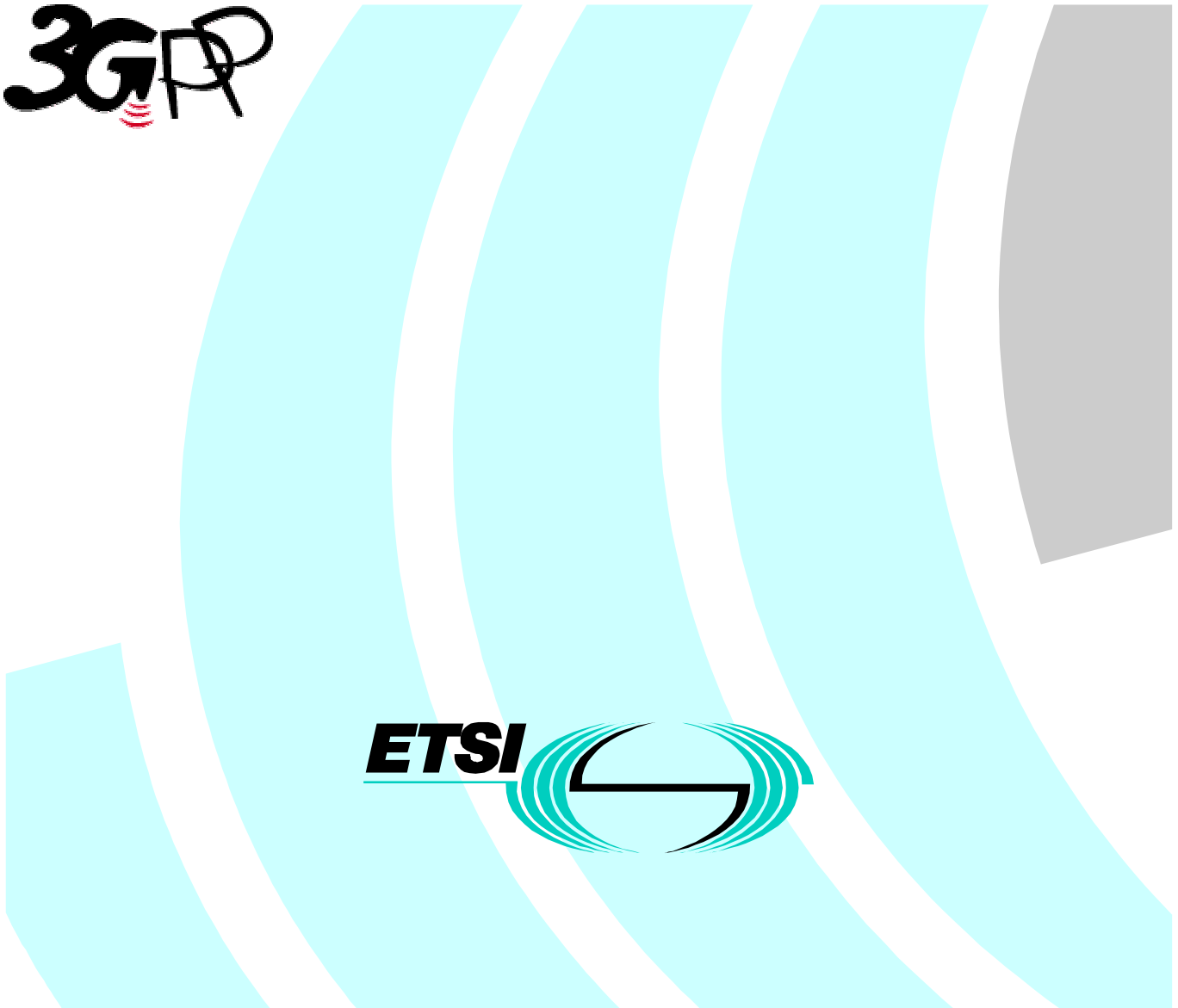
ETSI TS 132 111-1 V3.1.0 (2000-07)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Telecommunication Management; Fault Management;
Part 1: 3G fault management requirements
(3G TS 32.111-1 version 3.1.0 Release 1999)



Reference
RTS/TSGS-0532111UR1

Keywords
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

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://www.etsi.org/ipr).

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 the 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 www.etsi.org/key .

