ETSI

# ETSI TECHNICAL REPORT

**ETR 300-4**

**July 1997**

Source: EP-TETRA

Reference: DTR/TETRA-01011-4

ICS: 33.020

**Key words:** TETRA, network management

# Terrestrial Trunked Radio (TETRA); Voice plus Data (V + D); Designers' guide; Part 4: Network management

**ETSI**

European Telecommunications Standards Institute

**ETSI Secretariat**

**Postal address:** F-06921 Sophia Antipolis CEDEX - FRANCE
**Office address:** 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
**X.400:** c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

# Contents

Blank page

## Foreword

This ETSI Technical Report (ETR) has been produced by ETSI Project TErrestrial Trunked RAdio (TETRA) of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status.

An ETR may be used to publish material which is either of an informative nature, relating to the use or application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

Blank page

# 1 Scope

This ETSI Technical Report (ETR) is intended to serve as an informative reference document for network operators or managers of mobile radio systems who are contemplating TErrestrial Trunked RAdio (TETRA) solutions. It aims to explain the general requirements for network management, the implications of different network architectures on the services needed at particular locations and how these can be realised.

Within TETRA a standardized management interface (I5) will facilitate central management of inter-working between different systems (e.g. systems from different manufacturers). Management at a central level will generally require a different set of services to those provided locally in individual systems. Typical 'local' and 'central' services are summarized in this ETR (see subclause 5.2) and many of these are defined in greater detail in ETR 292 [1].

The use of the standardized interface is just one option for integrating different management systems. Other bespoke solutions may be required if additional central services are needed or if interface I5 is not available in early releases of TETRA systems. This ETR examines alternative options (see clause 6) to give practical guidance to those considering such integration and includes a useful check list for drawing up user specifications for network management facilities (see clause 7).

# 2 References

For the purposes of this ETR the following references apply:

[1] ETR 292: "Terrestrial Trunked Radio (TETRA); User requirements for network management".

[2] ITU-T Recommendation M.3400: "TNM Management Functions".

The reader is referred to annex A for a list of further useful information.

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of this ETR, the following definitions apply:

**Base Station (BS):** A physical grouping of equipment which provides the fixed portion of the air interface. One BS transmits and receives radio signals to and from a single location area (a single region of geographical coverage).

**gateway:** A device which will enable the interconnecting of two networks which inherently use different and incompatible protocols.

**network:** A collection of subscriber terminals interconnected through telecommunications devices.

**real time:** Refers to the generation of network management information in a timeframe comparative to the real life process that it is controlling or monitoring.

**signalling:** The exchange of information specifically concerned with the establishment and control of connections, and with management, in a telecommunication network.

**site:** Physical location within the network.

**subscriber activity log:** A system record which contains information on attach/detach Individual TETRA Subscriber Identity (ITSI); enable/disable terminal; registrations; location updates vs. time; call re-establishment; authentication; call start time, call end time, and called party; type of call; supplementary services invoked; whether uplink Bit Error Ratio (BER) or Message Error Rate (MER) are below an operator pre-determined threshold; plus any other relevant activity record.

**subscriber data:** A system record which contains information on the individual subscriber ITSI, Group TETRA Subscriber Identities (GTSIs), supplementary services allowed, privileges allowed and other system accesses allowed.

**subscriber management:** The functionality within the management system, for dealing with subscribers to the system.

**subscriber terminal:** An equipment which an internal user can use to communicate with another user. Mobile Stations (MS) and Line Stations (LS) are the only types of subscriber terminal.

**supplementary service:** A supplementary service modifies or supplements a bearer service or a teleservice. A supplementary service cannot be offered to a customer as a stand alone service. It should be offered in combination with a bearer service or a teleservice.

**Switching and Management Infrastructure (SwMI):** All of the TETRA equipment for a Voice plus Data (V+D) network except for subscriber terminals. The SwMI enables subscriber terminals to communicate with each other via the SwMI.

**transaction (packet transaction):** All the processes and procedures associated with the transmission of one packet of information between peer network layer protocol entities on opposite sides of the air interface.

**transaction (voice transaction):** Part of a voice call comprising the transmissions of each talking party. The total of all transactions make up the call.

