ETSI TR 102 512 V1.1.1 (2006-08)

Technical Report

Terrestrial Trunked Radio (TETRA); Security; Security requirements analysis for modulation enhancements to TETRA

Reference

DTR/TETRA-06139

Keywords

analysis, security, TETRA

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

1 Scope

The present document updates the threat analysis presented in ETR 086-3 [1] with respect to new services and capabilities offered by the enhancements to TETRA that aim to provide alternative modulation schemes with a view to offering higher data transmission rates.

NOTE: The analysis provided by ETR 086-3 [1] remains valid and the recommendations made by that document remain in force.

In clause 7 the analysis identifies security extensions required for EN 300 392-7 [3].

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

[2] ISO/IEC 9798-2: "Information technology - Security techniques - Entity authentication: Part 2: Mechanisms using symmetric encipherment algorithms".

[3] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[4] ETSI TR 101 053-1: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".

[5] ETSI TR 101 053-2: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".

[6] ETSI TR 101 053-3: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".

[7] ETSI TR 101 053-4: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".

[8] ETSI TR 101 052: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1".

[9] ETSI EN 300 392-5: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 5: Peripheral Equipment Interface (PEI)".

[10] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); requirements of Law Enforcement Agencies".

[11] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[12] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[13] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[14] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[15] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[16] Common Methodology for Information Technology Security Evaluation; Evaluation methodology; July 2005; Version 3.0 Revision 2 (CCMB-2005-07-004).

[17] Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive - OJ L 108, 24.04.2002).

[18] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorization of electronic communications networks and services (Authorisation Directive - OJ L 108, 24.04.2002).

[19] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive - OJ L 108, 24.04.2002).

[20] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - OJ L 108, 24.04.2002).

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications - OJ L 201, 31.07.2002).

[22] ETSI TS 100 392-3-6: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 6: Speech format implementation for circuit mode transmission".

[23] ETSI TS 100 392-3-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 7: Speech Format Implementation for Packet Mode Transmission".

[24] ITU-T Recommendation v.24: "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)".

[25] ITU-T Recommendation v.28: "Electrical characteristics for unbalanced double-current interchange circuits".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETR 086-3 [1] apply.

3.2 Abbreviations

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

3GPP	3rd Generation Partnership Project
AI	Air Interface
AT	Access Terminal
CCK	Common Cipher Key
DCK	Derived Cipher Key
ESI	Encrypted Short Identity
GTSI	Group TETRA Subscriber Identity
IP	Internet Protocol
ISI	Inter System Interface
IT	Information Technology
ITSI	Individual TETRA Subscriber Identity
KSS	Key Stream Segment

MS	Mobile Station
MoU SFPG	Memorandum of Understanding Security and Fraud Prevention Group
MT	Mobile Terminal
MT2	Mobile Termination type 2
OTAR	Over The Air Rekeying
PC	Personal Computer
PEI	Peripheral Equipment Interface
PDU	Protocol Data Unit
PSTN	Public Switched Telecommunications Network
QAM	Quadrature Amplitude Modulation
SAGE	Security Algorithm Group of Experts
SIM	Subscriber Identity Module
SwMI	Switching and Management Infrastructure
TAA1	TETRA Authentication and key management Algorithm suite 1
TDMA	Time Division Media Access
TE	Terminal Equipment
TE2	Terminal Equipment type 2
TEAx	TETRA Encryption Algorithm number x
TETRA	TErrestrial Trunked RAdio
TNP1	TETRA Network Protocol No. 1
TOE	Target Of Evaluation
TVRA	Threat Vulnerability Risk Assessment
TVP	Time Variant Parameter
UML	Unified Modelling Language
USB	Universal Serial Bus
WG6	EPT Security working group

4 Communications security model

4.1 Introduction

In the context of the present document, security means to be assured that the risk of a weakness being exploited either intentionally or unintentionally is low.

Many standards include aspects of security, such as:

- confidentiality;
- integrity;
- availability.

The goals of security and of evaluation are:

- to provide product owners with confidence that countermeasures bring the risk to assets to an acceptable level;
- to implement assurance techniques which give confidence that countermeasures bring the risk to assets to an acceptable level;
- to ensure that evaluation provides evidence of assurance giving confidence that countermeasures bring the risk to assets to an acceptable level.

The standardization process plays a significant role in achieving these objectives. Firstly, in order to ensure that the requirements identified in a standard are expressed accurately, clearly and unambiguously, a standard is critically reviewed by its potential implementors. Such review, along with other validation techniques, helps to provide the assurance that any specified countermeasures will, in fact, minimize risk. Secondly, a protocol standard is accompanied by a conformance test specification which can be used in the evaluation process to provide evidence that any countermeasures required by the protocol standard have been implemented correctly in a product.

4.2 General model identifying security relationships

Figure 1 shows a generic system model and the relationship of its components to each other. In order to assess a system it is necessary to identify the system components as these form the assets of the system under threat that may require protection by means of countermeasures.

