ETSI TR 104 246 V1.1.1 (2026-01)

TECHNICAL REPORT

TCCE Security;
Application of ETSI CVD process within TCCE

Reference
DTR/TCCE-06210

Keywords
coordination, security, TETRA, vulnerabilities

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Security vulnerabilities play a crucial role in all lifecycles of systems, components and services of telecommunication networks. The ETSI Coordinated Vulnerability Disclosure (CVD) process provides a way for Finders to disclose vulnerabilities found in TETRA standards. These vulnerabilities may have an impact on the security of numerous TETRA networks worldwide. This coordinated disclosure will help to respond to security vulnerabilities, to evaluate potential vulnerabilities, to mitigate confirmed vulnerabilities and therefore allow to reduce the risk of compromise.

The main clauses of the present document contain the following information:

- Clause 4 gives an overview on TETRA standardization, typical network environments, architectures and operations.
- Clause 5 outlines options to mitigate vulnerabilities in TETRA networks and explains the complexities of update processes.
- Clause 6 explains the ETSI CVD in the TETRA context.

1 Scope

The present document defines the policy of the Technical Committee (TC) Terrestrial Trunked Radio and Critical Communications Evolution (TCCE) in the ETSI Coordinated Vulnerability Disclosure (CVD) [i.1]. This policy is based on the ETSI CVD and applies to ETSI deliverables of the TCCE [i.2] only.

The present document is intended for all roles in the ETSI CVD process and provides guidance to: Finder, ETSI CVD Steering Committee, TC TCCE and the rapporteur(s) of the impacted standard(s). It details the process for Finders of potential vulnerabilities, explains the actions of the TC TCCE and may be used as guidance for all roles.

For Finders not acquainted with Terrestrial Trunked Radio (TETRA) the present document outlines typical TETRA network environments and explains typical constraints and complexities in vulnerability mitigations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI Coordinated Vulnerability Disclosure (CVD).

[i.2] ETSI Technical Committee (TC) Terrestrial Trunked Radio and Critical Communications Evolution (TCCE).

[i.3] ETSI TR 103 838 (V1.1.1): "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.4] ETSI EN/TS 3/100 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[i.5] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance).

[i.6] ETSI EN/TS 3/100 392-3 series: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

ETSI CVD Steering Committee: committee which, for each vulnerability report, triages the vulnerability, interacts with the Chair and the ETSI Technical Officer of the TC TCCE and the rapporteur(s) of the impacted standard(s) to resolve the vulnerability, and communicates on the progress of the handling of the vulnerability report with the Finder

NOTE: As defined in [i.1].

finder: individual or organization who has found a potential vulnerability

NOTE: As defined in [i.1].

manufacturer: designer or manufacturer of TETRA equipment or components of TETRA networks

Mobile Station (MS): physical grouping that contains all of the mobile equipment that is used to obtain TETRA services

network operator: organization that operates a TETRA network

subscription: permit for a Mobile Station to use a TETRA network, characterized by a subscriber identity and, optionally, an authentication key provided by the TETRA network

TCCE Technical Experts Group (TCCE TEG): expert group consisting of delegates of manufacturers and operators, which looks for a solution to reported vulnerabilities.

TETRA network: SwMI with one or more Base Station(s) broadcasting the same Mobile Network Identity

user organization: organization that holds subscriptions of a TETRA network

vulnerability: security weakness that can be abused to cause unintended behaviour

NOTE: As defined in [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BS	Base Station
CRA	Cyber Resilience Act
CVD	Coordinated Vulnerability Disclosure
DMO	Direct Mode Operation
EU	European Union
IOP	InterOPerability
ISG	Industry Specification Group
ISI	Inter-System Interfaces
ITSI	Individual TETRA Subscriber Identity
K, K2	authentication Key
MS	Mobile Station
NCSC	National Cyber Security Centre
PAMR	Public Access Mobile Radio
PMR	Private Mobile Radio
SDS	Short Data Service
SIM	Subscriber Identity Module

SwMI	Switching and Management Infrastructure
TB	Technical Body
TC	Technical Committee
TCCA	The Critical Communications Association
TCCE	Terrestrial Trunked Radio and Critical Communications Evolution
TEDS	TETRA Enhanced Data Service
TEG	Technical Experts Group
TETRA	TErrestrial Trunked RAdio
TF	Technical Forum
TMO	Trunked Mode Operation

4 Overview of TETRA networks

4.1 Standardization of TETRA networks

ETSI's Technical Committee (TC) Terrestrial Trunked Radio and Critical Communications Evolution (TCCE) is responsible for the design and standardization of Terrestrial Trunked Radio (TETRA) and its evolution to critical communications mobile broadband solutions.

