ETSI TS 132 111-1 V17.0.0 (2022-04)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Telecommunication management;
Fault Management;
Part 1: 3G fault management requirements
(3GPP TS 32.111-1 version 17.0.0 Release 17)

Reference
RTS/TSGS-0532111-1vh00

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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 3GPP systems. The TM principles and TM architecture are specified in 3GPP TS 32.101 [2] and 3GPP TS 32.102 [3].

A 3GPP 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. TS 32.600 [19]).
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 3GPP 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 3GPP 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 [19].

Clause 5 of the present document defines the functional requirements for the standard Itf-N, for the purpose of Fault Management of 3GPP systems , 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] Void.

[6] Void.

[7] Void.

[8] Void.

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

[10] Void.

[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] Void.

[15] Void.

[16] Void.

[17] Void.

[18] NGMN Top OPE Recommendations V1.0.

[19] 3GPP TS 32.600: "Configuration Management (CM); Concept and high-level requirements".

[20] 3GPP TS 28.625: "State management data definition Integration Reference Point (IRP); Information Service (IS)".

[21] 3GPP TS 32.302: "Configuration Management (CM); Notification Integration Reference Point (IRP); Information Service (IS)".

[22] 3GPP TS 32.332: "Notification Log (NL) Integration Reference Point (IRP); Information Service (IS)".

[23] ANSI/ISA standard 18.2 -2009: "Management of Alarm Systems for the Process Industries ".

[24] 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 [24] 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: An alarm signifies an undesired condition of a resource (e.g. network element, link) for which an operator action is required. It emphasizes a key requirement that operators (above Itf-N) should not be informed about an undesired condition unless it requires operator action. Use of this emphasis does not exclude this case: In certain

context, it is not possible for alarm reporters (below Itf-N) to know whether a particular undesired condition requires operator action or not. In such context, the NM may receive alarms that do not require operator action.

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: Network occurrence which has significance for the management of an NE. Events do not have state.

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

managed alarm: The management representation of the alarm in the NM domain.

notification: Information message originated below Itf-N.

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 [24] 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 [24], in that order.

ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
CM	Configuration Management
EM	Element Manger
FM	Fault Management
HMA	Highly Managed Alarm
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 a3GPP system, 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;
- 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 clause 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 clause 4.1.1.

Examples of criteria for setting the alarm severity to “critical” are [18]:

- Total disturbance of the system or significant service impact for customers
- Performance, capacity, throughput restrictions
- Accounting disturbed

Examples of criteria for setting the alarm severity to “major” are [18]:

- Outage of a redundant component (e.g. outage of a redundant power supply)
- Introduction of retaliatory actions required, to ensure the service availability

In order to ease the fault localization 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. clause 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 recognize 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 clause 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 localize 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.

Alarm maintenance manuals must contain a clear repair action for the dedicated malfunction. The repair action shall also be populated in the corresponding alarm field (see [18]).

Wherever possible, event-based automated repair actions to solve standard error situations without manual interaction should be implemented, if not already implemented on the Network Element level (see [18]).

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 initializations, 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 initializing 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 fault management system (within EM and/or NE) should reissue those alarms (as new alarms) in case the fault situation still persists.
- The NE detects the exchange of a faulty device by a new one and initializes 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 clause 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 (see clause 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 synchronization 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 Itf-N 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 Itf-N resides in the EM, proprietary means may be employed to forward the notifications to the EM. Note that, even if the Itf-N 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 (see clauses 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;
- 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 organized 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 ITU-T Recommendation X.735 [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 minimize 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 initializations (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. clause 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.

4.1.8 Correlation of Alarms and Events

A single network fault may result in the generation of multiple alarms and events from affected entities over time and spread over a wide geographical area. If possible, the OS should indicate which alarms and events are correlated to each other.

Alarms may be correlated in view of certain rules such as alarm propagation path, specific geographical area, specific equipment, or repeated alarms from the same source. The alarms are partitioned into sets where alarms within one correlated set have a high probability of being caused by the same network fault. A correlated set may also contain events. These events are considered having a high probability of being related to the same network fault.

The correlation describes relations between network events (e.g. current alarms as those captured in AlarmList, historical alarms as those captured in NotificationLog, network configuration changes).