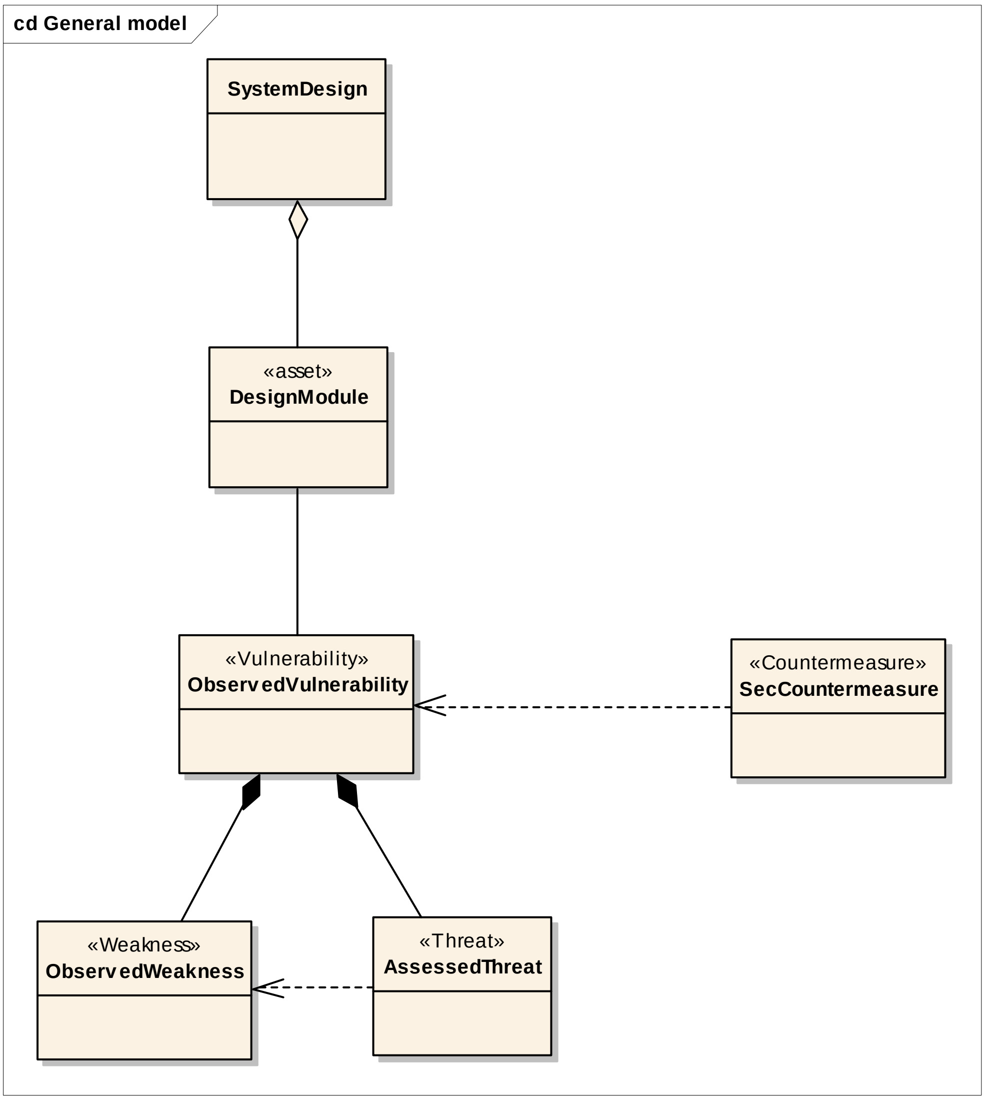

Figure 1: UML model of generic system security design

4.3 TVRA development model

In order to allow visibility there should be a clearly visible path identifying "Objective" to "Requirement" and of "Vulnerability" to "Threat" to "Risk".

