental issues
- Lightning strikes

At dispatch centers:

- Backhaul failures
- Fiber – operator errors
- Microwave - weather
- Theft and misuse

Subscriber devices:

- Too many to list!

Maintenance and administrative equipment:

- Calibration
- People accessing the terminal and changing parameters haphazardly without reporting it to anyone

Who should monitor your network?

The technical tools for monitoring P25 networks are well known and widely available. Network management applications can monitor system activity and compile useful analyses and reports. These, in turn, can be used to observe trends, identify over (or under) utilized sites and consoles, and anticipate where channels or sites need to be added.

A greater challenge is to obtain technical resource to monitor and interpret network status information.

Large systems

Systems with thousands of users (state-wide networks, large counties or major metropolitan areas) should operate their own 24/7 network operation centers (NOCs). NOC personnel typically monitor network performance and take responsibility for system configuration, user ID creation and talk group management.

Mid size systems

Where dedicated 24/7 NOCs are not feasible, you can look for a shared one, using a mix of vendors, local service shops, and large systems nearby.

A shared NOC can monitor system performance metrics, provide alerts, deliver performance reports. In the event of an alarm, often a vendor

Consider paying on-call staff one hour for every five hours on call, with minimum call out of two hours.

may not even need to involve you to rectify the issue. A disadvantage is that you may be competing for a shared NOC's attention with other systems, and a vendor is likely to be monitoring remotely via the internet, which is of less use in a disaster.

A multi-layered approach with a manufacturer or vendor, service provider and internal techs means lots of eyes watching your system from multiple perspectives - your in-house experts during the day, and a contracted local vendor or a friendly NOC at night.

Small systems

If you choose to monitor your system yourself, remember that the tools provided and expectations placed on your maintenance team are critical to success.

Active monitoring allows you to respond proactively, and not to simply rely on your users' complaints. Where this is feasible you should set up alarms to trigger paging or SMS to technicians on duty. If you involve your PSAP, educate your field staff and dispatch well. For example, when a call is dropped, users must report formally which radio and location, so you can keep track of events. Make this process a part of your standard operating procedures.

Monitoring by dispatch

Some agencies opt for dispatch personnel to monitor their networks. This is controversial for two reasons:

1. This additional task can potentially conflict with dispatchers' primary life-saving and property-saving responsibilities.
2. System monitoring and issue reporting requires technical knowledge beyond the understanding of most dispatchers.

Ideally you would not burden your dispatch personnel with monitoring, but it may be a matter of necessity, typically due to financial constraints. On the positive side, properly set-up alarm systems may be embraced by dispatch personnel.

If you must use your dispatch personnel for self-monitoring:

- provide appropriate training, including scheduled refresher sessions,
- provide clear instructions and SOPs,
- strive for a balance, making sure monitoring receives sufficient attention without interfering with the primary objectives of the dispatchers,

- bring all alarms, clearly labelled, to one terminal so that the monitoring personnel can easily interpret them and commence the appropriate course of action.

No Public Safety communication system should rely on complaints from users as its principal monitoring method.

However, officers in the field will provide invaluable radio performance information, for better diagnosis of issues like dead spots and interference.

“THE MOST COMMON POINT OF FAILURE IS THE INTERFACE BETWEEN THE SEAT AND THE KEYBOARD.”

WHAT SHOULD BE MONITORED?

The elements of the network that should be monitored are:

- RF Equipment
- Backhaul
- Sites
- Subscribers
- Dispatchers

RF Equipment

Many new base stations come with advanced monitoring functions built in, and third party devices are capable of monitoring transmitter power and antenna system malfunctions. The extent to which the RF equipment should be monitored depends on the needs of each system owner, but monitoring output of all transmitters is the recommended minimum.

Repeater functions and parameters that should be monitored include:

- Tx output power (out of repeater and into the antenna system),
- Tx modulation level,
- VSWR (Voltage Standing Wave Ratio),
- Tower Top Amplifier operation (where applicable),
- Rx channel interference.

