ETSI TS 132 111-1 V10.2.0 (2015-04)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Fault Management; Part 1: 3G fault management requirements (3GPP TS 32.111-1 version 10.2.0 Release 10)

Reference
RTS/TSGS-0532111-1va20

Keywords
GSM,LTE,UMTS

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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://ipr.etsi.org).

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 Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document is part of a TS-family covering the 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Telecommunication management; as identified below:

32.111-1 "Fault Management; Part 1: 3G fault management requirements".

32.111-2 "Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS)".

32.111-3 "Fault Management; Part 3: Alarm Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)".

32.111-6 "Fault Management; Part 6: Alarm Integration Reference Point (IRP): Solution Set (SS) definitions".

The present document is part of a TS-family, which describes the requirements and information model necessary for the Telecommunication Management (TM) of 3G systems. The TM principles and TM architecture are specified in 3GPP TS 32.101 [2] and 3GPP TS 32.102 [3].

A 3G system is composed of a multitude of Network Elements (NE) of various types and, typically, different vendors, which inter-operate in a co-ordinated manner in order to satisfy the network users' communication requirements. The occurrence of failures in a NE may cause a deterioration of this NE's function and/or service quality and will, in severe cases, lead to the complete unavailability of the respective NE. In order to minimize the effects of such failures on the Quality of Service (QoS) as perceived by the network users it is necessary to:

- detect failures in the network as soon as they occur and alert the operating personnel as fast as possible;
- isolate the failures (autonomously or through operator intervention), i.e. switch off faulty units and, if applicable, limit the effect of the failure as much as possible by reconfiguration of the faulty NE/adjacent NEs;
- if necessary, determine the cause of the failure using diagnosis and test routines; and,
- repair/eliminate failures in due time through the application of maintenance procedures.

This aspect of the management environment is termed "Fault Management" (FM). The purpose of FM is to detect failures as soon as they occur and to limit their effects on the network Quality of Service (QoS) as far as possible. The latter is achieved by bringing additional/redundant equipment into operation, reconfiguring existing equipment/NEs, or by repairing/eliminating the cause of the failure.

Fault Management (FM) encompasses all of the above functionalities except commissioning/decommissioning of NEs and potential operator triggered reconfiguration (these are a matter of Configuration Management (CM), cf. [1]).
FM also includes associated features in the Operations System (OS), such as the administration of a pending alarms list, the presentation of operational state information of physical and logical devices/resources/functions, and the provision and analysis of the alarm and state history of the network.

1 Scope

The present document specifies the overall requirements for 3G Fault Management (FM) as it applies to the Network Elements (NE), Element Manger (EM) and Network Manager (NM).

Clause 4 defines the FM concept and functional requirements for the detection of faults and the generation, collection and presentation of alarms, operational state data and test results across 3G systems. These functions are described on a non-formal level since the formal standardization of these functions across the different vendors' equipment is not required. The functional areas specified in the present document cover:

- fault surveillance and detection in the NEs;
- notification of alarms (including alarm cease) and operational state changes;
- retrieval of current alarms from the NEs;
- fault isolation and defence mechanisms in the NEs;
- alarm filtering;
- management of alarm severity levels;
- alarm and operational state data presentation and analysis at the Operations System (OS);
- retention of alarm and operational state data in the NEs and the OS; and
- the management of tests.

Any (re)configuration activity exerted from the EM as a consequence of faults will not be subject of the present document. These are described in [1].

Clause 5 of the present document defines the functional requirements for the standard Itf-N, for the purpose of Fault Management of 3G networks, as seen from the Network Manager (NM). The Itf-N is fully standardized so as to connect systems of any vendor to the NM via this interface.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 32.601: "Telecommunication management; Configuration Management (CM); Basic CM Integration Reference Point (IRP); Requirements".

[2] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".

[3] 3GPP TS 32.102: "Telecommunication management; Architecture".

[4] 3GPP TS 32.401: "Telecommunication management; Performance Management (PM); Concept and requirements".

[5] ITU-T Recommendation X.710: "Information technology - Open Systems Interconnection - Common Management Information Service".

[6] ITU-T Recommendation X.711: "Managed objects for diagnostic information of public switched telephone network connected V-series modem DCE's".

[7] ITU-T Recommendation X.721: "Information technology - Open Systems Interconnection - Structure of management information: Definition of management information".

[8] ITU-T Recommendation X.731: "Information technology - Open Systems Interconnection - Systems Management: State management function".

[9] ITU-T Recommendation X.733: "Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function".

[10] ITU-T Recommendation X.734: "Information technology - Open Systems Interconnection - Systems Management: Event report management function".

[11] ITU-T Recommendation X.735: "Information technology - Open Systems Interconnection - Systems Management: Log control function".

[12] ITU-T Recommendation X.745: "Information technology - Open Systems Interconnection - Systems Management: Test management function".

[13] 3GPP TS 32.111-2: "Telecommunication management; Fault Management; Part 2: Alarm Integration Reference Point (IRP); Information Service (IS)".

[14] 3GPP TS 32.111-3: "Telecommunication management; Fault Management; Part 3: Alarm Integration Reference Point (IRP); Common Object Request Broker Architecture (CORBA) Solution Set (SS)".

[15] Void.

[16] ISO 8571: "File Transfer, Access and Management".

[17] 3GPP TS 32.111-7: "Telecommunication management; Fault Management; Alarm Integration Reference Point (IRP); SOAP Solution Set (SS)".