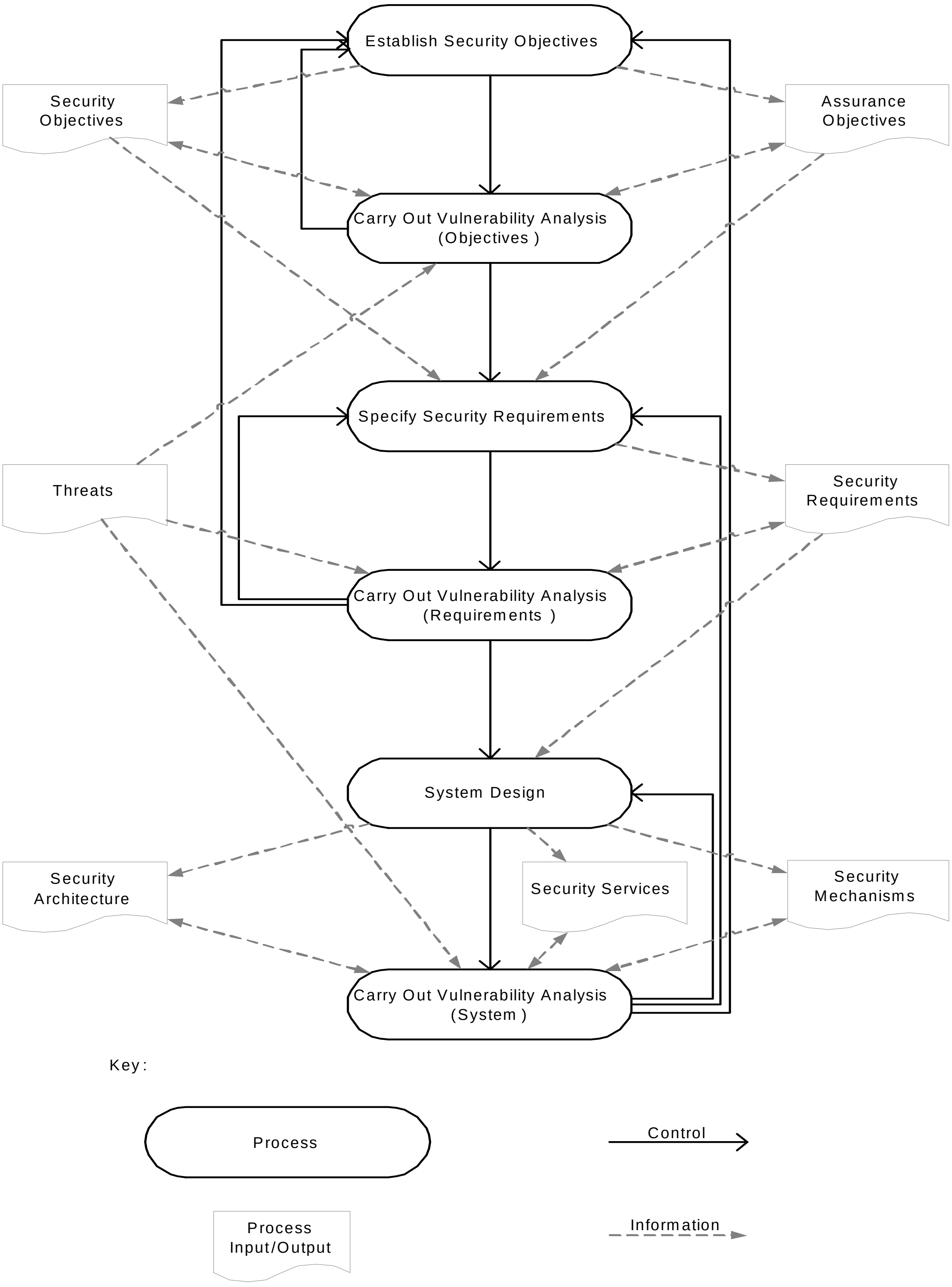
Establish Security Objectives
Security Objectives
Assurance Objectives
Carry Out Vulnerability Analysis (Objectives)
Specify Security Requirements
Threats
Security Requirements
Carry Out Vulnerability Analysis (Requirements)
System Design
Security Architecture
Security Services
Security Mechanisms
Carry Out Vulnerability Analysis (System)
Key:
Process
Control
Process Input/Output
Information

Figure 2: Structure of security analysis and development in standards documents

For the purposes of analysis, all assets should be considered to have weaknesses.

5 Security objectives

5.1 General objectives

The objectives to be met for systems in general, and for systems where the initial link is by radio in particular, where such systems are provisioned for commercial purposes, are summarized in the following bullets:

- to be able to prove the of identity of users and networks;
- to ensure confidentiality of communication;
- to ensure integrity of communication;
- to ensure the rights of privacy of the system's users;

NOTE: This is an objective that is maintained in law.

- to ensure the correct charging of the system's users;
- security management:
    - The complex security functions within the network call for sophisticated control and management. The management functions are security critical themselves and, therefore, subject to security requirements.

5.2 Objectives from the legislative framework

Operators of TETRA networks, and manufacturers of TETRA equipment, have an objective to ensure compliance with the legislative framework of the region in which they operate.

Telecommunications networks and systems are expected to operate within a particular legislative framework. Within Europe the Framework Directive [19] (comprising the Privacy Directive [21], the Authorisation Directive [18], the Access Directive [17] and the Universal Service Directive [20]) identifies a number of areas for which compliance is required and which are highlighted in the clauses that follow.

5.2.1 Privacy

Privacy legislation is of increasing importance; there are strong restrictions in many countries with regard to storage and visibility of data. Therefore, when offering a TETRA service, or when designing data processing functions and defining the kind of data being generated or stored within TETRA systems, TETRA service providers should consider the relevant national data protection laws.

The definition of privacy for TETRA includes:

- privacy of information: keeping information exchanged between TETRA service functions away from third parties;
- limitations on collection, storage and processing of personal data: personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of TETRA services;
- disclosure: the obligation of a network and service providers to keep information concerning customers away from third parties;
- inspection and correction: the right of the customer to inspect and correct information about himself stored by the service and/or network provider.

Privacy legislation mostly concerns the security objectives regarding "confidentiality" and "integrity". For TETRA special concern in this respect should be paid to the contents of personal data in the TETRA service profile. These data and the access conditions to it for the service provider's personnel, the subscriber and the user himself should be limited, in accordance with the relevant European guidelines and national laws.

This legislation will mostly concern the security objectives regarding "accountability", "confidentiality" and "integrity".