### 3.2 Abbreviations

For the purposes of this ETR the following general abbreviations apply:

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation one |
| BER | Bit Error Rate |
| BS | Base Station |
| CMIP | Common Management Information Protocol |
| CNM | Central Network Management |
| GTSI | Group TETRA Subscriber Identity |
| ISTI | Individual TETRA Subscriber Identity |
| LNM | Local Network Management |
| LS | Line Station |
| MER | Message Error Rate |
| MFA | Management Functional Area |
| MIB | Management Information Base |
| MS | Mobile Station |
| NMF | Network Management Facility |
| NMS | Network Management System |
| RFC | Request For Comment |
| OSI | Open Systems Interconnect |
| SMI | Structure of Management Information |
| SNMP | Simple Network Management Protocol |
| SwMI | Switching and Management Infrastructure |
| TMN | Telecommunications Management Network |
| V+D | Voice plus Data |

## 4 General principles of network management

### 4.1 Introduction

Network management provides a distributed application enabling monitoring and control of network resources, in order to control the overall environment in an orderly fashion. It has to interface across all of the physical elements in a network, and to this end it is increasingly important that open standards are adopted as the norm in all network elements, enabling the control of the network to be undertaken by an integrated network management system.

It is important to be able to receive information and apply controls to all elements in a network in an efficient manner. The elements and services that are contained within a managed network need to be modelled in an abstract manner, so as to allow the operator to exercise actions and controls without needing in-depth knowledge of each of the pieces of equipment being managed.

### 4.2 What it does

Network management covers all activities concerned with monitoring and controlling a network e.g. planning, building/expanding, operating and making the most efficient use of the available resources. The typical features of a network management system are:

- planning;
- service provision;
- network monitoring;
- fault management;
- network traffic management;
- configuration (including subscriber management).

Network management applications are based around management frameworks, examples of these are Open Systems Interconnect (OSI), Telecommunications Management Network (TMN) and Simple Network Management Protocol (SNMP). These frameworks provide an inter-operable interface to achieve interconnection between various types of equipment, communicating via a defined management protocol. The two most common open protocols are Common Management Information Protocol (CMIP) and SNMP.

A management framework enables the use of generic information models and standard protocols and identifies uniquely the inter-operable interface for co-operating management applications. Typical components of a framework are:

- managed objects:
    - the term managed object is used as means to describe management information;
- Structure of Management Information (SMI):
    - defines how to define new managed objects, places restrictions on their types and specifies rules for naming. A collection of managed objects is viewed as the schema for the Management Information Base (MIB);
- data representation:
    - to express the format of the packets exchanged in a machine independent way, a formal system is used, the most common form being Abstract Syntax Notation (ASN.1). This is used in the definition of the MIB.

The interoperable interface = SMI + MIB + management protocol.

### 4.3 General recommendations

Management systems need to be flexible and have a distributed modular architecture that allows service providers to adapt to customer needs. Given the sophistication and growth of services, a flexible management environment has to be established in order to:

- enable rapid service deployment;
- promote faster service activation;
- efficiently manage and distribute data throughout the network.

Network management systems should also aid the reduction of costs and the provisioning of services in a competitive and timely manner, this can be addressed by:

- elimination of redundant processes and equipment;

- improvement in service responsiveness;

- tuning the performance and capacity of the network.

Flexibility of management systems can be achieved by incorporating more of the intelligence into the network elements, this re-distribution of functionality will enable management systems to maintain a high level end-to-end view of the services and resources being managed.

### 4.4 Using network management as a tool

Management tools provide the ability to take raw information from a managed system and convert that information into an understandable form suitable for the person using it.

A network management terminal is capable of representing the network in a form which reflects the users function and their need for information. This is not restricted to a purely physical interpretation of the network, but can be used to show administrative information, such as usage, billing information, subscriber statistics etc. Management terminals may be used by many functions within an organization, e.g. network administrators and accountants.

Users access the same source of information, however it will be presented as different views of the system. An accountant may display regions denoting financial centres. Each region containing tariff, service and subscriber details, including details of calls made, network usage and discounting packages for each subscriber or sub network.

The network administrator will be interested in the low level physical components and their inter-connectivity within the whole system.