[18] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions in 3GPP TS 32.101 [2], 3GPP TS 32.102 [3], 3GPP TS 21.905 [18] and the following apply:

active alarm: an alarm that has not been cleared and which is active until the fault that caused the alarm is corrected and a "clear alarm" is generated.

ADAC Faults: faults that are "Automatically Detected and Automatically Cleared" by the system when they occur and when they are repaired.

ADMC Faults: faults that are Automatically Detected by the system when they occur and Manually Cleared by the operator when they are repaired.

alarm: abnormal network entity condition, which categorizes an event as a fault.

alarm notification: notification used to inform the recipient about the occurrence of an alarm.

clear alarm: alarm where the severity value is set to "cleared".

event: this is a generic term for any type of occurrence within a network entity.

NOTE: A notification or event report may be used to inform one or more OS(s) about the occurrence of the event.

fault: a deviation of a system from normal operation, which may result in the loss of operational capabilities of the element or the loss of redundancy in case of a redundant configuration.

Itf-N: Management interface defined in 3GPP TS 32.101 [2] subclause 5.1.2.2 and 3GPP TS 32.102 [3] subclause 7.3.2.

notification: information message originated within a network entity to inform one or more OS(s) about the occurrence of an event.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TS 32.101 [2], 3GPP TS 32.102 [3], 3GPP TS 21.905 [18] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TS 32.101 [2], 3GPP TS 32.102 [3] and 3GPP TS 21.905 [18], in that order.

ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
CM	Configuration Management
EM	Element Manger
FM	Fault Management
ISO	International Standards Organisation
IRP	Integration Reference Point
MMI	Man-Machine Interface
MOC	Managed Object Class
MOI	Managed Object Instance
NE	Network Element
NM	Network Manager
OS	Operations System
QoS	Quality of Service
TMN	Telecommunications Management Network

4 Fault Management concept and requirements

4.0 Introduction

Any evaluation of the NEs' and the overall network health status require the detection of faults in the network and, consequently, the notification of alarms to the OS (EM and/or NM). Depending on the nature of the fault, it may be combined with a change of the operational state of the logical and/or physical resource(s) affected by the fault. Detection and notification of these state changes is as essential as it is for the alarms. A list of active alarms in the network and operational state information as well as alarm/state history data are required by the system operator for further analysis. Additionally, test procedures can be used in order to obtain more detailed information if necessary, or to verify an alarm or state or the proper operation of NEs and their logical and physical resources.

The following clauses explain the detection of faults, the handling of alarms and state changes and the execution of tests.

Only those requirements covered by clause 5 and related IRPs shall be considered as valid requirements for compliance to the standard defined by the present document.

4.1 Faults and alarms

4.1.0 Introduction

Faults that may occur in the network can be grouped into one of the following categories:

- Hardware failures, i.e. the malfunction of some physical resource within a NE.

- Software problems, e.g. software bugs, database inconsistencies.
- Functional faults, i.e. a failure of some functional resource in a NE and no hardware component can be found responsible for the problem.
- Loss of some or all of the NE's specified capability due to overload situations.
- Communication failures between two NEs, or between NE and OS, or between two OSs.

In any case, as a consequence of faults, appropriate alarms related to the physical or logical resource(s) affected by the fault(s), shall be generated by the network entities.

The following clauses focus on the aspects of fault detection, alarm generation and storage, fault recovery and retrieval of stored alarm information.

4.1.1 Fault detection

When any type of fault described above occurs within a 3G network, the affected network entities shall be able to detect them immediately.

The network entities accomplish this task using autonomous self-check circuits/procedures, including, in the case of NEs, the observation of measurements, counters and thresholds. The threshold measurements may be predefined by the manufacturer and executed autonomously in the NE, or they may be based on performance measurements administered by the EM, cf. [4]. The fault detection mechanism as defined above shall cover both active and standby components of the network entities.

The majority of the faults should have well-defined conditions for the declaration of their presence or absence, i.e. fault occurrence and fault clearing conditions. Any such incident shall be referred to in the present document as an ADAC fault. The network entities should be able to recognize when a previously detected ADAC fault is no longer present, i.e. the clearing of the fault, using similar techniques as they use to detect the occurrence of the fault. For some faults, no clearing condition exists. For the purpose of the present document, these faults shall be referred to as ADMC faults. An example of this is when the network entity has to restart a software process due to some inconsistencies, and normal operation can be resumed afterwards. In this case, although the inconsistencies are cleared, the cause of the problem is not yet corrected. Manual intervention by the system operator shall always be necessary to clear ADMC faults since these, by definition, cannot be cleared by the network entity itself.

For some faults there is no need for any short-term action, neither from the system operator nor from the network entity itself, since the fault condition lasted for a short period of time only and then disappeared. An example of this is when a NE detects the crossing of some observed threshold, and in the next sampling interval, the observed value stays within its limits.

For each fault, the fault detection process shall supply the following information:

- the device/resource/file/functionality/smallest replaceable unit as follows:
  - for hardware faults, the smallest replaceable unit that is faulty;
  - for software faults, the affected software component, e.g. corrupted file(s) or databases or software code;
  - for functional faults, the affected functionality;
  - for faults caused by overload, information on the reason for the overload;
  - for all the above faults, wherever applicable, an indication of the physical and logical resources that are affected by the fault if applicable, a description of the loss of capability of the affected resource.
- the type of the fault (communication, environmental, equipment, processing error, QoS) according to ITU-T Recommendation X.733 [9];
- the severity of the fault (indeterminate, warning, minor, major, critical), as defined in ITU-T Recommendation X.733 [9];
- the probable cause of the fault;
- the time at which the fault was detected in the faulty network entity;