5.2.2 Data protection

Data protection measures are those measures made to cover the security of data over and above those dealing purely with privacy and cover the access to and use of data volunteered for any transaction to a third party. Additional protection measures may be necessary to ensure that measures related to data retention and lawful interception remain lawful.

This legislation will mostly concern the security objectives regarding "accountability", "confidentiality" and "integrity".

5.2.3 Security order

National laws concerning the security order:

- demand proper protection of information and infrastructure to ensure the availability and the integrity of the telecommunication network;
- may restrict the usage of cryptographic methods.

This legislation will mostly concern the security objectives regarding "confidentiality", "integrity" and "availability".

5.2.4 Lawful Interception

Lawful interception means the obligation of the network operator to co-operate and provide information in case of criminal investigations (see TS 101 331 [10]).

This legislation will mostly influence the security objectives regarding "confidentiality".

5.2.5 Contract

It should be possible to use information concerning the contract for communication services between two entities in case of a dispute in a court of law.

This legislation will mostly influence the security objectives regarding "accountability" and "integrity".

5.3 Summary

The objectives listed above can be summarized to the following main security objectives:

- **confidentiality** of TETRA service data, of TETRA management data, and of communications using TETRA;
- **integrity** of TETRA service data, of TETRA management data, and of communications using TETRA;
- **availability** of all TETRA services and of all TETRA management functions; and
- **accountability** for all TETRA service invocations and for all TETRA management activities.

Therefore the TVRA and security measures will only be based on these objectives.

6 Vulnerability analysis

6.1 Introduction

The vulnerability analysis for TETRA is presented in accordance with the guidance given in ETR 332 [11] and ISO/IEC 15408-3 [14] to ensure that the system strength can be independently evaluated.

A deployment of a TETRA system is analysed for possible threats. The base for this analysis is the TETRA system as developed to date for TETRA with those extensions required for the data rate extensions for an update of the TETRA air interface. Where existing security measures are available they have been included into the analysis in order to identify threats to the existing countermeasures.

The analysis is made for both private and public systems. The impacts of connection of the TETRA system to public or private fixed networks are included in the analysis.

A potential threat is doing no harm unless there is a corresponding weakness in the system and until the point in time when a weakness is exploited by the intruder. Thus, the threats must be evaluated, i.e. it should be attempted to characterize them according to cost/effort involved (occurrence likelihood) and according to potential benefit/damage that can be done (impact value).

For the risk assessment, the occurrence likelihood of threats is estimated with values from "1" to "3". The meaning of a certain value associated to the occurrence likelihood of a particular threat is explained as follows:

Table 1a: Occurrence likelihood

1	for "unlikely"	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.
2	for "possible"	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	for "likely"	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

The likelihood of any attack can be qualitatively calculated using a formula as below:

Table 1b: Attack potential

Factor	Range	Value
Elapsed time (1 point per week)	<= 1 day	0
	<= 1 week	1
	<= 1 month	4
	<= 3 months	13
	<= 6 months	26
	> 6 months	Note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge of TOE	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Window of opportunity	Unnecessary / unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	Note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7
NOTE 1: Attack potential is beyond high NOTE 2: Attack path is not exploitable		

Each of these attack factors are summed (i.e. Elapsed time + Expertise + Knowledge of TOE + Window of opportunity + Equipment) to give an overall vulnerability rating as shown in table 2. The vulnerability rating is then mapped to the Occurrence likelihood as shown in table 3.

Table 2: Vulnerability rating

Range of values	Resistant to attacker with attack potential of:
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
>26	Beyond high

Table 3: Mapping of vulnerability rating to likelihood

Vulnerability rating	Likelihood
Beyond high	Unlikely
High	
Moderate	Possible
Basic	Likely
No rating	

The impact of a threat is also estimated with values from "1" to "3". The meaning of a certain value associated to the impact is explained as follows:

Table 4: Impact

1	for "low impact"	The concerned party (asset) is not harmed very strongly; the possible damage is low.
2	for "medium impact"	The threat addresses the interests of providers/subscribers and cannot be neglected.
3	for "high impact"	A basis of business is threatened and severe damage might occur in this context.

The product of occurrence likelihood and impact value gives the risk which serves as a measurement for the risk that the concerned management function is compromised. The result is classified into the following three categories:

Table 5: Risk

1, 2, 3	for "minor risk"	Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats causing minor risks have no primary need for counter measures.
4	for "major risk"	Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimized as soon as possible.
6, 9	for "critical risk"	Critical risks arise, when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks should be minimized with highest priority.

NOTE: The values 5, 7 and 8 cannot occur.

6.2 TETRA system under evaluation

The TETRA system considered for evaluation has a very small set of open interfaces as shown in figure 3.