### 4.5 Management Functional Areas (MFA)

Management Functional Areas (MFAs) are described in ITU-T Recommendation M.3400 [2]. A MFA will contain many management functions, which are the smallest part of the management framework as described by TMN. Table 1 provides an overview of each of the MFAs.

**Table 1: Overview of MFAs**

| Functional Area | Description |
|---|---|
| Performance | This provides functions to evaluate and report on the behaviour of equipment and the effectiveness of the operation of the network. The functions generally supported are:<br><br>- performance monitoring;<br>- performance control<br>- performance analysis. |
| Fault | This is a set of functions which allow the detection, isolation and correction of abnormal operation and fault conditions within a telecommunications network. Typical functions provided are:<br><br>- alarm management;<br>- fault localization;<br>- testing;<br>- trouble management. |
| Configuration | Provides functions to exercise control, collect and provide information to network elements. Typical uses of this function are:<br><br>- provisioning;<br>- element configuration;<br>- database management;<br>- status and control;<br>- subscriber management. |
| Accounting | Provides functions to allow the use of the network or service to be measured and the costs for the usage to be determined. The main functions in this area are:<br><br>- billing;<br>- tariffing. |
| Security | This function is concerned with the overall security of network management information. The areas it should address are:<br><br>- audit trail;<br>- intrusion;<br>- access rights. |

# 5 Architecture and services

## 5.1 CNM/LNM concept

The concept of Central Network Management (CNM) and Local Network Management (LNM) arises from the need to consider facilitating central management of inter-working between TETRA systems from different manufacturers (see figure 1).

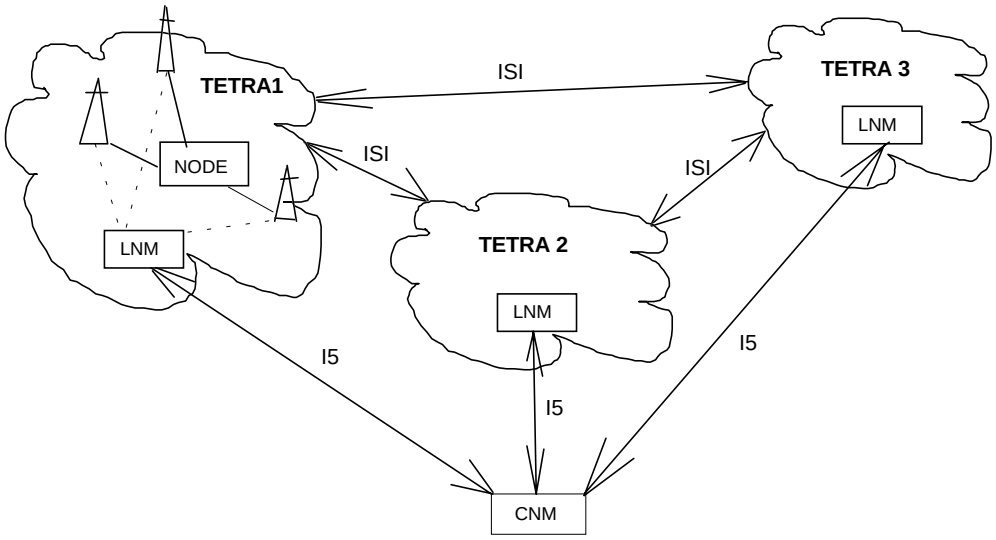


**Figure 1: Example of interconnection of different TETRA networks**

A number of individual TETRA systems may originate from more than one manufacturer. Each TETRA system has its own LNM facility which handles all aspects local to the system itself. There is also a CNM facility which monitors or controls certain functions within and between the individual systems. Each system has a link to the CNM facility.

The CNM system manager manages the CNM on a day-to-day basis. The LNM system manager manages each TETRA system on a day-to-day basis, reconfiguring it dynamically as required, managing subscribers and arranging maintenance when required.

In this ETR the CNM is described as a single facility, however, in the case of a large system, e.g. hosting several end user organizations, it may be possible for each organization to have access to CNM facilities.