TETRA standards define the TETRA air interface, TETRA algorithms of the air interface, the TETRA speech codec and external interfaces of TETRA networks. This enables the development and deployment of interoperable solutions. To ensure interoperability, The Critical Communications Association (TCCA) has established an Interoperability (IOP) certification process managed by TCCA's Technical Forum (TF). This allows for an open multi-vendor market for TETRA infrastructure and mobile equipment.

The standardized frequency bands range from 100 to 900 MHz. TETRA networks are narrowband systems optimized for voice services and Short Data Services (SDSs). The use of TETRA Enhanced Data Service (TEDS) allows for higher packet data rates depending on bandwidth, modulation and coding rate. However, as these narrowband systems provide moderate data rates, TETRA data services are usually not used to deploy firmware updates to Mobile Stations (MSs).

4.2 Typical TETRA network environments

TETRA is used in Private and Public Access Mobile Radio (PMR and PAMR) networks. Major markets include:

- Public Safety
- Transportation
- Utilities
- Government
- Military
- Commercial and Industry
- Oil and Gas

4.3 TETRA network architectures

In TETRA standards TETRA networks comprise Mobile Stations (MSs) and components of the Switching and Management Infrastructure (SwMI).

A MS comprises all of the mobile equipment that is used to obtain TETRA services. In TETRA networks a MS may be directly provisioned with the Individual TETRA Subscriber Identity (ITSI) and authentication Keys (K or K2 or both) or instead make use of a removable Subscriber Identity Module (SIM). MSs are available in different device types, e.g. handheld devices, mobile devices installed in vehicles or aircraft or fixed stations with wireless access to the network.

The SwMI comprises the network equipment, e.g. Base Stations (BSs), switching centres and additional system components. Only the relevant SwMI interfaces are standardized by ETSI, the SwMI itself is not standardized. Typically a TETRA network is supplied by one vendor of the SwMI components and one or multiple vendors of MSs.

As TETRA is a cellular network technology it is based on a single or multiple Base Stations (BSs) that cover the service area. Typically BSs are connected by wire or microwave links to switching centres, while for high availability requirements redundant connections are preferred. The terrestrial cell size may be limited by different factors. For instance the path delay may allow terrestrial cell sizes up to 58 km radius when using phase modulation. The use of Air-Ground-Air service may further extend cells radius [i.4]. Anyway, the typical design range of cell sizes primarily depends on capacity requirements as well as terrain in rural areas or building density in urban areas.

The deployment sizes of TETRA networks can vary in the following range:

- a single or a few Base Stations (BSs) covering a local site, e.g. an industrial plant;
- tens of BSs covering urban areas, e.g. a public transportation network; or
- hundreds to thousands of BSs covering an entire country, e.g. a national public safety network.

The number of subscriptions can vary according to the user organizations. Industrial plants may use tens to hundreds of subscriptions, public transportation networks up to over a thousand subscriptions. In national public safety networks the number of subscriptions can exceed one million. Such national networks typically serve multiple independent user organizations, e.g. police, fire brigades and emergency medical services in regional organizations. Typically these user organizations provide and maintain their own MSs.

TETRA can be used in Trunked Mode Operation (TMO) and Direct Mode Operation (DMO). TMO is the primary mode of operation used by TETRA networks. Each MS connects to a BS in the respective service area. Control and user data are transferred through the network between the MSs, e.g. from the calling MS to multiple called MSs in a group call. DMO is independent of cellular infrastructure services and relies on direct communication between MSs. DMO is primarily used for local short range communications or where TMO is not reliably available. DMO can be combined with repeaters to extend the range as well as with gateways that connect DMO and TMO.