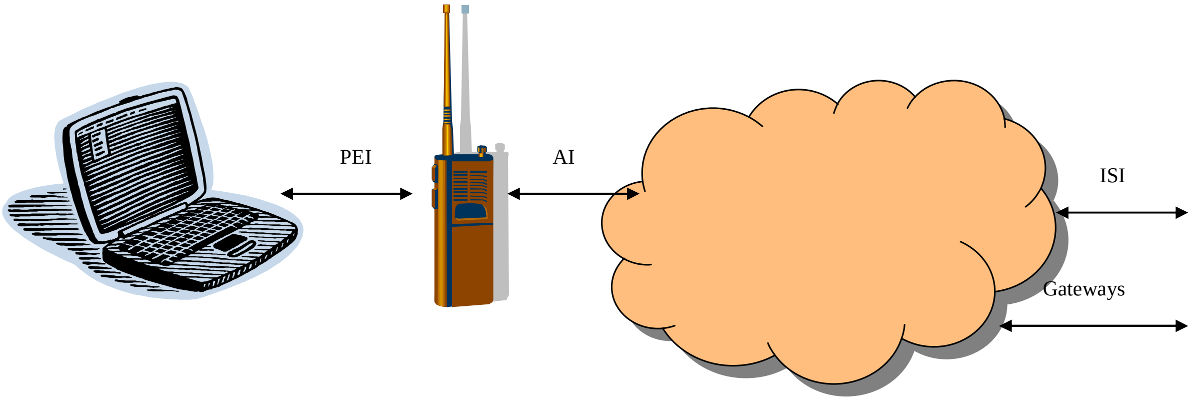

Figure 3: TETRA open interfaces considered for TVRA

6.3 TETRA use cases (security scenarios)

6.3.1 Point to point communication within single TETRA SwMI

A call made using ITSI as the source and destination address.

6.3.2 Point to multipoint communication within single TETRA SwMI

A call made using ITSI as source address and GTSI as destination address.

6.3.3 Broadcast communication within single TETRA SwMI

A call made with reserved broadcast address as destination address.

6.3.4 Point to point communication within multiple TETRA SwMIs

A call made using ITSI as the source and destination address utilising ISI as communications (media and signaling) link between SwMIs.

6.3.5 Point to multipoint communication within multiple TETRA SwMIs

A call made using ITSI as the source and GTSI as destination address utilising ISI as communications (media and signaling) link between SwMIs.

6.3.6 Broadcast communication within multiple TETRA SwMIs

A call made with reserved broadcast address as destination address utilising ISI as communications (media and signaling) link between SwMIs.

6.4 Overview of existing TETRA security measures

6.4.1 Security analysis and recommendation

The analysis presented as design input for TETRA in ETR 086-3 [1] and the ongoing development of EN 300 392-7 [3] has offered a set of security solutions to counter those threats identified in the referred documents.
The current countermeasures defined in EN 300 392-7 [3] and the ongoing work of the TETRA MoU SFPG group address the risks present at the Air Interface and the risks involved in deploying the mechanisms defined to ensure that best practice is maintained.

6.4.2 Air interface capabilities

6.4.2.1 Security profiles or classes

TETRA security is defined in terms of class (see EN 300 392-7 [3]). Each class has associated features that are mandatory or optional and are summarized in table 6.

Table 6: Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable
1	O	-	-	O
2	O	O	M	O
3	M (note 1)	M (note 2)	M	O†

KEY: M = Mandatory;
O = Optional;
- = Does not apply;
† = Recommended.				

NOTE 1: Authentication is required for generation of DCK. NOTE 2: OTAR for CCK is mandatory, other key management OTAR mechanisms are optional.				

6.4.2.2 Authentication

All authentication services in TETRA release 1 are enabled by the secret key relationship of the root key K to ITSI and support the following services:

- authentication of MS by SwMI;
- authentication of SwMI by MS;
- mutual authentication (where the decision to make the authentication mutual is made by the challenged party).

The authentication protocol is of the challenge-response format described in ISO/IEC 9798-2 [2] with the random variable being provided by random numbers.

6.4.2.3 Over the air key management support

Keys may be provided for one or more of the encryption services over the air in TETRA. In each case both individual and group distribution is defined. The former uses a key sealing service using K as the root key. The latter uses a group sealing key which may itself be distributed by the former method.

In addition for class 3 systems the core key CCK is provided over the air. The Derived Cipher Key (DCK) is derived during the authentication process. The Common Cipher Key (CCK) is sealed with the DCK resulting from authentication and transmitted in sealed form over the air.

6.4.2.4 Encryption

The encryption service in TETRA offers confidentiality of traffic, both voice and data, and some protection of the signaling.

The Encrypted Short Identity (ESI) mechanism provides a means of protection of identities transmitted over the air interface. The mechanism applies only to those networks with air interface encryption applied (class 2 and class 3 systems). When encrypted signaling is used the ESI is sent instead of the true identity

6.4.2.5 Over the Air enable and disable

The enable disable capability in TETRA (sometimes referred to as "stun' n' kill") allows a malfunctioning or stolen terminal to be either temporarily or permanently prevented from operation. In the former case the terminal can be re-enabled over the air, whereas in the latter case to reinstate operation requires a visit to a service centre.

6.4.3 Crypto capabilities

6.4.3.1 TAA1

TAA1 is the authentication and key management algorithm set defined by SAGE in accordance with the algorithm specifications given in EN 300 392-7 [3] and the rules of management given in TR 101 052 [8].