Contents

Foreword

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

The present document is part 1 of a multi-part TS covering the 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, as identified below:

Part 1: "3G Fault Management Requirements";

Part 2: "Alarm Integration Reference Point: Information Service";

Part 3: "Alarm Integration Reference Point: CORBA Solution Set Version 1:1";

Part 4: "Alarm Integration Reference Point: CMIP Solution Set".

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 set of TSs which describe the requirements and information model necessary for the Telecommunication Management (TM) of 3G systems. The TM principles and TM architecture are specified in 3G TS 32.101 [2] and 3G 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 minimise 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. 3G TS 32.106 [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 standardisation 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 3G TS 32.106 [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 standardised 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.

[1] 3G TS 32.106-x: "3G Configuration Management".

[2] 3G TS 32.101: "3G Telecom Management principles and high level requirements".

[3] 3G TS 32.102: "3G Telecom Management architecture".

[4] 3G TS 32.104: "3G Performance Management".

[5] ITU-T Recommendation X.710: "Common management information service definition for CCITT applications".

[6] ITU-T Recommendation X.711: "Common management information protocol specification for CCITT applications".

[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] 3G TS 32.111-2: "Alarm Integration Reference Point: Information Service".

[14] 3G TS 32.111-3: "Alarm Integration Reference Point: CORBA Solution Set Version 1:1".

[15] 3G TS 32.111-4: "Alarm Integration Reference Point: CMIP Solution Set".

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

3 Definitions and abbreviations

3.1 Definitions

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

Active alarm: an alarm that has not been cleared. An alarm 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: an alarm is an abnormal network entity condition, which categorises an event as a fault.

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

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

Event: this is a generic term for any type of occurrence within a network entity. 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. This deviation may result in the loss of operational capabilities of the element or the loss of redundancy in case of a redundant configuration

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 following abbreviations apply:

ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
CCITT	The International Telegraph and Telephone Consultative Committee
CM	Configuration Management
CMIP	Common Management Information Protocol
EM	Element Manger
ETSI	European Telecommunications Standards Institute
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

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 subclauses 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

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 subclauses 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. 3G TS 32.104 [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 recognise 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;
- the nature of the fault, e.g. ADAC or ADMC;
- any other information that helps understanding the cause and the location of the abnormal situation (system/implementation specific).

For some faults, additional means, such as test and diagnosis features, may be necessary in order to obtain the required level of detail. See subclause 4.3 for details.

4.1.2 Generation of alarms

For each detected fault, appropriate alarms shall be generated by the faulty network entity, regardless of whether it is an ADAC or an ADMC fault. Such alarms shall contain all the information provided by the fault detection process as described in subclause 4.1.1.

In order to ease the fault localisation and repair, the faulty network entity should generate for each single fault, one single alarm, also in the case where a single fault causes a degradation of the operational capabilities of more than one physical or logical resource within the network entity. An example of this is a hardware fault, which affects not only a physical resource but also degrades the logical resource(s) that this hardware supports. In this case the network entity should generate one single alarm for the faulty resource (i.e. the resource which needs to be repaired) and a number of events related to state management (cf. subclause 4.2) for all the physical/logical resources affected by the fault, including the faulty one itself.

In case a network entity is not able to recognise that a single fault manifests itself in different ways, the single fault is detected as multiple faults and originates multiple alarms. In this case however, when the fault is repaired the network entity should be able to detect the repair of all the multiple faults and clear the related multiple alarms.

When a fault occurs on the connection media between two NEs or between a NE and an OS, and affects the communication capability between such NE/OS, each affected NE/OS shall detect the fault as described in subclause 4.1.1 and generate its own associated communication alarm toward the managing OS. In this case it is the responsibility of the OS to correlate alarms received from different NEs/OSs and localise the fault in the best possible way.

Within each NE, all alarms generated by that NE shall be input into a list of active alarms. The NEs shall be able to provide such a list of active alarms to the OS when requested.

4.1.3 Clearing of alarms

The alarms originated in consequence of faults need to be cleared. To clear an alarm it is necessary to repair the corresponding fault. The procedures to repair faults are implementation dependent and therefore they are out of the scope of the present document, however, in general:

- the equipment faults are repaired by replacing the faulty units with working ones;
- the software faults are repaired by means of partial or global system initialisations, by means of software patches or by means of updated software loads;
- the communication faults are repaired by replacing the faulty transmission equipment or, in case of excessive noise, by removing the cause of the noise;
- the QOS faults are repaired either by removing the causes that degraded the QOS or by improving the capability of the system to react against the causes that could result in a degradation of the QOS;
- Solving the environmental problem repairs the environment faults (high temperature, high humidity, etc.).