## 5.2 Services

### 5.2.1 Typical central services

The central service aspects of TETRA network management are high-level functions which require to be standardized to allow the management of several TETRA networks from a central entity. Typical standardized central network management functions are:

- subscriber management:
  - temporary withdrawal of registration permission;
  - restoration of registration permission (after temporary withdrawal);
  - subscriber activity history;
  - current status of a subscriber;
  - initiate trace of future subscriber activities;
- performance management:
  - performance data transfer in standard format from the LNM to the CNM;

- fault or maintenance management:

    - alarm trigger corresponding to serious equipment failure;
    - alarm trigger corresponding to serious security breach;
    - alarm trigger corresponding to serious traffic alarm;

- accounting management:

    - transfer of accounting data for users with wide roaming capability;

- security aspects:

    - security procedures (authentication and authorization).

### 5.2.2 Typical local services

Certain aspects of TETRA network management will only be performed within a single TETRA network at a local level and therefore do not need to be standardized across networks. The following list gives typical examples of the services available locally:

- subscriber management:

    - subscriber basic data management;
    - basic service data management;
    - supplementary service management;
    - subscriber location;
    - group management;
    - closed user group management;

- configuration management:

    - influenced network elements (maintaining integrity of system hardware and software);
    - system parameters (area and call based, network configuration, system administration);
    - software management (software version tracking);
    - radio network management;
    - routing management (local and inter-system);

- performance management:

    - measurement data generation and collection;
    - measurement data storage;
    - measurement data presentation;

- fault or maintenance management:

    - alarm status monitoring;
    - alarm collection and logging;
    - alarm history handling;
    - diagnostics and test handling;
    - recovery from fault state;
    - equipment state handling;

- accounting management:

    - collecting and storing the accounting data (call logging);
    - billing;

- security aspects:

    - management of security of Network Management System (NMS);
    - security management (e.g. encryption key management).

### 5.3 Architectures

This subclause discusses how a Network Management Facility (NMF) may be mapped onto TETRA systems of various sizes.

#### 5.3.1 Single tier system

A single tier TETRA system, such as may be used for a small compact network, will probably comprise a number of base stations inter-connected by some form of network. Attached to this network is a NMF from which all the necessary management functions can be exercised. This is shown in figure 2.

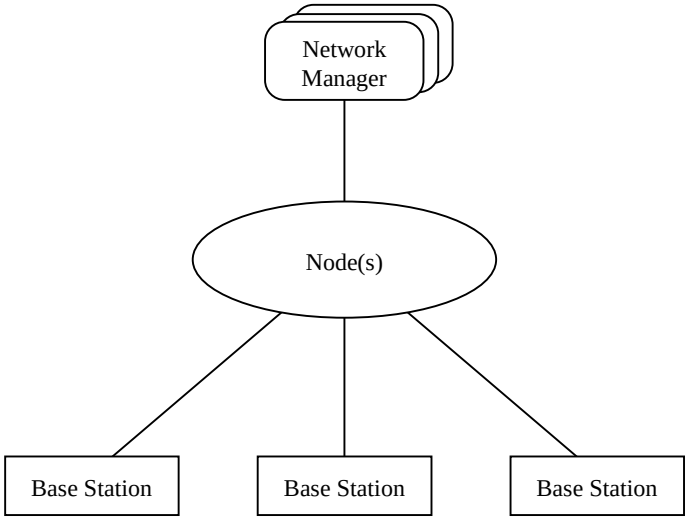


**Figure 2: A single tier system**

The management facility may be a single terminal used by a single operator who can perform all the network management functions. Alternatively, for a slightly larger system, it may be used by more than one network operator each of whom may have different permitted roles, using perhaps more than one terminal. For example the different operators, service providers, users or managers may be concerned with different sets of functions, in whole or in part. Such functions include subscriber and security management, network configuration and fault management, performance management, etc.

#### 5.3.2 Multi-tier system

For a large TETRA system, there may be several regions each of which may have its own network management facility. There may also be an additional NMF to provide co-ordination between the regions. This is shown in figure 3.