6.4.3.2 TEAx

6.4.3.2.1 Overview

All TETRA encryption algorithms for use with π/4-DQPSK modulation generate a key stream of up to 432 bits using an input Cipher-Key and Time Variant Parameter derived from the timing sequence of the TDMA broadcast.

An independent analysis of the TEAx algorithms in order to determine the impact of requesting a longer key stream segment from the TEAx algorithms identified no security or cryptanalysis concerns in the definition of any of the TEAx algorithms. The analysis is available on request from the ETSI TETRA WG6 chair.

The conclusion of the study is that there is no change in the level of risk to loss of confidentiality for encrypted air interface traffic when moving from the existing TETRA to the modified air interface being standardized in TETRA.

6.4.3.2.2 TEA1

For use in the region specified in the rules of procedure for TEA1 [4].

6.4.3.2.3 TEA2

For use in the region specified in the rules of procedure for TEA2 [5].

6.4.3.2.4 TEA3

For use in regions specified in the rules of procedure for TEA3 [6].

6.4.3.2.5 TEA4

For use in regions specified in the rules of procedure for TEA4 [7].

6.5 System capabilities not covered by existing TETRA security measures

6.5.1 PEI

6.5.1.1 Overview

The Peripheral Equipment Interface is defined in EN 300 392-5 [9] and allows for a split of the TETRA terminal to two separate devices connected using the PEI at reference point RT: Terminal Equipment type 2 (TE2); and a Mobile Termination type 2 (MT2).

The equipment that may act as TE2 includes PCs and PDAs as well as specialist data equipment (including sensors). The existing scope of PEI restricts MT2 to be a TETRA Trunked Mode equipment, and further restricts PEI to a single point to point connection.

With respect to data services, the TETRA PEI will be used for the following:

- transmission and reception of packet data (including setting of packet data parameters);
- transmission and reception of circuit data (including setting of circuit data parameters);
- transmission and reception of short data (including setting of short data parameters).

In addition to data services the TETRA PEI may be used for the following:

- set-up and control of speech calls (including setting of speech call parameters);
- access to general information of MT2 and network;
- access to user applications located in MT2.

The TETRA PEI includes components which are not required by all the functions listed above and therefore, depending on the functionality that a MT2 supports, not all aspects of the PEI need to be implemented.

TETRA PEI has been designed to fulfil the following key requirements:

- a standard physical interface, widely adopted in the Information Technology (IT) world;
- minimal extra software in the TE2;
- broad compatibility with other wireless data systems;
- access to the full range of MT2 functionality (TE applications may use profiles to restrict functionality).

The impact of adoption of standard physical interfaces may allow a number of standard PC connectivity arrangements to be adopted and the security models of these should be considered. The range of physical interfaces include:

- Wireless:
    - Optical (InfraRed).
    - Radio (Bluetooth).
- Wired:
    - USB.
    - RS-232 using V.28.

The purpose of PEI is to enable control therefore only the call set up, maintenance and clear down signaling for speech calls are sent on the PEI, and therefore voice packets are never sent over the PEI (voice packets go directly from the MT codec to the TMD-SAP). However it is noted that circuit mode data may be sent over the PEI.

6.5.1.2 Objectives

The objectives of PEI are to enable remote control of MT2 and thus to allow expanded functionality within TE2.

The security objectives to be met by PEI are to ensure that the remote TE2 offers the same risk to the TETRA user and TETRA SwMI as if the TE and MT were collocated.

6.5.1.3 Threats and threat agents

The scope of services enabled remotely over PEI are shown in figure 4.

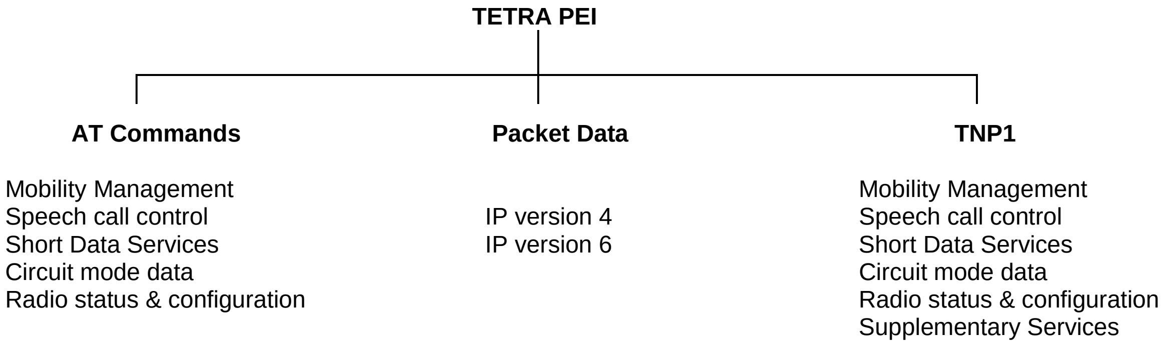

Figure 4: PEI components

Any unprotected PEI may allow access to any of the three service categories.

The following key differences are noted:

- TNP1 commands can be sent in parallel with ongoing packet data services.
- AT commands can only be sent in the command state.