4.1.9 Root Cause Analysis

For a set of correlated alarms, one alarm may relate to the fault which is the root cause of all the correlated alarms and events. If possible, the OS should perfom a Root Cause Analysis to identify and indicate the Root Cause Alarm.

Root Cause Analysis is a process that can determine and identify the network condition (e.g. fault, mis-configuration) causing the alarms. The determination may be based on the following (for example):

- Information carried in alarm(s);
- Information carried in correlated alarm sets;
- Information carried in network notifications;
- Network configuration information;
- Operators' network management experience.

4.1.10 Managed Alarm

The alarm severities set by the network elements (NEs) in a mobile system, visible across the Itf-N, are basically resource focused (e.g. severity is set to major if NE available capacity is low). Vast amount of alarms classified as critical are potentially sent to operator's management centers but are rarely critical from the overall business perspective. They may even not be critical from the aspect of time to respond.

An operator's view can obviously be very different from the alarm severity defined by the NEs' resource focused views.

Operators need to enrich the information, i.e. the NE's resource focused view, for the purpose of the alarm management processes, see ref. [23]. The figure 4.1.10 introduces the concept of Managed Alarm, the management representation of the alarm in the NM domain (above Itf-N).

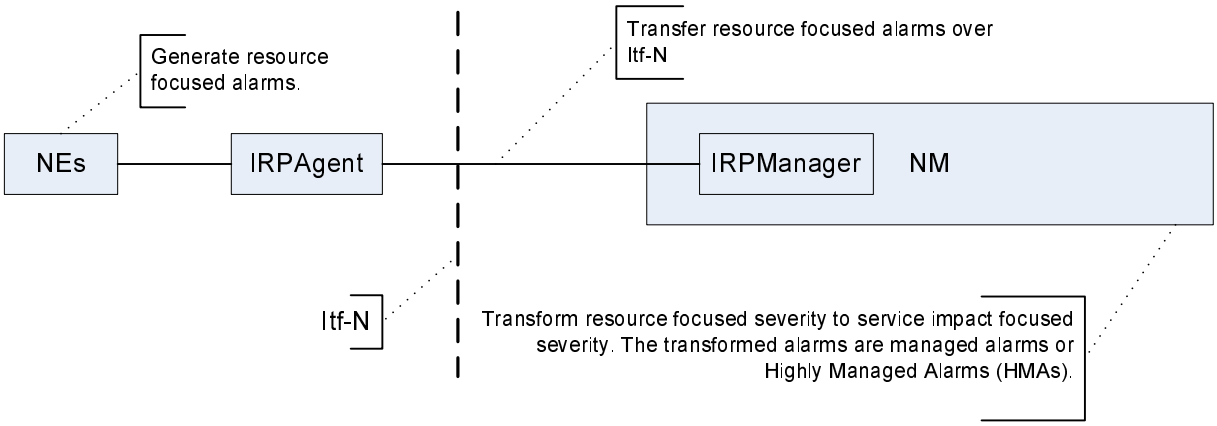

Figure 4.1.10

Within the NM, the received resource alarms are transformed so that the alarm severity is no longer resource focused but service impact focused, to prevent or mitigate network and service outage and degradation. The transformation applies to all severity levels.

A very special important class of managed alarm is the Highly Managed Alarm (HMA) class, introduced by the ANSI/ISA standard in ref. [23].

These HMAs are the most critical alarms, catastrophic from operations, security, business or any other top level point of view. These HMAs should receive special treatment particularly when it comes to viewing their status in the Human-Machine Interface (HMI). These are the alarms that shall never be allowed to be delayed or lost and must always be given the highest attention.

Considerable high levels of administrative requirements are applicable for the HMAs. For companies following this standard, detailed documentation and a multitude of special administrative requirements in a precise way, need to be fulfilled.

These include:

- Specific shelving requirements, such as access control with audit trail;
- Specific "Out of Service" alarm requirements, such as interim protection, access control, and audit trail;
- Mandatory initial and refresher training with specific content and documentation;
- Mandatory initial and periodic testing with specific documentation;
- Mandatory training around maintenance requirements with specific documentation;
- Mandatory audit requirements.

The HMA classes are also subject to special requirements for operator training, frequency of testing, and archiving of alarm records for proof of regulatory compliance.