TETRA networks can also be connected to other TETRA networks to allow the migration of MSs from home into visiting networks. This feature is standardized using Inter-System Interfaces (ISI) covered by ETSI EN/TS 3/100 392-3 series [i.6].

4.4 TETRA network operations

Most user organizations in TETRA networks require high availability. For example police, fire brigades, emergency medical services or critical operations personnel in industrial plants form typical user organizations. Due to their mission critical duties these users demand high availability and fast remediation of communication service degradations.

For many user organizations the availability of the communication services can be seen as the most important security objective. Almost all TETRA networks operate continuously 24 hours a day. Various technologies are applied to support high availability and fast disaster recovery of the SwMI, e.g. redundant backhaul network design, redundant active or standby components, uninterruptable power supplies and backup solutions.

5 Mitigation of vulnerabilities in TETRA networks

5.1 Options to mitigate vulnerabilities in TETRA networks

As outlined in clause 4.1 implementations of the TETRA air interface, TETRA algorithms, the TETRA speech codec and external interfaces of TETRA networks follow ETSI standards. Therefore vulnerabilities in those standards may have direct impact on a high number of components in TETRA networks worldwide. Usually these vulnerabilities impact MSs and/or components of the SwMI, e.g. BSs, switching centres or additional system components.

Options to provide mitigations in any of these components are:

- changes in configuration;

- updates of embedded firmware;
- updates of software; and
- updates, extensions or replacements of hardware.

Compared to mobile broadband networks the data bandwidth of TETRA is very limited. This generally prevents firmware updates of MSs over the TETRA air interface. The following clauses explain the complexities of the update process and the vulnerability mitigation at MSs and in SwMI.

5.2 Update processes in TETRA networks

Update processes in TETRA networks typically contain multiple steps of different stakeholders. To update components all stakeholders have to work together. To illustrate this complexity the following list shows an example of the necessary steps in the mitigation of a vulnerability found in TETRA standards. In this example all of the following steps need to be performed by the respective roles:

- vulnerability assessment and definition of mitigations by ETSI TCCE as defined in clause 6.4;
- adaption and approval of the revised specification by ETSI TCCE as defined in clause 6.4;
- adaptation and approval of revised TETRA interoperability specification by TCCA TF;
- development of updates and quality assurance tests by manufacturers;
- cross-manufacturer TETRA interoperability tests and certification of MS and SwMI and/or of MS and MS or of SwMI and SwMI in test centre by certification body;
- in some networks additionally: certification/re-certification of MS and/or approval tests of SwMI components in tests centres by network operator;
- release of updates by manufacturers; and
- roll-out of updates to TETRA network components (MSs and/or SwMI) by network operator and/or user organizations.

Some of these steps may overlap and are not necessary consecutive. After the last step is completed and updates are installed on all affected components, the vulnerability in an affected TETRA network has been mitigated. The following clauses explain the options for mitigations at MSs and in SwMI in more detail.

5.3 Vulnerability mitigation at Mobile Station

Vulnerability mitigations at the MS may comprise configuration changes and/or updates of firmware or the exchange of MS hardware. Due to bandwidth constraints MS firmware updates are not provided over the TETRA air interface. For configuration or firmware updates the MS has to be brought to a particular location where updates are applied via wired connection or secure local wireless networks. Further methods may be provided by MSs that include additional mobile broadband network access.

In large TETRA networks typically every user organization maintains and manages their own MSs. This results in different update processes of varying efficiency. Based on MS quantities, organizational structures and available funding the required time for updating an organization's fleet can last from weeks to years.

For a typical MS configuration or firmware update all MSs of an organization have to be present at a particular location. In order not to massively hinder day-to-day operations this is done in batches. Whenever a subset of MSs can be present at a suitable location the MSs are temporarily taken out of service for the duration of the process.

Only user organizations can deploy MS configuration and firmware updates on their own MSs. TETRA network operators typically cannot enforce updates of MSs affected by vulnerabilities. The disabling of a single MS by the network operator might be acceptable for some user organizations, but the uncoordinated disabling of fleets of MSs by the network operator would usually not be compatible with the high availability requirements of most user organizations.