It is also possible that an ADAC fault is spontaneously repaired, without the intervention of the operator (e.g. a threshold crossed fault). In this case the NE behaves as for the ADAC faults repaired by the operator.

In principle, the NE uses the same mechanisms to detect that a fault has been repaired, as for the detection of the occurrence of the fault. However, for ADMC faults, manual intervention by the operator is always necessary to clear the fault. Practically, various methods exist for the system to detect that a fault has been repaired and clear alarms and the faults that triggered them. For example:

- The system operator implicitly requests the NE to clear a fault, e.g. by initialising a new device that replaces a faulty one. Once the new device has been successfully put into service, the NE shall clear the fault(s). Consequently, the NE shall clear all related alarms.
- The system operator explicitly requests the clearing of one or more alarms. Once the alarm(s) has/have been cleared, the NE shall detect that the fault condition has ceased.

- The NE detects the exchange of a faulty device by a new one and initialises it autonomously. Once the new device has been successfully put into service, the NE shall clear the fault(s). Consequently, the NE shall clear all related alarms.

- The NE detects that a previously reported threshold crossed alarm is no longer valid. It shall then clear the corresponding active alarm and the associated fault, without requiring any operator intervention. The details for the administration of thresholds and the exact condition for the NE to clear a threshold crossed alarm are implementation specific and depend on the definition of the threshold measurement, see also subclause 4.1.1.

- ADMC faults/alarms can, by definition, not be cleared by the NE autonomously. Therefore, in any case, system operator functions shall be available to request the clearing of ADAC alarms/faults in the NE. Once an ADMC alarm/fault has been cleared, the NE shall clear the associated ADAC fault/alarm.

Details of these mechanisms are system/implementation specific.

Each time an alarm is cleared the NE shall generate an appropriate clear alarm event. A clear alarm is defined as an alarm, as specified in subclause 3.1, except that its severity is set to "cleared". The relationship between the clear alarm and the active alarm is established:

- by re-using a set of parameters that uniquely identify the active alarm (cf. subclause 4.1.1); or

- by including a reference to the active alarm in the clear alarm.

When a clear alarm is generated the corresponding active alarm is removed from the active alarm list.

4.1.4 Alarm forwarding and filtering

As soon as an alarm is entered into or removed from the active alarms list Alarm notifications shall be forwarded by the NE, in the form of unsolicited notifications;

If forwarding is not possible at this time, e.g. due to communication breakdown, then the notifications shall be sent as soon as the communication capability has been restored. The storage space is limited. The storage capacity is Operator and implementation dependent. If the number of delayed notifications exceeds the storage space then an alarm synchronisation procedure shall be run when the communication capability has been restored.

The OS shall detect the communication failures that prevent the reception of alarms and raise an appropriate alarm to the operator.

If the N interface is implemented in the NE, then the destination of the notifications is the NM, and the interface shall comply with the stipulations made in clause 5. If the N interface resides in the EM, proprietary means may be employed to forward the notifications to the EM. Note that, even if the N interface is implemented in the NE, the EM may still also receive the notifications by one of the above mechanisms, however, the present document does not explicitly require the NEs to support the EM as a second destination.

The event report shall include all information defined for the respective event (cf. subclauses 4.1.1, 4.1.2 and 4.1.3), plus an identification of the NE that generated the report.

The system operator shall be able to allow or suppress alarm reporting for each NE. As a minimum, the following criteria shall be supported for alarm filtering:

- the NE that generated the alarm, i.e. all alarm messages for that NE shall be suppressed;

- the device/resource/function to which the alarm relates;

- the severity of the alarm, except "clear". Suppression of alarm clear messages shall be determined according to the following stipulations:

  - if the initial alarm was not suppressed, then the alarm cleared message shall also be forwarded;

  - if the initial alarm was suppressed, then the criteria set for alarm suppression at the time the cleared message occurs shall be taken into account;

- the time at which the alarm was detected, i.e. the alarm time; and,

- any combination of the above criteria.

The result of any command to modify the forwarding criteria shall be confirmed by the NE to the requesting operator.

4.1.5 Storage and retrieval of alarms in/from the NE

For Fault Management (FM) purposes, each NE shall have to store and retain the following information:

- a list of all active alarms, i.e. all alarms that have not yet been cleared; and
- alarm history information, i.e. all notifications related to the occurrence and clearing of alarms.