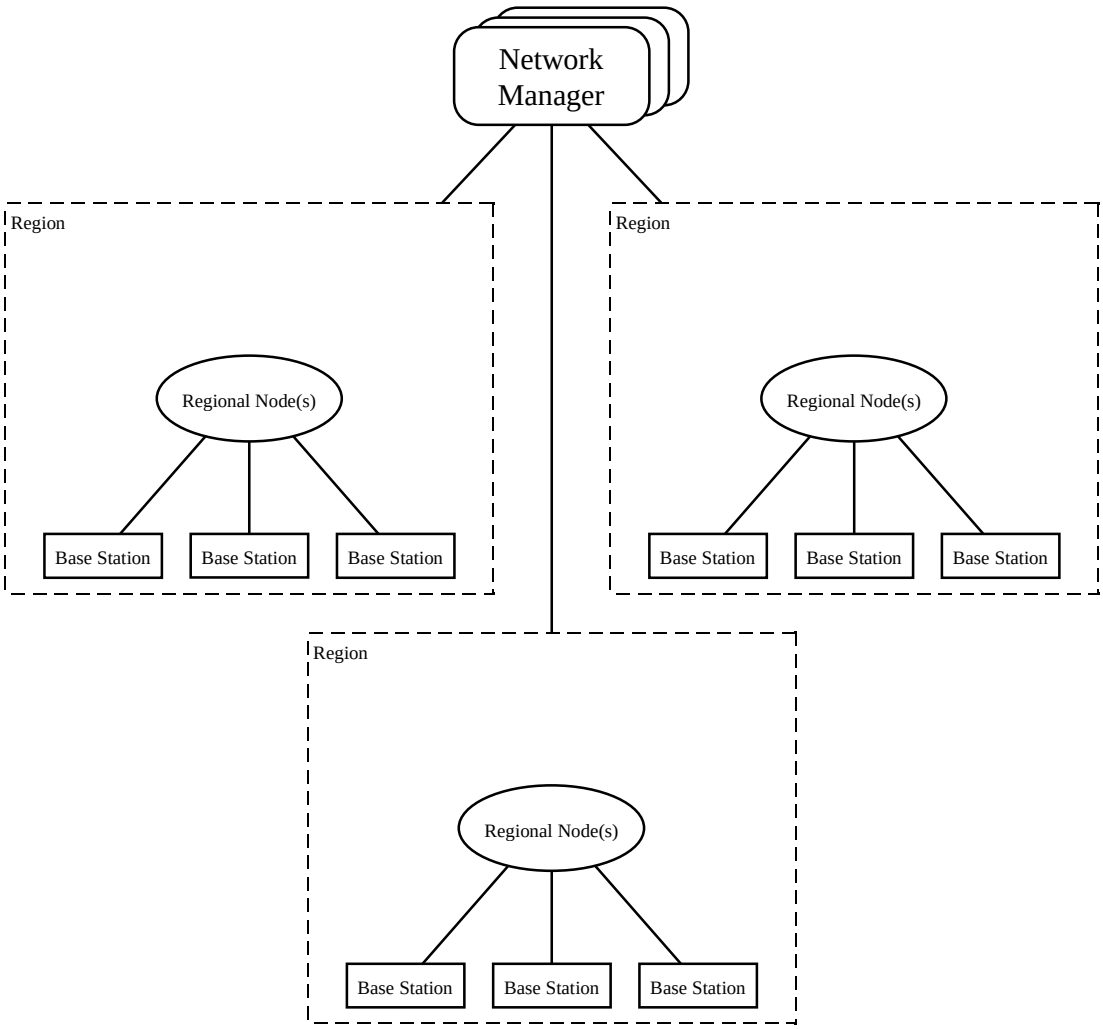


**Figure 3: A multi-tier system**

Each region may have control over its own network configuration and fault management, subject of course to any network management policy that may be in place. The region may also send any faults that are deemed of sufficient severity to the network manager.

The NMFs will probably retain control of subscriber and security management, and of performance management, etc. They may also be responsible for the configuration of any inter-regional aspects of the network and receive fault reports about such aspects. In addition, the network manager may have the capability to take-over from any other management facility that is not in use for any reason.

With multiple management facilities, simultaneous updates of the network by these facilities are a possibility. Therefore it is important that a means of protection against simultaneous updates is implemented.

### 5.3.3 Multiple supplier system

A TETRA system that is supplied by more than one manufacturer can be viewed as a large system comprising several tiers and branches and each branch may have a different number of tiers and regions. An example of such a network is shown in figure 4. Each of two branches could be supplied by different manufacturers and each will be therefore largely independent of the other. Each supplier's system can then be viewed as separate networks each with their own local network management facility. Within each supplier's network the local network manager is equivalent to the network manager function shown in figures 2 and 3.