The primary assumption in PEI is that the connection is between two trusted equipments (TE and MT) and there is no authentication or authorization. It is further assumed that the connection is wired using a short non-radiating cable (within the constraints set for V.24 [24] and V.28 [25] in ITU-T).

Where the physical connection does not comply with clause 5 of EN 300 392-5 [9] and instead adopts wireless modes, the MT, and all capabilities open to TNP1 and the AT command set, are open to attack. To counter this Bluetooth should not be set to discoverable mode.

6.5.1.4 Summary of unwanted incidents

The following unwanted incidents may arise when PEI is exploited:

- harvesting of data on the SIM (this is currently restricted to the PSTN phonebook and some local configuration data); and
- remote invocation of packet data connections.

6.5.2 ISI

The ISI provides the technical links between two TETRA networks that have agreed to allow intercommunication. The form of physical link used for the ISI is not specified. There are two specifications for the transmission of TETRA speech that may apply (references TS 100 392-3-6 [22] and TS 100 392-3-7 [23]) on the ISI which will allow support of encrypted speech across the ISI.

Details of the ISI are currently insufficient to permit a full TVRA to be carried out but a general assumption that the end-points are trusted but that the linking network is itself untrusted may be applied. In this way the general assumptions and TVRA models for use of untrusted networks apply.

6.5.3 IP

The use of Internet Protocol in TETRA is possible but not explicitly protected other than by the existing radio interface mechanisms and by the explicit TETRA identity authentication. The bulk of air interface protocols for establishment of an IP connection in TETRA share a common root with those of GPRS and 3GPP in the use of the PDP-context activation and deactivation and the use of IPsec in the TETRA environment is able to share the profiles being developed in both 3GPP for 3rd generation cellular and wireless access, and in TISPAN for IP access.

NOTE: Work in progress in ETSI and with the IPv6 forum towards a suite of interoperability and conformance tests for IPv6 covering the capabilities of IPsec in addition to the core and mobility capabilities of IPv6 may be used as the basis of a formal TETRA IPsec profile.

6.5.4 Application level security

All applications in TETRA are assumed to exist within the trusted TETRA SwMI space and therefore considered out of scope for this TVRA (within the trusted zone).

There are a number of solutions for security within applications but the selection of countermeasures and identification of risk cannot be generalized. The use of tools such as Digital Rights Management and Kerberos like models of distributed secure access control may be usefully reviewed in the application context.

7 Identification of requirements for countermeasures

7.1 Overview

Countermeasures should be applied to those vulnerability/asset relationships where the risk is significant (i.e. where the risk identified in clause 6 is critical or major). Countermeasures can take a number of forms:

- Redesign to eliminate the weakness (as with no weakness there is no threat-weakness pair hence no vulnerability).
- New assets offering specific protection for specific vulnerabilities.

NOTE 1: Any new asset introduced to the system has to be assessed for vulnerabilities and any concurrent risk identified.

NOTE 2: A single asset performing as a countermeasure may reduce the risk associated with many vulnerabilities and assets.

7.2 TETRA air interface modifications

The major areas in TETRA where additional risk is to be encountered that lie within the scope of TETRA to provide countermeasures for are in the areas of the ISI and PEI. In both cases ongoing work in both TETRA and the TETRA MoU SFPG are addressing these areas. For those areas outside of TETRA's immediate control such as application level security and IP security the TETRA MoU SFPG is addressing the principal areas of risk and appropriate countermeasures to be applied. This work allied with ongoing best practice in the market and in particular the trends in 3GPP and TISPAN for use of IPsec should be followed and applied where appropriate.

One of the biggest changes arising from the update of the TETRA air interface is the greater data carrying capacity and as such there are requirements to modify the KSS length output from the KSG (see clause 6.4.3.2.1) to support confidentiality of both π /8-D8PSK and QAM modulation. One further consequence of the greater data carrying capacity is that there will be greater likelihood of PDU association in π /8-D8PSK and QAM channels. Changes have been developed in WG6 to provide for additional precautions in the case of QAM modulation to avoid KSS repeat where PDU association occurs.

7.2.1 Outline of modifications to TETRA air interface security

The TETRA air interface security specification has been progressively updated during the period of development of the present document. The main changes are summarised in the table below and refers to specific Change Requests to be incorporated.

Table 7: Outline CRs updating TETRA Air interface security in response to ongoing TVRA work