You should monitor base stations' receive frequencies for interference, and take them out of service remotely if necessary – either automatically or manually.

Backhaul

If you are using your own microwave or fiber network, these technologies have network monitoring built in and can trigger alarms/switchovers when transmission parameters are compromised. If your backhaul is provided by a third party, 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 Public Safety radio systems, especially dispatch.

Sites

Site monitoring can employ techniques from motion detectors, contact closures on doors, to live video monitoring at high risk sites. Sites should be monitored for:

- high or low temperature inside the shelter,
- humidity/moisture ingress,
- power disruption,
- generator fuel/battery bank voltage levels,

- tower light malfunctions (where applicable),
- grounding system malfunction,
- intrusion,
- smoke,
- back-up generator malfunction.

Subscribers

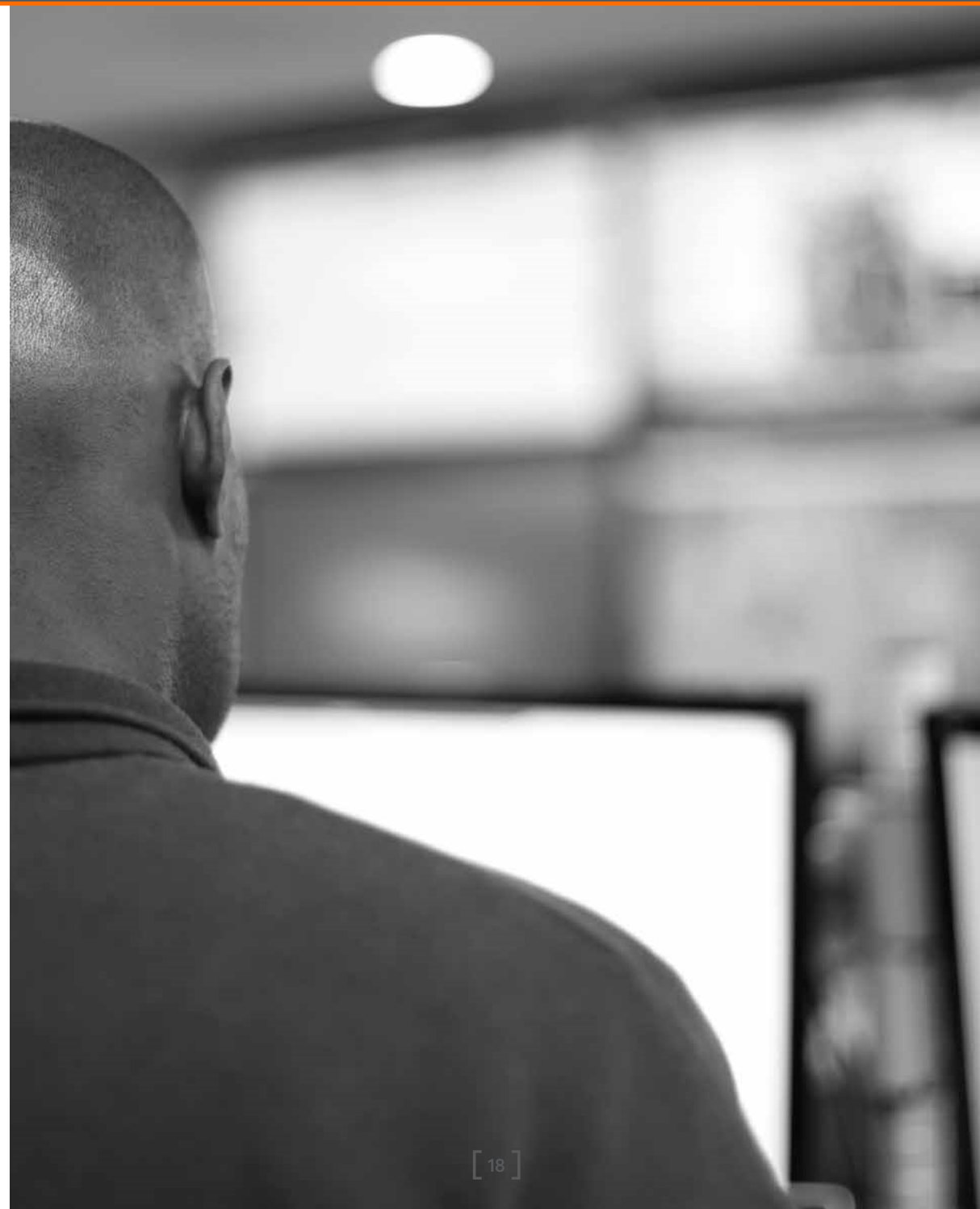
Systems and devices that remotely monitor the technical parameters of subscriber units can detect some problems early, especially those related to transmitter performance and antennas, saving you time, money and grief.