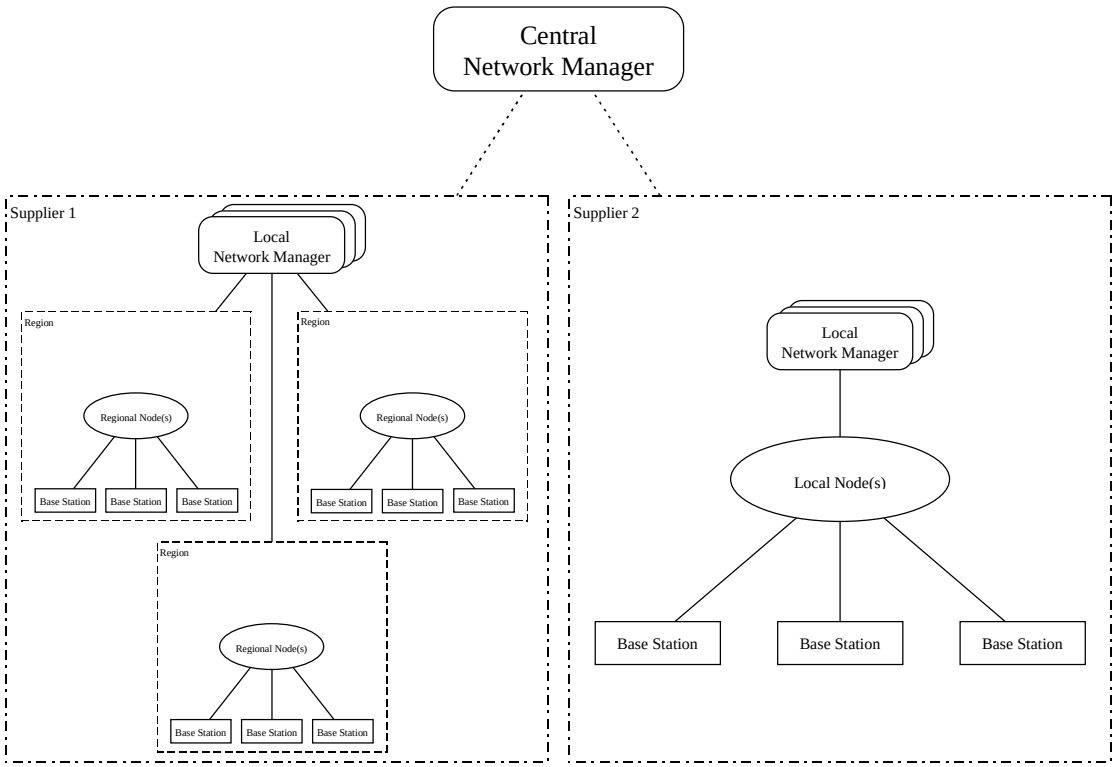


**Figure 4: Multiple supplier system**

The range of facilities available to the CNM will depend on the level of integration between the suppliers' network management systems.

## 6 Options for integration

For a single supplier system, it is assumed that the supplier will provide a network management system capable of supporting centralized management over the whole network.

For a multiple supplier system, a centralized NMF that can exercise control over the whole the network may not be readily available. In this instance, the centralized NMF can be provided via bespoke integration of the different schemes in use, each of which may use different protocols, information flows and management information structure. Various levels of integration can be envisaged:

- full:
  - for a fully integrated central network management system, all or most of the facilities described in ETR 292 [1] will be available from a single management platform. Co-ordinated control of the system will be available from this platform;
  - the CNM can be positioned and re-positioned wherever and whenever convenient.
- limited:
  - the central management facility may only be able to use limited capabilities such as remote logon to each of the local network management facilities. Any co-ordinated control of the system may therefore need to be done manually;
  - the CNM can be positioned and re-positioned possibly subject to restrictions.
- none:
  - where there is no integration between systems, separate management platforms, perhaps co-located, will be needed. Any co-ordinated control of the system will need to be done manually;

- it is unlikely that the CNM can be re-positioned with ease.

As time progresses, it is expected that all systems will become more and more integrated.

## 7 User's specification check list

This clause attempts to assist end user organizations in writing organization-specific functional requirements specifications for NMFs for TETRA systems, using ETR 292 [1] as a guideline.