Millions of mobile customers are from time to time affected by major failures in the infrastructure of mobile systems. Service assurance management of the continuously increasing complexity of our mobile systems could benefit from concepts like HMAs. The most critical equipment should be identified and secured. The HMAs should be treated in the most thoughtful way. The HMAs should never be hidden, delayed etc. in e.g. alarm flooding.

Setup of HMAs, within the scope and responsibility of the NM, will include many of the processes identified in the alarm management lifecycle, see ref. [23].

4.2 State Management

4.2.0 Introduction

The State Management is a common service 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 TS 28.625 [20].

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 localize the faulty resource, tests can be executed to better localize 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 localize 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.

4.4 Operators' alarm handling

A 3GPP system is composed of a multitude of network elements of various types and with a variety of complexity. 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.

Alarm Surveillance of the network is the first line Network Management Assurance Activity and is often maintained in near real time. The very essence of the surveillance functionality is to alert the operating personnel when failures appear in the networks. This is emphasized by the following sentence from 3GPP TS 32.101 [2] clause 7.5.2 Standardisation objectives:

"In order to minimise the effects of such failures on the 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;".

The operating personnel are confronted with most of the alarm notifications. It is of significant importance that the alarms are of operational relevance otherwise valuable time and resources will be spent to identify the irrelevant alarms.

Operator response to an alarm may consist of many different steps such as:

- Recognizing the alarm;
- Acknowledging the alarm;
- Verifying that the alarm is valid and not a malfunction;
- Getting enhanced information related to the alarm;
- Analysing the situation in order to try to determine the cause of the alarm, potential service impact and decide upon actions on the alarm. This may include reporting/activating other people from the second line support;
- Taking actions which may include activating reset of network elements, replacing the faulty equipment, creating trouble reports, etc;
- Continuing the surveillance of the network element(s) to ensure the fault correction.

The alarm notifications are basically a human-machine interface and a common expectation is that operators should never miss alarms requiring an operation action. To be able to fulfil such a request the goal is to only monitor the necessary alarms at the right time by extracting the relevant ones.

The key criterion is that alarms must require an operator response – that is, an action.

The expectation of alarm handling includes the following:

- Few alarms;
- Alarms are clearly prioritized and presented to the operator;
- Each alarm requires a needed action;
- Each action is taken by the operator;
- Alarms suppression methods aid the operator to handle alarm flooding so that saturation of the alarm management systems will not happen and control of the network is never lost.

4.5 Quality of Alarms

The assumption to efficiently handle the potentially vast amount of alarms in a mobile system is that alarms must exist solely as a tool for the benefit of the operator, see clause 4.4. They are not to be configured as a miscellaneous recording tool or for the prime benefit of maintenance personal.

The information carried in the alarm message should also be good enough to ultimately feed and partly enable automatic-correlation engines. However, alarm response is still not an automated process involving deterministic machines; it is a complex human cognitive process involving thought and analysis. The human factors involved in alarm response are subject to many variables. The quality of the alarm notifications is of fundamental importance to enable an efficient management of a mobile system.

The key to secure the quality of the information presented to the operator is to present alarm notifications of high operational relevans, in a timely fashion. If e.g. secondary logs, status or performance data are provided, it must be possible to easily separate those from the alarms.

Some of the characteristics that an alarm should have are summarized below:

- Relevance i.e. not spurious or of low operational value;
- Uniqueness i.e. not duplicating another alarm;
- Timeliness i.e. not long before any response is needed or too late to do anything;
- Importance i.e. indicating the importance that the operator deals with the problem;
- Explicability i.e. having a message which is clear and easy to understand;
- Recognizance i.e. identifying the problem that has occurred;
- Guidance i.e. indicative of the action to be taken;
- Prioritization i.e. drawing attention to the most important issues.

5 Fault Management over Itf-N

5.1 Fault Management concept

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

The 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 Itf-N.

This clause describes the properties of an interface enabling a NM to supervise a 3GPP system 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 3GPP system ;
- the network configuration (due to the fact that alarms and related state change information are always originated by network resources, see [19]). 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 synchronization 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.

The following examples describe potential mediation function behaviour:

- Alarm notifications generated by a functional object in a subordinate entity can be mapped to alarm reports 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.