CR	Title	Rationale
102	Redundant Key Change Type Values	With the addition of the "Class 3 CCK and GCK Activation" Key Change Type in D-CK CHANGE DEMAND, the following Key Change Types are no longer required and should be removed from the standard: • GCK Activation • GCK Deactivation The purpose of this CR is to replace these redundant values with “reserved”.
103	Definition of security related information and group identity security related information element	The DGNA standard refers to an element named "Security Related Information". The latter element allows the possibility of associating a group with one or more keys. In addition, there is a need to add a similar information element "Group Identity Security Related Information" to group attachment/detachment signalling, to permit the SwMI to indicate key associations for a given group. The purpose of this CR is to define these information elements and their use.
105	Incorporating CMG GTSI within D-OTAR GSKO Provide	In order to simplify the provisioning of security related information over the air interface (for the use of group OTAR operations), it would be advantageous to include the CMG GTSI as part of D-OTAR GSKO PROVIDE, even if the inclusion would result in the PDU being fragmented on the downlink. Downlink fragmentation of D-OTAR GSKO PROVIDE is not perceived as an issue when considering the long lifetime of such a key and, therefore, its infrequent rekeying. The inclusion of the CMG GTSI would remove the need for an operator to manage the provisioning of CMG GTSI separately from the GSKO; leading to a simplification of user/operator procedures for a system using group OTAR. The behaviour required from the MS in the event of a CMG GTSI change also needs to be covered, specifically the deletion of SCK, GCK and GSKO.
106	Authentication during enable disable	When specifying IOP behaviour, the security standard appears to be ambiguous in relation to the need for authentication as part of the enable/disable protocol. Furthermore, the coupling between security classes and enable/disable appears unnecessary and adds confusion. There are a number of statements in the security standard that give the impression that authentication is mandatory during enable/disable on SC3 cells, however there are other statements and PDU specifications that support an enable/disable mechanism without authentication. Suggested re-wording of the Enable/Disable clause is enclosed, which would address any current concerns within the IOP group regarding this behaviour. Note that a significant part of section 5.4.6 was removed because EN 300 392-7 CR011 superseded EN 300 392-7 CR004, but the standard includes the text from both and, as a result, contradicts itself in a number of places. Changes to the section on DCK construction have been incorporated into this CR, for instances where mutual authentication is requested by one party but not supported by the other.

107	Modifications to OTAR mechanisms	The purpose of this CR is to clean-up the sections on OTAR pertaining to SCK and GCK. In particular, it explains that the SwMI may respond to an MS's request for keys using group addressed group sealed keys. TD016 and TD029 have also been incorporated into this CR – reasoning as follows: The security standard permits the MS requesting multiple SCK in U-OTAR SCK DEMAND, however the standard does not permit a request for multiple GCK in U-OTAR GCK DEMAND. The purpose of this CR is to address the latter imbalance and permit the MS to obtain multiple GCK in a single U-OTAR GCK DEMAND PDU. As a consequence, D-OTAR GCK PROVIDE, U-OTAR GCK RESULT and D-OTAR GCK REJECT need to be revised to refer to multiple GCKs. At the request of WG6, the number of GCKs and SCKs requested/provided/rejected within a single PDU has been increased from 4 to 7, for both SCK and GCK. In addition to the changes above, it has been observed that definition of the "Number of SCKs rejected" information element is missing from the existing security standard, and must be added. The definition of U-OTAR SCK REJECT requires further structuring to avoid encoding ambiguities. A different CR on a proposed OTAR retry mechanism has been incorporated into this CR due to its associated impact on the construction of SCK and GCK OTAR PDUs. It describes a mechanism to control and vary the interval between retries of MS key requests. Said mechanism is designed to be bandwidth efficient and dynamically controllable by the SwMI, e.g. under varying control channel load conditions.
109	Re-specification of SCK information element	The definition of the *SCK Information* element does not support a future SCK having a different SCKN and/or SCK-VN (that is not the current SCK-VN plus 1). This information element needs to be re-defined to allow the future SCK to have independent SCKN/SCK-VN.
110	Modified use of cipher parameters	Following recent discussion in WG3 and WG6, related to the use of the *Class of MS* element to indicate support for "GCK encryption", it is now apparent that there are no longer bits available in this element for the purposes of indicating new MS security capabilities. Therefore, this change request proposes an alternative means of indicating said capabilities. Specifically, this proposal assigns 3 bits from the Cipher Parameters element (available when the MS is registering for SC3 operation) to indicate support for TM-SCK OTAR, SDMO and DM-SCK OTAR, and GCK encryption/OTAR. The SwMI may use the information provided to ensure that any relevant MS support the new service(s) prior to use.
111	Actions following authentication failure	EN 300 392-7 does not describe what the MS should do if a BS fails to authenticate itself. Also, table A.91 is redundant as it is already given in EN 300 392-2.
112	Use of LIP during temporary disable	This change allows an MS that is in the temporary disabled condition to transmit location information protocol (LIP) signalling.
113	Encryption of π/8 D8PSK and QAM logical channels	Extension of the encryption mechanism to π/8 D8PSK and QAM logical channels, to keep EN 300 392-7 in step with the TEDS version of EN 300 392-2.
115	Handling of PDUs not-conforming to link ciphering mode	EN 300 392-7 is not clear on what an MS or SwMI should do if it receives a PDU that does not conform to the negotiated cipher state. This CR clarifies the options allowed.
117	Definition of "ignore" in 6.7.1.4 to be refined	EN 300 392-7 is not clear on what an MS or SwMI should do if it receives a PDU that does not conform to the negotiated cipher state. This CR clarifies the options allowed.
118	Inclusion of OTAR RETRY Interval element in D-OTAR-xxx-Reject PDUs	No retry interval provided when an OTAR request is rejected.
119	Correction of OTAR PDUs use of network codes	Inconsistency in use of network codes in OTAR PDUs.

History

Document history		
V1.1.1	August 2006	Publication