### 7.1 Matters to be taken into account

Before one starts to write down functional requirements, a number of issues will have to be addressed. The following subclauses discuss in brief a few aspects that will have their impact on the structure as well as the complexity of the NMFs.

#### 7.1.1 Organization of network management

Before a detailed functional specification is written, it should be clear in what way the TETRA infrastructure will be managed (i.e. how will the management be organized). For practical as well as historic reasons, management of the network will be performed differently, depending on the end user organization.

The end user organization may be divided into a number of regions, each with their own facilities for network and subscriber management. In general, four types of management can be distinguished in such an organization:

- central technical management (which covers all TETRA infrastructure within the organization);

- central subscriber management (which covers all subscribers within the organization);

- local technical management;

- local subscriber management.

Depending on the end user organization, each type will contain different network management functions. Please note that the central and local management as mentioned above do not imply that the infrastructure consists of multiple TETRA networks (see subclause 5.3). Also, not every end user organization will need to implement all four types of management (e.g. in a small TETRA network only local management functions will have to be available).

#### 7.1.2 Geographical division of management facilities

In general, network management will take place from more than one location. On every location, one or more management terminals will be available. Important questions to be answered here are:

- On which locations will management terminals have to be installed (and how many)?

- Is it required that technical and subscriber management be logically and/or physically separated?

- Which management functions are (roughly) required on which locations?

#### 7.1.3 Distribution of management functions among players

In general, network management will be performed by a number of staff. Different management functions will have to be accessed by different players (e.g. subscriber and technical management generally will be done by different personnel). Questions to be answered here are:

- What will be the division of responsibilities between the various players?

- Is it necessary that players can access certain management functions from more than one location?

- Will there be a hierarchy of managers?

### 7.1.4 Flexibility of the network management system

Depending on the end user organization, the TETRA infrastructure, as well as the supporting management facilities will need to have a different degree of flexibility. Questions to be answered here are:

- Is the end user organization likely to undergo any change during the lifetime of the network, and what will be the impact on the organization of the network management?

- Which facilities are required to be able to anticipate the expected changes (e.g. are extra facilities needed to support change management)?

## 7.2 Writing requirements

### 7.2.1 What is in ETR 292

Clauses 1 to 4 of ETR 292 [1] introduce the subject of TETRA network management standardization. Clause 5 describes a reference management architecture for TETRA networks, and also introduces a number of players. It is assumed that (multiple) TETRA networks are managed locally as well as from a central location, with specific local and central management functions available. Clause 6 gives an extensive overview of network management functions, indicating for each function whether it should be available centrally or locally, and by whom (i.e. by which player) it is to be used. Both subscriber and technical Management are covered, grouped according to a number of MFAs.

Although ETR 292 [1] lists a number of standardized CNM-LNM services, a CNM may also provide additional services.

### 7.2.2 Writing functional requirements

Using ETR 292 [1] as a guideline, an end user organization can write functional requirements specifications for management of any TETRA system. Briefly, the steps to be taken will be the following:

1) Decide how the Network Management will be organized (see subclause 7.1.1).

2) Decide from which locations Network Management activities will take place (see subclause 7.1.2).

3) Decide which players are to be distinguished, and what will be their tasks (see subclause 7.1.3).

4) Develop some ideas on how flexible the Network Management system needs to be (see subclause 7.1.4).

5) Go over all management functions mentioned in the subclauses of ETR 292 [1], clause 6.

6) For every separate management function, decide whether or not it is required in some form or another. Take into account the conditions formulated in steps 1 through 4.

7) If necessary, extend, or change slightly, the definition of the management function to suit the specific requirements of the end user organization.

8) Consider on which geographic locations the management function should be available.

9) Consider by which players the management function is to be used.

10) Finally, consider if, for every one of the MFAs as described in ETR 292 [1], clause 6, extra functions need to be added to suit the organization's requirements.

The above procedure will result in a list of management functions, grouped according to the MFAs as defined in ETR 292 [1].

### 7.2.3 Writing requirements for network management protocols and platforms

When specifying a network management solution the following factors should be considered:

- ease of integration with existing and future systems;
- up-gradability;
- support and ongoing maintenance;
- multi-sourcing;
- availability of applications software;
- ability to test;
- performance issues;
- ergonomics.