It shall be possible to apply filters when active alarm information is retrieved by the Manager and when the history information is stored by the NE and retrieved by the Manager.

The storage space for alarm history in the NE is limited. Therefore it shall be organised as a circular buffer, i.e. the oldest data item(s) shall be overwritten by new data if the buffer is full. Further "buffer full" behaviours, e.g. those defined in [11], may be implemented as an option. The storage capacity itself, and thus the duration, for which the data can be retained, shall be Operator and implementation dependent.

4.1.6 Fault Recovery

After a fault has been detected and the replaceable faulty units have been identified, some management functions are necessary in order to perform system recovery and/or restoration, either automatically by the NE and/or the EM, or manually by the operator.

The fault recovery functions are used in various phases of the Fault Management (FM):

1) Once a fault has been detected, the NE shall be able to evaluate the effect of the fault on the telecommunication services and autonomously take recovery actions in order to minimise service degradation or disruption.

2) Once the faulty unit(s) has (have) been replaced or repaired, it shall be possible from the EM to put the previously faulty unit(s) back into service so that normal operation is restored. This transition should be done in such a way that the currently provided telecommunication services are not, or only minimally, disturbed.

3) At any time the NE shall be able to perform recovery actions if requested by the operator. The operator may have several reasons to require such actions; e.g. he has deduced a faulty condition by analysing and correlating alarm reports, or he wants to verify that the NE is capable of performing the recovery actions (proactive maintenance).

The recovery actions that the NE performs (autonomously or on demand) in case of faults depend on the nature and severity of the faults, on the hardware and software capabilities of the NE and on the current configuration of the NE.

Faults are distinguished in two categories: software faults and hardware faults. In the case of software faults, depending on the severity of the fault, the recovery actions may be system initialisations (at different levels), activation of a backup software load, activation of a fallback software load, download of a software unit etc. In the case of hardware faults, the recovery actions depend on the existence and type of redundant (i.e. back-up) resources. Redundancy of some resources may be provided in the NE in order to achieve fault tolerance and to improve system availability.

If the faulty resource has no redundancy, the recovery actions shall be:

a) Isolate and remove from service the faulty resource so that it cannot disturb other working resources;

b) Remove from service the physical and functional resources (if any) which are dependent on the faulty one. This prevents the propagation of the fault effects to other fault-free resources;

c) State management related activities for the faulty resource and other affected/dependent resources, cf. subclause 4.2;

d) Generate and forward appropriate notifications to inform the OS about all the changes performed.

If the faulty resource has redundancy, the NE shall perform action a), c) and d) above and, in addition, the recovery sequence that is specific to that type of redundancy. Several types of redundancy exist (e.g. hot standby, cold standby, duplex, symmetric/asymmetric, N plus one or N plus K redundancy, etc.), and for each one, there is a specific sequence

of actions to be performed in case of failure. The present document specifies the Fault Management aspects of the redundancies, but it does not define the specific recovery sequences of the redundancy types.

In the case of a failure of a resource providing service, the recovery sequence shall start immediately. Before or during the changeover, a temporary and limited loss of service shall be acceptable. In the case of a management command, the NE should perform the changeover without degradation of the telecommunication services.

The detailed definition of the management of the redundancies is out of the scope of the present document. If a fault causes the interruption of ongoing calls, then the interrupted calls shall be cleared, i.e. all resources allocated to these calls shall immediately be released by the system.

4.1.7 Configuration of Alarms

It shall be possible to configure the alarm actions, thresholds and severities by means of commands, according to the following requirements:

- the operator shall be able to configure any threshold that determines the declaration or clearing of a fault. If a series of thresholds are defined to generate alarms of various severities, then for each alarm severity the threshold values shall be configurable individually.

- it shall be possible to modify the severity of alarms defined in the system, e.g. from major to critical. This capability should be implemented on the manager, however, in case it is implemented on the NE, the alarms forwarded by the NE to the OS and the alarms displayed on the local MMI shall have the same severity.

The NE shall confirm such alarm configuration commands and shall notify the results to the requesting system operator.

4.2 State Management

The State Management is a common service defined within Configuration Management (3G TS 32.106 [1]) and used by several management areas, including Fault Management. In this clause, some detailed requirements on State Management as they apply to the Fault Management are defined.