Traffic reports from network management tools can provide information about the activities of individuals and groups, that can identify misuse, capacity problems or technical issues that subscribers may be unaware of.

Dispatchers

The biggest challenge for dispatch centers is backhaul network failure. The actual dispatch positions do not need much technical monitoring, assuming they are manned 24/7 and that dispatchers recognize and report issues quickly.

Some industry practitioners recommend monitoring and analyzing dispatch position usage stats, such as number of PTTs in a given period of time. This can be useful in managing workload efficiently.



REPAIRS, UPGRADES AND CHECKS

The role of Public Safety radio technicians is rapidly changing, and their willingness to learn and attack any technical challenge is paramount. Intimate familiarity with the discrete elements of the radios is being replaced with thorough understanding of the network and system configuration, high-level troubleshooting and radio programming. The ability to perform component level repairs is no longer important, except where legacy equipment is no longer serviced by vendors.

Conversely, with the increase in system complexity, the ability to troubleshoot at network level and diagnose and resolve the source of system failure - antenna system problems, power problems, backbone issues, system configuration errors - is very important. Administrative and computer skills are taken for granted.

Repairs

Virtually all electronic boards are built with surface mount devices, rendering them unserviceable except in highly specialized settings. So the scope of repairs that can be performed in the field is systematically decreasing. Field repairs are typically limited to replacement of antennas, knobs, switches, display boards, speakers, and microphones. For network elements, field repair is now limited to swapping faulty boards or even entire devices. For all other problems, all equipment needs to be returned for factory-based repairs.

The ideal techs? Radio geeks that gobble up new technology that others find hard to keep up with.

Whether to use your own technicians or a third party for repairs is seldom a question of technology, but most often dictated by cost, 24/7 availability or warranty/liability. Whatever the process, responsibility for day-to-day maintenance must be clearly defined.

Upgrading hardware and software

Upgrades are seen as a necessary evil to be avoided by most system administrators. However, every aspect of your P25 system is dependent on software, so it is important that you fully understand the implications of upgrading (or not upgrading).

You need to consider:

- interoperability with your mutual aid partners,
- compatibility with other network components,
- the impact of operating system obsolescence on your upgrade plans,
- the advantages of useful new features and functions.

One-off upgrades are typically more expensive than long term maintenance agreements.

When upgrading software, the best approach is to test it on a dummy system through a local vendor before it is rolled out. It is important to avoid having to roll back – this can have huge implications for your network, and leave

communications vulnerable while the issues are resolved. Nevertheless, it is wise to have a rollback plan for worst-case scenarios.

When developing your upgrade roadmap, you can plan to upgrade biennially, but you can budget this annually, to spread the cost and avoid budget peaks.

Occasionally, manufacturers and vendors may offer you the opportunity to evaluate early versions of software. This has advantages and disadvantages, which you need to weigh up carefully.

- ☑ You will usually pay considerably less for early pre-release software versions.
- ☑ It is likely to have more bugs than later releases.
- ☑ You can influence features in product development, so you are likely to end up with software that better suits your needs.