ETR 292 [1], clause 8 provides an overview of network management protocol standards.

### 7.2.4 Other requirements

Depending on the type of end user organization, additional requirements on the network management system may apply, for example:

- requirements on the performance (e.g. response time of "real time" and other actions) of the network management system;
- requirements on the availability of the network management system;
- practical issues such as remote alarm indications in case of fire, burglary or otherwise, in components of the TETRA infrastructure;
- requirements with respect to network management under special circumstances.

# Annex A: Annotated list of references

The following list of references is provided to give an overview of network management information available, these documents are probably the most useful, however this list is not exhaustive.

The TMN and OSI documents are available from ITU-T. The SNMP documents are available on the Internet.

## A.1 TMN

| ITU-T Recommendation | Title |
|---|---|
| M.3000 | Overview of TMN Recommendations |
| M.3010 | Principals objectives and concepts and reference configurations of TMN. Introduction of the TMN Architecture and the separation into three components; Functional Informational and Physical Architecture |
| M.3020 | Describes the processes to be used for functional and protocol specification of TMN interfaces |
| M.3100 | Conformance proforma for TMN systems |
| M.3180 | Catalogue of TMN Information |
| M.3200 | Overview of a set of recommendations containing descriptions of TMN Management services |
| M.3300 | TMN from the perspective of a user. (F Interface) |
| M.3400 | Description of TMN management functions in terms of the OSI management functional areas |

## A.2 OSI management

| ITU-T Recommendation | Title |
|---|---|
| X.700 | Management framework for OSI |
| X.701 | Overview of the X.700 series and how they relate to each other |
| X.710 | Common Management Information Service definition |
| X.711 | Common Management Information Protocol specification |
| X.712 | Common Management Information Protocol, protocol implementation conformance specification |
| X.720 | Management information model |
| X.721 | Definition of management information |
| X.722 | Guidelines for the definition of managed objects |
| X.723 | Generic Management Information for use in the specification of managed objects |
| X.730 | Object Management function |
| X.731 | State Management Function services |
| X.732 | State Management Function attributes |
| X.733 | Alarm Reporting Function |
| X.734 | Event Report Management Function |
| X.735 | Log Control Function |
| X.736 | Security Alarm Reporting Function |
| X.737 | Confidence and Diagnostic Test Categories |
| X.738 | Summarization Function |
| X.739 | Metric Objects and Attributes |
| X.740 | Security Audit Trail Function |
| X.741 | Objects and Attributes for Access Control |
| X.742 | Usage Metering Function |
| X.744 | Software Management Function |
| X.745 | Test Management Function |
| X.746 | Scheduling Function |

## A.3 SNMP

| Specification | Title |
|---|---|
| RFC 1155 | SNMP V1 Structure of Management Information |
| RFC 1157 | Simple Network Management Protocol Version 1 |
| RFC 1212 | Concise MIB Definition |
| RFC 1213 | Management Information Base (MIB II) |
| RFC 1215 | Convention for defining traps for use with SNMP v1 |
| RFC 1303 | Convention for describing SNMP Agents |
| RFC 1351 | SNMP Administrative Model |
| RFC 1352 | SNMP Security Protocols |
| RFC 1441 | Introduction to SNMP v2 |
| RFC 1442 | Structure of Management Information for SNMP v2 |
| RFC 1443 | Textual Conventions for SNMP v2 |
| RFC 1444 | Conformance statement for SNMP v2 |
| RFC 1445 | Administrative Model for SNMPv2 |
| RFC 1446 | Security protocols for SNMP v2 |
| RFC 1447 | Party MIB for SNMP v2 |
| RFC 1448 | Protocol Operations for SNMP v2 |
| RFC 1449 | Transport Mappings for SNMP v2 |
| RFC 1450 | MIB for SNMP v2 |
| RFC 1451 | Manager to Manager MIB SNMP v2 |
| RFC 1452 | Coexistence between SNMP v1 & SNMP v2 |

## History

| Document history | |
|---|---|
| July 1997 | First Edition |
| | |
| | |
| | |
| | |

ISBN 2-7437-1626-6
Dépôt légal : Juillet 1997