From the point of view of Fault Management, only two of the three primary state attributes are really important: the Administrative state and the Operational state. In addition the resources may have some secondary "status" attributes which give further detailed information about the reason of the primary state.

The Administrative state is used by the Operator to make a resource available for service, or to remove a resource from service. For example:

- for fault correction the Administrative state can be used to isolate a faulty resource;

- in case of redundancy the Administrative state can be used to lock the active resource and let the standby resource to become active (preventive maintenance);

- for Test management the Administrative state can be used to put a resource out of service to run an intrusive test on it.

The Operational state gives the information about the real capability of a resource to provide or not provide service.

- The operational state is "enabled" when the resource is able to provide service, "disabled" when the resource cannot provide service.

- A resource can lose the capability to provide service because of a fault or because another resource on which it depends is out of service (e.g. disabled or locked).

- In case a resource does not loose completely its capability to provide service, the Operational state shall be "enabled" and the Availability status shall be "degraded".

The changes of the state and status attributes of a resource shall be notified to the relative manager(s) as specified in 3G TS 32.106 [1].

When a state change is originated by a failure, the alarm notification and the related state change notifications shall be correlated to each other by means of explicit relationship information.

4.2.1 Propagation of state change

Within a managed element, when for any reason a resource changes its state, the change shall be propagated, in a consistent way, to all the other resources that are functionally dependent on the first one. Therefore:

- In case of a fault occurring on a resource makes that resource completely out of service, if the current operational state is "enabled", it shall be changed to "disabled" and a state change notification shall be generated. Then, all the dependant resources (following the fault dependency diagram specific to that managed element) shall be checked and, in case they are "enabled" they shall be changed to "disabled". In this process, also the secondary status shall be changed consistently, in a way that it shall be possible to distinguish whether an object is disabled because it is faulty or because of it is functionally dependent on another object which is disabled.

- In case a faulty resource is repaired, the Operational state of that resource is changed from "disabled" to "enabled" and all the dependent resources are turned back to "enabled" (this is the simple case). In more complex cases, some of the objects may be disabled for different causes (different faults or faults plus locks on different superior resources), in this cases the repaired resource can be turned "enabled" only when all the causes are cleared (i.e. faults are repaired and superior resources are unlocked). Also in this process the secondary status shall be changed consistently.

- In case the operator locks a resource, the process of the state change propagation is similar to the first case (resource failure) except for the locked resource which does not change its operational state but only the administrative state from "unlocked" to "locked". The dependent resources are processed as in the first case.

- In case the operator unlocks a resource, the process of the state change propagation is similar to the second case (fault reparation) except for the first resource (the unlocked one) which does not change its operational state but only the administrative state from "locked" to "unlocked". The dependent resources are processed as in the first case.

4.3 Test management

This management function provides capabilities that can be used in different phases of the Fault Management (FM). For example:

- when a fault has been detected and if the information provided through the alarm report is not sufficient to localise the faulty resource, tests can be executed to better localise the fault;

- during normal operation of the NE, tests can be executed for the purpose of detecting faults;

- once a faulty resource has been repaired or replaced, before it is restored to service, tests can be executed on that resource to be sure that it is fault free.

However, regardless of the context where the testing is used, its target is always the same: verify if a system's physical or functional resource performs properly and, in case it happens to be faulty, provide all the information to help the operator to localise and correct the faults.

Testing is an activity that involves the operator, the managing system (the OS) and the managed system (the NE). Generally the operator requests the execution of tests from the OS and the managed NE autonomously executes the tests without any further support from the operator.

In some cases, the operator may request that only a test bed is set up (e.g. establish special internal connections, provide access test points, etc.). The operator can then perform the real tests, which may require some manual support to handle external test equipment. Since the "local maintenance" and the "inter NE testing" are out of the scope of the present document, this aspect of the testing is not treated any further.

The requirements for the test management service are based on ITU-T Recommendation X.745 [12], where the testing description and definitions are specified.

5 N interface (Itf-N)

5.1 Fault Management concept of Itf-N

An operations system on the network management layer (i.e. the NM) provides fault management services and functions required by the 3G operator on top of the element management layer.

The N interface (Itf-N) may connect the Network Management (NM) system either to Element Mangers (EMs) or directly to the Network Elements (NEs). This is done by means of Integration Reference Points (IRPs). In the following, the term "subordinate entities" defines either EMs or NEs, which are in charge of supporting the N interface.