Routine Maintenance

There is a great variety in practice and recommendations for frequency and thoroughness of routine maintenance – from weekly structured checks to a fully reactive approach.

Our recommendation is to schedule thorough maintenance checks, accounting for local geography and weather patterns. Obviously, as your system ages, you will need to schedule maintenance more

Offer to evaluate developmental infrastructure and SU software so you can influence features and often benefit financially.

frequently, but an annual check is the recommended minimum.

Run regular tests and reports on your microwave system. Microwave links will typically have the means to check their operation on site, so your maintenance technician can measure and record parameters such as signal strength, BER or others.

For backhaul networks designed for automatic switchover, you should simulate failure conditions to test switchover functions periodically.

Electronic hardware is becoming ever more reliable. Systems with appropriate environmental (such as temperature and humidity) control can manage with annual checks, but systems working at high capacity or in difficult environments should be checked more often. Maintenance for any base station should include thorough examination of the receiver, transmitter and, above all, antenna system.

Scheduled site maintenance

Site inspections should be scheduled regularly – 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. Remote sites need the best equipment you can purchase, to reduce the chance of failure, and to minimize callouts during winter. And while it may seem obvious, make sure that your crews have all necessary spares and tools with them for remote site checks – returning to base to pick up overlooked or forgotten items is costly and inefficient.

One of the most-often overlooked subsystems at the radio sites is back-up power – generators and UPSs. 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 and less field-serviceable, routine tune-ups become less common. Instead, radios are tested when they come to the local shop for reprogramming or repair, supplemented by remote monitoring.

However, subscriber equipment is not always as robust as expected. Every radio needs to return to base regularly, especially your portable fleet, which are subject to physical damage as well as malfunction. Give your portables a checkup whenever they are in the shop, and update your records.

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

Schedule annual checks, in addition to checks performed whenever the radio is in the shop.

Subscribers are very forthcoming with complaints but it is still useful to schedule touch points.

Network checklist

- ☑ Perform manual switch over monthly to ensure microwave transmitters on hot standby are fully functional.
- ☑ Test physical systems regularly
- ☑ Save emergency callouts by purchasing suitably robust equipment for mountaintops.
- ☑ Check generators and batteries monthly.
- ☑ Inspect and replace reels of antenna repair coax at sites during and after weather events.
- ☑ Switch active and redundant equipment bi-monthly to ensure both are fully functional.
- ☑ Check propane tanks for evaporation.

Consider making each department pay its own way, to encourage greater focus on radio tracking.

ASSET TRACKING

Diligent record-keeping is at the heart of efficient asset tracking, but the requirements and benefits are not yet widely understood, addressed and realized. Few operators maintain up-to-date documentation with detailed information about hardware and software versions. As devices become more interconnected and their life cycles get shorter, accurate documentation will grow in importance.

Keeping track of repairs is essential for identifying chronically faulty equipment or abusive operators. A simple 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 it up for asset management reporting, and make departments responsible for their assets and control access.

Tracking network devices and subsystems

Most radio system owners rely on their radio equipment vendors in this area. This works well as long as you have a good vendor relationship. In a standards-based P25 system where equipment may come from different vendors, you should create and maintain a centralized, unified database for all network elements.

Tracking subscriber equipment

Maintaining subscriber information is important for day-to-day operations and for future planning, so it is easy to justify the cost/benefit for asset tracking tools.

Few systems have formal asset tracking processes for subscriber equipment. This is hard to understand, given that radios are expensive, and those who use asset tracking tools are so enthusiastic about their value.

Of course any database 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.

Publicly-funded projects often demand that you track any item worth more than $100. Good processes will mean fewer unpleasant surprises at audit, and give you solid information when upgrading or replacing your system in the future. Here are some guidelines.

- Delegate responsibility for keeping track of information to one person.
- Use maintenance records to track assets, and to assess reliability for replacement purposes.
- Control access for accountability
- Outsourcing maintenance services can compromise recording of system information. Establish clear, common processes with support partners.

