June 2019

TETRA: Today and Tomorrow

TRUSTED · ALWAYS · EVERYWHERE

Important Note

The opinions and information given by TCCA in this paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, TCCA is unable to guarantee the accuracy or completeness of any information contained herein. TCCA, its employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information.

First issued by TCCA's TETRA Industry Group, June 2019.

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

TRUSTED

• CONTROL

Mission critical communication users often operate in dangerous situations within challenging environments. Trusted communication capabilities are very important for these users, and in extreme situations the communication channel is a vitally important – it can literally save lives. Therefore it is essential that critical communications users can control the communications. The key control aspects are service availability, quality of service, operational management and cost.

Communication services need to be available always and everywhere – it is impossible to predict when and where incidents take place. Good geographical radio coverage (both on network and off network) is the most important vehicle needed for high service availability. Resiliency solutions (for the critical communication network, for the transmission network …) are other important high availability enablers.

However, high service availability is not enough. The quality of communication services needs to match with user requirements. This means that communication services need to seamlessly support users' operational processes, users need to have interoperable services and prioritisation of communication needs in order to work effectively between users/user organisations and switch efficiently between routine and emergency communication.

Communication needs vary depending on incidents and applied operational processes. It is important that there are means for adjusting the communication structure efficiently – this includes for example creating new communication groups, managing group memberships and combining different groups. This kind of operational management needs to be addressed autonomously and independently by mission critical user organisations.

Costs of mission critical communication are typically covered from governmental, state or city budgets. There is careful planning for annual and longer term framework budgets, and critical communication costs need to be predictable. This same principle holds both for CAPEX and OPEX costs.

The critical communication community needs to have control over the above mentioned aspects. There are different ways to implement this control, such as contractual setup with the service provider or acquisition of related assets.

• EXPERTISE

Designing and building mission critical service requires special expertise – a skill TETRA vendors and integrators have a proven record of delivering. The world of police, fire, rescue, and other industrial professionals are so vastly different than that of consumers; the first responders deliver mission critical services to society and need to be supported by mission critical expertise and networks.

TETRA vendors transfer expertise to owners of TETRA networks to enable them to operate their networks in a way that exactly matches their operational needs. Expertise from one special installation somewhere in the world is being transferred to other customers elsewhere.

Employees in companies providing TETRA solutions have decades of experience, bringing the expertise needed to provide the mission critical solution that the police in the dark alley at night and the fire and rescue team going into a burning building rely on.

The front line staff who use radios every day are employees who have a legal right to a safe working environment. The responsible management therefore rely very much on special expertise in the design and build of mission critical solutions.

• LONGEVITY

TETRA equipment lasts. Investments in infrastructure easily cover 10-15 years in the core and even longer for base stations. Devices have been shown to have a typical lifespan of 7-10 years in the field. Users, operators and investors rely on the very well documented standard, constantly being maintained and improved by ETSI.

TETRA has been developed from the bottom up to meet the needs of mission critical users. ETSI has developed and enhanced the TETRA standard over many years, bringing the number of dedicated features and functions to well over 300 - functions and features that are useful today and will be for many years ahead.

TETRA provides multi-vendor choice - allowing customers to switch from one supplier to another without sacrificing the multitude of functions and features TETRA provides.

Many national networks have been upgraded in the last five years and had their life extended – some have maintenance contracts beyond 2035.

Control room vendors have their systems tightly integrated with TETRA networks, and many users have optimised operational processes around the flexible capabilities of TETRA.

ALWAYS

• AVAILABLE

TETRA network availability is critical to ensure mission-critical communications. TETRA networks are designed to fulfil very high availability levels – typically between 99.95 to 99.999% for operation of TETRA core and access (base station) components.

This level of availability can only be achieved by using redundancy in order to protect against equipment failures. The status of the redundant components must be kept synchronised with the active components to allow instant failover without the intervention of the network operator.

Battery backup and component redundancy can also be included in the base station design in order to improve availability. Furthermore, coverage redundancy by overlapping base station sites may be considered in the network design to further enhance availability.

In addition to equipment redundancy, link redundancy to the base station must also be considered. Link redundancy is essential to achieve high network-wide coverage availability, important for TETRA radio users to stay in contact with the control room and other TETRA radio users outside the coverage area of the base station.

As a last resort, TETRA base stations support local fallback mode, allowing TETRA radio users to continue communication within the base station coverage area when no links are available to the core infrastructure. Specific TETRA features are developed to give base stations with network-wide coverage priority above isolated ones.

TETRA networks are designed and built to fulfil these mission-critical availability requirements, and TETRA network operators have full control in order to benefit from these high availability solutions.

• INSTANT

When dealing with mission critical communication, time is of the essence; instant reactions in emergencies are crucial as even a small delay can mean the difference between life and death. Similarly, within business critical communication, instantly available communication and information is vital to ensure a minimum of downtime and thereby a minimum of economic losses.

With instant communication at its core, TETRA is built for such situations. Call setup is immediate, and important calls can be given pre-emptive status to ensure timeslot availability. Furthermore, the caller is given instant visual and audible feedback in case the called party is unreachable or busy.

Likewise, SDS messages are delivered instantly so can also be used for emergency purposes. The instant SDS feature enables real-time tracking of mobile devices and on-the-spot DGNA group creation, making it possible to deliver a fast and accurate response to emergencies in the field.

TETRA instantly provides comprehensive and accurate voice and data recording facilities and a wide range of logging facilities for CDR, enabling fast and easy incident reconstruction and traceability. Among other things, this means immediate access to voice recordings for playback, eliminating the need for additional clarifying calls in life-critical situations where time is of the essence.

A TETRA system is up and running as soon as the power is switched on. In case of operational failure, there is a built-in automatic recovery system supporting switchover to hot standby components or graceful degradation of the system in order to maintain instant communication.