This clause describes the properties of an interface enabling a NM to supervise a 3G-telecommunication network including - if necessary - the managing EMs. To provide to the NM the Fault Management capability for the network implies that the subordinate entities have to provide information about:

- events and failures occurring in the subordinate entities;
- events and failures of the connections towards the subordinate entities and also of the connections within the 3G network;
- the network configuration (due to the fact that alarms and related state change information are always originated by network resources, see 3G TS 32.106 [1]). This is, however, not part of the FM functionality.

Therefore, for the purpose of FM the subordinate entities send notifications to a NM indicating:

- alarm reports (indicating the occurrence or the clearing of failures within the subordinate entities), so that the related alarm information can be updated;
- state change event reports, so that the related (operational) state information can be updated. This is, however, not part of the FM functionality.

The forwarding of these notifications is controlled by the NM operator using adequate filtering mechanisms within the subordinate entities.

The Itf-N provides also means to allow the NM operator the storage ("logging") and the later evaluation of desired information within the subordinate entities.

The retrieval capability of alarm-related information concerns two aspects:

- retrieval of "dynamic" information (e.g. alarms, states), which describes the momentary alarm condition in the subordinate entities and allows the NM operator a synchronisation of its alarm overview data;
- retrieval of "history" information from the logs (e.g. active/clear alarms and state changes occurred in the past), which allows the evaluation of events that may have been lost, e.g. after an Itf-N interface failure or a system recovery.

As a consequence of the requirements described above, both the NM and the subordinate entity shall be able to initiate the communication.

5.2 Management of alarm event reports

5.2.1 Mapping of alarm and related state change event reports

The alarm and state change reports received by the NM relate to functional objects in accordance with the information model of Itf-N. This information model tailored for a multi-vendor capability is different from the information model of the EM-NE interface (if an EM is available) or from the internal resource modelling within the NE (in case of direct NM-NE interface). Thus a mapping of alarm and related state change event reports is performed by a mediation function within the subordinate entity.

The mediation function translates the original alarm/state change event reports (which may contain proprietary parameters or parameter values) taking into account the information model of the Itf-N.

If a mediation application function is needed, it works according to the following principles:

- Every alarm notification generated by a functional object in a subordinate entity is mapped to an alarm report of the corresponding ("equivalent") functional object at the Itf-N. If the functional object generating the original alarm notification has not a direct corresponding object at the Itf-N, the mediation functions maps the alarm to the next superior functional object in accordance with the containment tree of the Itf-N.

- Every state change notification generated by a functional object in a subordinate entity is mapped to a state change report of the corresponding ("equivalent") functional object at the Itf-N. If the functional object generating the original state change notification has not a direct corresponding object at the Itf-N, the mediation functions maps the alarm to the next superior functional object in accordance with the containment tree of the Itf-N.

Every alarm notification generated by a manufacturer-specific, equipment-related object in the subordinate entity is mapped to an alarm report of a generic logical object, which models the corresponding equipment-related resource.

5.2.2 Real-time forwarding of event reports

If the Itf-N is in normal operation (the NM connection to the subordinate entities is up), alarm reports are forwarded in real-time to the NM via appropriate filtering located in the subordinate entity. These filters may be controlled either locally or remotely by the managing NM (via Itf-N) and ensure that only the event reports which fulfil pre-defined criteria can reach the superior NM. In a multi-NM environment each NM shall have an own filter within every subordinate entity which may generate notifications.

5.2.3 Alarm clearing

On the Itf-N, alarm reports containing the value "cleared" of the parameter perceivedSeverity are used to clear the alarms. The correlation between the clear alarm and the related active alarms is performed by means of unambiguous identifiers.

This clearing mechanism ensures the correct clearing of alarms, independently of the (manufacturer-specific) implementation of the mapping of alarms/state change events in accordance with the information model of the Itf-N.

5.3 Retrieval of alarm information

The retrieval of alarm information comprises two aspects:

a) Retrieval of current information

   This mechanism shall ensure data consistency about the current alarm information between the NM and its subordinate entities and is achieved by means of a so-called synchronisation ("alignment") procedure, triggered by the NM. The synchronisation is required after every start-up of the Itf-N, nevertheless the NM may trigger it at any time.

b) Logging and retrieval of history information

   This mechanism offers to the NM the capability to get the alarm information stored within the subordinate entities for later evaluation.