5.4 Vulnerability mitigation in SwMI

Vulnerability mitigations in SwMI may comprise configurations changes and/or updates of software or hardware of SwMI components. Updates of SwMI components usually temporarily decrease network availability down to service outages. Therefore updates may be scheduled to low traffic periods in order to reduce downtime or rolled-out in service windows that have been agreed before with the user organizations.

Updates may be installed remotely or on-site. Especially on-site installations at multiple locations (e.g. all BSs of a large network or all geo-redundant components) can cause high expenses and long delays in the roll-out process.

6 ETSI CVD in TCCE TETRA context

6.1 Roles and responsibilities

ETSI CVD contains a definition of roles and responsibilities [i.1]. The following list specifies this definition further for the context of TC TCCE in the TETRA environment:

- **Finder:** individual or organization who has found a potential vulnerability in the TETRA standards.
- **ETSI CVD Steering Committee:** committee which, for each vulnerability report, triages the vulnerability, interacts with the Chair and the ETSI Technical Officer of the TCCE and the rapporteur(s) of the impacted standard(s) to resolve the vulnerability, and communicates on the progress of the handling of the vulnerability report with the Finder.
- **TCCE Chair:** chair of the ETSI Technical Committee Terrestrial Trunked Radio and Critical Communications Evolution.
- **TCCE Technical Officer:** technical officer of the TCCE.
- **Rapporteur(s) of the impacted standard(s):** rapporteur(s) of the impacted TCCE standard(s).
- **TCCE:** delegates of Technical Committee Terrestrial Trunked Radio and Critical Communications Evolution.
- **TCCE TEG:** TCCE Technical Expert Group consisting of delegates of manufacturers and operators, which looks for a solution to reported vulnerabilities.

6.2 Reporting obligations of network operators

As outlined in clause 4, TETRA networks are in operation in critical infrastructures or public safety. Network operators in these markets have to follow particular national regulations and laws in cybersecurity. The details are subject to national legislation, but typically network operators in critical infrastructure or public safety are obligated to share information on vulnerabilities with the respective National Cyber Security Centres (NCSCs). By this confidential information exchange vulnerability reports are not disclosed to the public.

6.3 Reporting obligations of manufacturers

Cybersecurity regulations may require manufacturers to report vulnerabilities in their products. These reporting obligations are independent from ETSI CVD and may require the manufacturer to follow additional processes outside the scope of the present document.

For example, in the European Union (EU) the Cyber Resilience Act (CRA) may require manufacturers of connected devices to immediately report any actively exploited vulnerabilities in their products [i.5]. As this does not apply to products for national security or defence purposes or to products that process classified information, it may be required for TETRA products used in all other markets in the EU.

6.4 ETSI CVD process in the TCCE environment

Table 1 shows the ETSI CVD process in the TCCE environment. To illustrate the process in more detail the four steps of the ETSI CVD [i.1] have been divided into sub-steps.

Table 1: ETSI CVD process in TCCE environment

Step No	Leading role	Involved role(s)	Action listed to ETSI CVD [i.1]	Follow-up step(s)
0	Finder	ETSI CVD Steering Committee	Submit vulnerability report to ETSI	1.1
1.1	ETSI CVD Steering Committee	TCCE Chair, TCCE Technical Officer, Rapporteur(s)	Once a vulnerability report is submitted by a Finder, it is shared with the ETSI CVD Steering Committee. They triage the vulnerability and share the report with the Chair and the ETSI Technical Officer for the relevant TB/ISG and the rapporteur(s) of the impacted standard(s).	1.2 and 2.1
1.2	ETSI CVD Steering Committee	Finder	The Finder will receive an email from the ETSI CVD Steering Committee that the report has progressed to the impacted TB/ISG.	none
2.1	TCCE Chair	TCCE, TCCE Technical Officer, Rapporteur(s)	Next, the impacted TB/ISG assesses the vulnerability report at a committee-wide meeting. The vulnerability is assessed, and either accepted or rejected as to its validity.	2.2 and (3.1 or 5)
2.2	TCCE Chair	Finder	In either case, the Finder is notified.	none
3.1	TCCE Chair	TCCE TEG	If the vulnerability report is assessed as valid, the impacted TB/ISG works to create a resolution. The resolution is prepared and adopted using the ETSI decision-making procedures by the impacted TB/ISG,	3.2 and 4
3.2	TCCE Chair	Finder	And the Finder is informed by email of what the resolution is and that it has been made.	none
4	TCCE Chair	TCCE	ETSI aims to resolve all valid vulnerabilities within 90 days of reporting though it may take longer for complicated fixes.	5
5	none		End	none

6.5 Example time frames for resolving vulnerabilities in the TETRA standards

Time frames for resolving vulnerabilities in TETRA standards are mainly influenced by the following factors:

- the complexity of the resolution; and
- the severity of the vulnerability assessed by TCCE TEG.