• SECURE

Communication security is an essential prerequisite for the success of mission critical operations.

The protection against eavesdropping and manipulation of voice and data as well as the exclusion of third-party use are therefore indispensable requirements for mission critical communication systems. This is particularly true against the background of increasing cybercrime.

TETRA's security features, developed by mission critical communication experts, are modular and complement each other to meet the security requirements of mission critical applications. They are an integral part of the standard and thus guarantee security even when using devices and infrastructure from different manufacturers.

The TETRA standard supports powerful mutual authentication of a devices on the one hand and the network on the other. This makes it possible for a TETRA system to control the access to it and for a device to check if a network can be trusted. In addition, applications enable authentication down to the user level.

If a device is lost or stolen it is fundamental in a mission critical environment to exclude this device from using the network. TETRA supports different options for a direct secure disabling over the air. The disabling can be either temporary, which leaves the possibility to enable again or permanent, which is irreversible.

As any air interface is very vulnerable to eavesdropping, TETRA provides air interface encryption where user and signalling information is encrypted over the air interface between devices and infrastructure, both for individual and group communications. The air interface encryption mechanism is available for voice and data and direct mode operation. The use of several encryption algorithms, both standard and proprietary, also is supported.

End-to-end encryption service can be realised in TETRA in any number of ways. This means that a user organisation may easily tailor an end-to-end encryption system to its own requirements. This flexibility is essential und unique in TETRA, which can be implemented in many forms for different user groups.

The security management features of TETRA allow the user organisation to control, manage and operate the individual security mechanisms. They form the heart of the security and guarantee that the security features are integrated into a consistent security system. As key management is the most essential security management function, a large number of features are integrated to support it. The TETRA standard security mechanism will be constantly updated to guarantee secure communication beyond 2030.

In addition the all-IP design of TETRA networks enables the use of state-of-the-art external protection devices such as firewalls.

TETRA networks are able to operate either completely stand alone, i.e. disconnected from the Internet, or integrated into the user organisations communication and IT environment, which enables the use of the protection mechanism of the organisation against cyberattacks and other threats.

TETRA devices are equipped with closed and secure operating systems, which complete the leading edge TETRA system security.

EVERYWHERE

• CUSTOMISED COVERAGE

In mission critical operations, communication services need to be available everywhere as it is impossible to predict where incidents and, emergencies and disruption of operations may occur.

Extensive geographical network radio coverage is fundamental even in sparsely populated areas such as rural, mountain or desert regions where there is usually no or insufficient service from public cellular networks.

TETRA can provide rich and efficient off-network communication capabilities that allow field users to communicate everywhere (even outside network coverage) and in any occurrence (when the network is unavailable, overloaded, or to communicate independently from the network for local operations) through direct connection between devices (DMO – Direct Mode Operation).

Off network direct communications can be further optimised in terms of coverage range through the use of devices acting as DMO repeaters or DMO gateways, the latter basically providing local extension of a network base station to users operating in DMO (e.g. to provide immediate and prompt in-tunnel or in-door service).

Only dedicated communication networks can provide such a required level of service coverage and TETRA is natively conceived and constantly upgraded to provide extensive and cost effective coverage. TETRA can operate in low frequency UHF bands thus minimising the required number of network sites and the high level of competition typical of the TETRA market leads to a continuous product improvement. Today TETRA radio terminals and base stations offer extremely optimised receivers with sensitivity levels well beyond the minimum required by the standard, thereby dramatically further improving TETRA coverage capabilities and cost effectiveness.

• OFF NETWORK

There are always circumstances both planned and unplanned when it is essential for mission critical users to operate outside the coverage of their network. It is a fundamental requirement to ensure that communications can be maintained between operational groups of users regardless of the scenarios they find themselves in. Operation outside network coverage might be needed for a variety of reasons: to compensate for poor network signal strength areas, when service from a local base station site is lost, or there is a prior knowledge of operating in an area where there is no or poor network coverage. TETRA provides a range of off network services to enable users to retain key services such as group calls, point to point calls, emergency calls and pre-emption, text messages and to maintain security and encryption used on network. TETRA's off network services are comprehensive and provide:

- Back-to Back operation - communication directly between two or more devices
- Repeater Operation – Range extension using a standard TETRA device acting as a relay between other devices
- Gateway operation – Range extension back to the TETRA network, connecting devices working off-network to the TETRA network to maintain wide area coverage.
- Long range communications – back-to back operation can extend to more than 3km for handheld devices and much further for in-vehicle devices.

Off network services are provided in all standard TETRA devices and can be activated by the user simply selecting the required mode of operation.

• VARIETY OF DEVICES

The world's mission critical users have a wide variety of requirements and use cases. Devices need to be available for many different types of use and be robust enough to withstand use in extreme environments while still delivering return on investment through length of service.. Products are designed from first principles to be mission critical and secure, negating the need for constant security patches. Devices operate in a real time manner, performing their communications tasks within strict performance criteria and have predictable and repeatable responses to all critical actions (e.g. emergency button press), regardless of how the device is being used. The TETRA ecosystem covers a wide variety of use cases and devices are available in many form factors to suit user requirements. These include devices designed for front line public safety usage, for use in a range of vehicles: motorcycles, cars, vans, aircraft, boats, within control centre environments and for covert installations. Devices are designed and built for durability, with a field deployment expectation of between five and seven years and supported life of much longer. Devices are designed with components that have long term support ensuring that products can be manufactured, maintained and supported throughout their life. All devices are supported by a wide variety of specialist accessories to fit the exacting needs of mission critical users' demands. All TETRA devices are subject to TCCA's stringent and independently managed interoperability testing process, ensuring that a wide variety of cost effective compatible solutions from multiple vendors are available.