“TAKE THE TIME TO UNDERSTAND WARRANTY AND SERVICE AGREEMENT AND ENTITLEMENT - THEY ARE NOT THE SAME. WARRANTY TYPICALLY ALLOWS FOR RETURN FOR REPAIR ONLY. YOU NEED A SERVICE AGREEMENT TO BE FULLY COVERED.”

ADMINISTRATION

Large multi-agency P25 networks demand significant active administration, but even small networks require proper set-up and active management.

Network configuration

In the majority of Public Safety systems, network 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 network configuration knowledge.

But radio systems are changing. This evolution makes network configuration skills and related processes paramount. Instead of single vendor hardware, they are much more software-driven and include inter-dependent sub-systems from different vendors.

A system should have at least one person fully versed in network configuration, even if, due to the increased complexity, it may be better still to rely on assistance from vendors for any major changes.

Subscriber management

While network configuration changes may be relatively infrequent, adding or removing subscribers, status changes or access to specific functions can be a daily event. Inter-system interoperability means the skills necessary to successfully manage subscriber units on the network side are growing in complexity and importance.

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

P25 programming is not yet standardized. System keys or advanced system keys preventing unauthorized cloning, programming or network access, vary between vendors. If you have different types of radios on one network, becoming proficient in programming different radio models is challenging and time-consuming, so you need to factor in the cost of this.

Dispatchers and consoles

Regardless of your maintenance arrangements, the equipment at the heart of your day to day business is your dispatch consoles. This is one of the major functions for any system operator – directing traffic, allocating tasks, identifying technical or safety issues.

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

Managing IDs, templates, and talkgroup names are vital, and are all functions that need to be staffed.

If a Console Sub-System Interface (CSSI) protocol is used to connect your dispatch systems to P25 Trunked systems, you will need to carefully monitor any changes in hardware, software releases, configuration, and policy changes across the entire network, anyhh of which can affect services and performance. Both a support team and a close regular cooperation with vendors is necessary to keep this complex environment running smoothly.

Time spent understanding your console options will result in better, future-proof decisions.

NETWORK OPTIMIZATION

Optimization is uncommon in Public Safety communications systems, which are often fine-tuned at the time of initial implementation and then left alone for their entire useful lives.

This section includes some suggestions for continuous improvement of the network.

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 and 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 notes. They can provide you with new operational or security functions.

Technology

Is your hardware and software up to date? Would upgrading some elements of the systems - for example base stations or servers - yield better performance or lower your costs?

People

It is common to see an organization go through the expense and disruption of the initial installation, but fail to take full advantage of system features or new improvements, for lack of commitment to ongoing training.

Training your users, technicians and administrators, and enforcing your standard operating procedures (SOPs) is vital to getting the most out of the system and user equipment you have invested in. Your initial training plan should include hands-on experience for all users, together with scheduled repeats and refresher courses.

Processes

Review your SOPs regularly, asking these questions:

- Is your system used in the best way?
- Are all the right people involved in standard communications procedures?
- Are some people involved, who should not be?
- Do some procedures put an unnecessary burden on users and slow down the exchange of information?

Operating costs

Are you paying more than you need, to other parties? Here are some aspects to consider that may substantially reduce your operating costs.

- You bought your system several years ago and agreed to pay a local Telco a high rate for the backhaul. Since then, new providers offer less expensive alternatives so switching providers may be feasible.
- You bought your system and radios from the same vendor and you are still paying a premium for new subscriber units. You may be able to negotiate a lower cost or purchase from another vendor.
- You are paying for a comprehensive, long-term maintenance agreement. You may be better re-examining its scope and dividing it, with separate software license agreements, and a service agreement with your local competent provider.

User experience

The opinions of your users are well worth considering. User satisfaction surveys are virtually unheard of among Public Safety organizations, yet conducting simple surveys regularly encourages people to voice their opinions – they will often generate ideas to improve your SOPs, or identify training needs.