5.3.1 Retrieval of current alarm information on NM request

The present document defines a flexible, generic synchronisation procedure, which fulfils the following requirements:

- The alarm information provided by means of the synchronisation procedure shall be the same (at least for the mandatory parameters) as the information already available in the alarm list. The procedure shall be able to assign the received synchronisation-alarm information to the correspondent requests, if several synchronisation procedures triggered by one NM run at the same time.
- The procedure shall allow the NM to trigger the start at any time and to recognise unambiguously the end and the successful completion of the synchronisation.
- The procedure shall allow the NM to discern easily between an "on-line" (spontaneous) alarm report and an alarm report received as consequence of a previously triggered synchronisation procedure.
- The procedure shall allow the NM to specify filter criteria in the alignment request (e.g. for a full network or only a part of it.
- The procedure shall support connections to several NM and route the alignment-related information only to the requesting NM.
- During the synchronisation procedure new ("real-time") alarms may be sent at any time to the managing NM.

If applicable, an alarm synchronisation procedure may be aborted by the requesting NM

5.3.2 Logging and retrieval of alarm history information on NM request

The alarm history information may be stored in the subordinate entities in dependence of the NM requirements. The NM is able to create logs for alarm reports and to define the criteria for storage of alarm information according to ITU-T Recommendation X.735 [11].

Nevertheless these particular requirements are not specific for alarm or state change information.

5.4 Co-operative alarm acknowledgement on the Itf-N

The acknowledgement of an alarm is a maintenance function that aids the operators in his day to day management activity of his network. An alarm is acknowledged by the operator to indicate he has started the activity to resolve this specific problem. In general a human operator performs the acknowledgement, however a management system (NM or EM) may automatically acknowledge an alarm as well.

The alarm acknowledgement function requires that:

a) All involved OSs have the same information about the alarms to be managed (including the current responsibility for alarm handling).

b) All involved OSs have the capability to send and to receive acknowledgement messages associated to previous alarm reports.

A co-operative alarm acknowledgement means that the acknowledgement performed at EM layer is notified at NM layer and vice versa, thus the acknowledgement-related status of this alarm is the same across the whole management hierarchy.

The co-operative alarm acknowledgement on Itf-N shall fulfil the following requirements:

- Acknowledgement messages may be sent in both directions between EMs and NM, containing the following information:
- Correlation information to the alarm just acknowledged.
- Acknowledgement history data, including the current alarm state (active | cleared), the time of alarm acknowledgement and, as configurable information, the management system (EM | NM) and the operator in charge of acknowledgement (the parameter operator name or, in case of auto-acknowledgement, a generic system name).
- Acknowledgement notifications sent to NM shall be filtered with the same criteria applied to the alarms.
- Taking into account the acknowledgement functionality, the above described synchronisation procedure for retrieval of current alarm information on NM request may be extended. Additionally to the requirements defined in subclause 5.3.1, this extended synchronisation procedure relates not only to the active, but also to the "cleared and not acknowledged" alarms, which have still to be managed by the EM.

5.5 Overview of IRPs related to Fault Management (FM)

The N interface is built up by a number of IRPs. The basic structure of the IRPs is defined in 3G TS 32.101 [2] and 3G TS 32.102 [3].

For the purpose of FM the following IRPs are needed:

- Alarm IRP, see Part 2 of this TS, i.e. 3G TS 32.111-2 [13]
- Notification IRP, see 3G TS 32.106 [1]
- Log IRP

NOTE: The Log IRP is not part of Release 1999, therefore the requirements related to the log functionality are not valid for Release 1999).

Annex A (informative): Change history

Change history					
TSG SA#	**Version**	**CR**	**Tdoc SA**	**New Version**	**Subject/Comment**
S_07	2.0.0	-	SP-000013	3.0.0	Approved at TSG SA #7 and placed under Change Control
Mar 2000	3.0.0			3.0.1	cosmetic
S_08	3.0.1	001	SP-000247	3.1.0	Split of TS - Part 1: Main part of spec – Requirements
S_08	3.0.1	002	SP-000248	3.1.0	Split of TS - Part 1: Merged Clause X into Clause 4
S_08	3.0.1	003	SP-000249	3.1.0	Split of TS - Part 1: Alignment of FM requirements with IRP, etc

History

Document history		
V3.0.1	March 2000	Publication as TS 132 111
V3.1.0	July 2000	Publication