The complexity of the resolution in TETRA standards is determined by the appropriate technical solution and the number of impacted ETSI deliverables.

The severity rating provides an assessment of the impact on confidentiality, integrity and availability. It also takes into account how easily the vulnerability could be exploited by an attacker in TETRA networks [i.3].

Table 2 shows three example time frames for the resolving of vulnerabilities in TETRA standards that are explained below.

Table 2: Example time frames for resolving vulnerabilities in TETRA standards

Example	Complexity of the resolution	Severity rating of the vulnerability by TCCE TEG	Example time frame for resolving vulnerability in TETRA standards
1	low	critical impact	up to three months
2	medium	medium impact	three to six months
3	high	low impact	more than six months

Example 1 represents a vulnerability that has a low complexity in the resolution and has been assessed by TCCE TEG to a critical impact. An example is a vulnerability in one ETSI deliverable that allows to exploit it in TETRA networks, but that can be easily resolved e.g. by a change in configuration that can be applied remotely and has been tested before.

Example 2 represents a vulnerability that has a medium complexity in the resolution and has been assessed by TCCE TEG to a medium impact. An example is a vulnerability in one ETSI deliverable that needs some adjustments.

Example 3 represents a vulnerability that needs a complex mitigation and has been assessed by TCCE TEG to a low impact. An example is a vulnerability that affects multiple ETSI deliverables and IOP specifications that need to be updated.

6.6 Example time frames for resolving vulnerabilities in TETRA networks

As explained in clause 5.1 vulnerabilities in TETRA standards may have direct impact on a high number of components in TETRA networks worldwide. Time frames for resolving vulnerabilities in TETRA networks depend on multiple parties, have a wide variance and are therefore difficult to estimate.

To mitigate a vulnerability in components of a TETRA network typically one or more options outlined in clause 5.1 have to be chosen. These update processes may require very different time frames. As outlined in clause 5.2 also the number of parties involved can be seen as an important influence.

Time frames for resolving vulnerabilities in TETRA networks are substantially influenced by:

- the complexity of the mitigation as outlined in clause 5.2;
- the number of parties involved in the mitigation as outlined in clause 5.2; and
- the severity rating of the vulnerability assessed by TCCE TEG.

Table 3 shows three example time frames for resolving vulnerabilities in TETRA networks that are explained in the following.

Table 3: Example time frames for resolving vulnerabilities in TETRA networks

Example	Complexity of the mitigation	Number of parties involved	Severity rating of the vulnerability by TCCE TEG	Example time frame for resolving vulnerability in a TETRA network
1	low	low to medium	critical impact	three to six months
2	medium	low to medium	medium impact	six to 12 months
3	high	high	low impact	more than 12 months

Example 1 represents a vulnerability that has low complexity in the mitigation and involves an easily manageable low to medium number of parties. An example may be a mitigation that involves the change of a SwMI parameter that is defined in the TETRA standards, has been tested before in IOP tests with all relevant components and can be applied remotely on all affected SwMI components. Such a change may be evaluated by the SwMI manufacturers and applied by the network operators in a priority process for critical vulnerabilities within three to six months.

Example 2 represents a vulnerability that has medium complexity in the mitigation and involves an easily manageable low to medium number of parties. An example may be a mitigation that involves software updates of SwMI components that need to be tested by the manufacturers but does not need new IOP tests of the affected components.

Example 3 represents a vulnerability that has high complexity in the mitigation and involves a high number of parties. An example may be a mitigation that demands firmware updates of MSs as outlined in clause 5.3.

History

Version	Date	Status
V1.1.1	January 2026	Publication