The biggest subscriber training challenge is managing the expectations of young, cell-savvy officers.

Security

Encryption practices and related SOPs benefit from periodic reviews. For example, your system may have started with everyone using encryption, 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.

A regular review gives you the information and opportunity to maintain good processes and get the maximum benefit from your encryption.

Encryption and other security measures will be covered in a separate P25 Best Practice Guide.

MAJOR EVENT PREPAREDNESS

Your level of investment for major events depends upon your location and risk assessment. You need to invest enough to stay on air through critical events, ensuring power to your sites throughout.

The greatest barrier to effective emergency response is low levels of preparedness - lack of training, and being unfamiliar with emergency operating procedures. Technical issues come second.

This section outlines measures to prepare for major events, whether they are planned exercises, natural or man-made disasters.

Planning and preparation

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 you can look to local event history - is your jurisdiction at risk from floods, hurricanes, forest fires, blizzards, or earthquakes? Of course you will also need to plan for risks such as terrorist attack, multiple motor vehicle accidents, plane crashes and civil unrest.

- ☑ Identify, protect and prioritize your critical user groups in advance, and build them into your talkgroup structure.
- ☑ You will not have enough channels for all your users in extreme situations so your disaster planning must limit network access to critical users only.

- ☑ Define the complexity of your interoperability needs with a matrix – who needs to talk to whom?
- ☑ Plan how you will use encryption. Can you communicate effectively with all the necessary agencies and groups?
- ☑ Estimate how long different disaster scenarios might leave you without power, fuel or support. You may have to be independent for 72 hours or more.
- ☑ Invest in transportable networks that can be rapidly deployed.
- ☑ Maintain a cache of radios that all your mutual aid partners can use. A strike team needs to know where the caches are.
- ☑ Keep cached radios programmed, maintained and updated with the rest of your fleet – don't discover this has not happened when you are under pressure.
- ☑ Schedule and practice simulated emergencies with your interoperability partners annually. Take a lead from fire departments, who do this well.
- ☑ Ensure your procedures are thoroughly documented, easy to follow and easy to find. Ideally, they will be in both electronic and hard copy.

Resiliency

Often, low-risk system equipment gets the attention and funding, while crucial equipment is neglected. Ironically, most money is spent on standby controllers, which are seldom used. When you prioritize, 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),
- poor wiring (people tripping over cables in shelters or other equipment rooms).

Performance

While your level of investment for events depends on your location and risk assessment, there are some basic principles you should build in to your day-to-day planning.

- ☑ Eliminate single points of network failure.
- ☑ You will lose power – 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 your sites throughout.
- ☑ In a major disaster, telephone systems (especially cell phone systems) frequently fail.
- ☑ Plan for a scenario in which your computer systems (including CAD) are not available.

Site equipment

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

A generator may take five to seven minutes to fire up, which may leave officers without communication at a critical time. In an emergency, utilities and propane companies may not have power to pump fuel.

Coverage

What will happen to your ability to communicate if you lose a site? Some systems use geographically-distributed back-up sites (typically, mutual aid channels). Others over-provision the sites so that every important area of operations is covered by more than one site. While this is highly recommended, it is expensive and creates technical challenges, especially in multicast system configuration, requiring finely-tuning roaming performance of subscriber units.

Capacity

The basic rule of thumb is to have enough capacity to handle three times more traffic than your typical weekly busy hour. Any more than this becomes impractical and costly, while less is likely to be insufficient. Verify this against your circumstances: for a smaller rural agency it may be overkill, for a large metropolitan area, you may want to plan more capacity.

In every case, you need to limit traffic on your system to those who need to be involved. Contingency plans for emergencies should include means to cut off “roamers” and anyone that does not need to participate. Depending on your configuration, allowing people to monitor activities while they are scanning means additional groups will load, which may choke your system.

Be prepared to completely isolate a site in an emergency, especially on larger multi-site systems as it will likely improve capacity for the incident.

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

Ultimately though, your system design should not require any substantial changes on how it is used in an emergency, if emergency capacity has been factored into the system design.

“THE BEST THING ABOUT INTEROPERABILITY IS THAT EVERYBODY CAN TALK TO EACH OTHER. THE WORST THING ABOUT INTEROPERABILITY IS THAT EVERYBODY CAN TALK TO EACH OTHER.”

INTEROPERABILITY

The only interoperability 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 in the radios will not help unless your users understand how to take advantage of them.

Keep your processes simple and make sure all your users are well trained. Do not spend large sums of money on high tech devices when the best solutions may be operational.

Interoperating with other agencies

Interoperability and roaming are often confused: ensure that everyone understands the difference.

Planning for critical event interoperability with partner agencies is a daily task, so that you are prepared for rapid deployment with your interoperability partners.

At the outset, you will need to establish agreement on process and technology with those you will need to work with in a disaster.

- ☑ Define the complexity of your interoperability needs with a matrix of who will need to talk to whom.
- ☑ Identify critical user groups in advance and build these priorities 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. Allow only critical groups to operate.
- ☑ Identify the need for unencrypted interoperability channels for external agencies.
- ☑ Use transportable networks and portable repeaters
- ☑ 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 which allows you to connect your network to other radio networks. This might be invaluable for interoperability, but it requires significant effort and ongoing cooperation between participating network owners.

SOPs 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 scenarios regularly are important to your overall preparedness.

Everyone needs to know how to interoperate before they need it 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.

Training with the equipment should include training the users to stay off their radios unless they urgently need to communicate.

A major benefit of regular training and drills is to identify weaknesses in your equipment, procedures, or people. You then have the opportunity to improve. Reviews and debriefs after training 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.

To summarize:

- ☑ Factor in the roles of other 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.
- ☑ Empower dispatchers to turn off non-priority talk groups during events.

- ☑ Uncontrolled interoperability consumes valuable bandwidth – establish process and train users in it.
- ☑ Train for different scenarios, including reduced communication capacity.

"CONSIDER HOW LITTLE RADIO TRAINING POLICE OFFICERS GET. MOST HAVE FOUR DAYS EACH YEAR ON FIREARMS, YET ALMOST NONE ON RADIO. THEY USE THEIR RADIOS CONSTANTLY, WHILE OFTEN NOT DRAWING A FIREARM DURING AN ENTIRE CAREER."

POST-EVENT PERFORMANCE TESTING

- ☑ Perform high level system testing after every event, storm and incident.
- ☑ Review network performance and integrity against specification and expectation.
- ☑ Debrief - did your communications perform well?

INSIGHTS

All quote bubbles are direct insights from the industry participants at the Tait P25 round table discussions. To find out who the participants were, visit **www.p25bestpractice.com**

Contractors and advisors need rigorous training for system key use.

Moderate new talkgroups so people don't get swamped. New groups should be needs based. Applications for new ones should have visibility.

When the radios are in tune, suddenly the system works better!

Understand the implications of software upgrades (or not upgrading) on your interoperability.

Hold combined training days with your interop partners. Pool funding.

Consider a dedicated radio alias manager as a vital admin role.

A radio guy can learn IT, but IT won't do radio. You won't find them (IT) up a mast at two in the morning with a baseball bat, knocking ice off the antennas. They will only remote in.

Optimization issues are secondary to reliability for mission-critical communications.

Hospitals are keen to understand radio comms and interoperate with Public Safety.

Include transit, schools, anyone on your municipal network – they are likely to be less familiar with radio so will benefit from inclusion. Involve everyone in emergency drills.

Track repairs. Barcode all equipment, build a spreadsheet and record every touch. Your database should log every radio so all are tracked, including preventative maintenance. This is required for federal grants.

While frequently requested, Over-The-Air-Programming is infrequently used.

Empower dispatchers to turn off non-priority talk groups during events.

Learn more and subscribe at

www.p25bestpractice.com

www.taitradio.com