- State change notifications generated by a functional object in a subordinate entity can be mapped to state change reports 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.

The IRP manager may also clear alarms manually.

5.3 Retrieval of alarm information

5.3.0 Introduction

The retrieval of alarm information comprises two aspects:

- 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 synchronization ("alignment") procedure, triggered by the NM. The synchronization is required after every start-up of the Itf-N, nevertheless the NM may trigger it at any time.

- 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 synchronization procedure, which fulfils the following requirements:

- The alarm information provided by means of the synchronization 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 synchronization-alarm information to the correspondent requests, if several synchronization 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 recognize unambiguously the end and the successful completion of the synchronization.

- 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 synchronization 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 synchronization procedure new ("real-time") alarms may be sent at any time to the managing NM.

- If the EM loses confidence to its alarm list and rebuilds it, then the EM shall indicate to the NM that the alarm list have been rebuilt. If the rebuild of the alarm list only concerns alarms for e.g. one NE then the EM may indicate that it is only that part of the alarm list that has been rebuilt. In the latter case the NM may use the knowledge that only a specific subset of the alarm list has been rebuilt to perform a partial resynchronization using filters.

If applicable, an alarm synchronization 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. 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.

The alarm history information should be returned by files when IRPAgent finished collecting all the alarm history information that NM requested.

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 OSs often gives the operator(s) a possibility to add a comment to an alarm. An OS can have the capability to record more than one comment for each alarm. To make the same alarm look the same in all OSs subscribing to the alarm, it should be possible to distribute the recorded comments in the same way as for the acknowledgement information.

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 synchronization procedure for retrieval of current alarm information on NM request may be extended. Additionally to the requirements defined in clause 5.3.1, this extended synchronization 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 Itf-N is built up by a number of IRPs. The basic structure of the IRPs is defined in 3GPP TS 32.101 [2] and 3GPP TS 32.102 [3].

For the purpose of FM, the following IRPs are needed:

- Alarm IRP, see 3GPP TS 32.111-2 [13];
- Notification IRP, see [21]; and
- Notification Log (NL) IRP, see [22].

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

Annex A (informative): General principles of alarm generation

This annex, as additional guidelines to subclause 4.1.2, lists and explains some general principles of alarm generation.

The definition of 'alarm' can be found in subclause 3.1.

- Alarm should convey the identified management entity information to operator

  For the faults of cell, carrier, channel, port, etc., if these faults need operator action, alarms need to be generated. Alarm location information should be accurate enough to identify the units which can be repaired or replaced by the maintenance staff.

- No alarms for those faults that occurred once and then disappeared

  Faults that have occurred only once and then disappeared should not be reported as alarms, because these faults need no operator action. For example, for single call establishment failure, single handover failure or single call drop alarms are not needed since these faults usually only occur once and will not last permanently. Instead these events should be captured by performance measuement counters.

- No alarms for those faults that were self-healed

  For the faults that cannot be perceived by operator, for example some internal software faults like stack overflow, loss of messages, insufficient memory, etc., no alarms are needed if these faults were fixed by network entity's self-healing actions such as software restart, since these faults need no operator action. However, as the service usually is negatively impacted by these faults before they are self-healed, these faults should be recorded into the related logs.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Mar 2000	SA_07	SP-000013	--	--	32.111 Approved at TSG SA#7 and placed under Change Control	2.0.0	3.0.0
Mar 2000	--	--	--	--	cosmetic	3.0.0	3.0.1
Jun 2000	SA_08	SP-000247	001	--	Split of TS 32.111 - Part 1: Main part of spec – Requirements	3.0.1	3.1.0
Jun 2000	SA_08	SP-000248	002	--	Split of TS 32.111- Part 1: Merged Clause X into Clause 4	3.0.1	3.1.0
Jun 2000	SA_08	SP-000249	003	--	Split of TS 32.111 - Part 1: Alignment of FM requirements with IRP, etc	3.0.1	3.1.0
Sep 2000	SA_09	SP-000437	001	--	Clarification On Mediation Function Algorithms	3.1.0	3.2.0
Sep 2000	SA_09	SP-000437	002	--	Clarification On Clear Alarm Suppression	3.1.0	3.2.0
Jun 2001	SA_12	SP-010282	003	--	Added two new features 'partial resynchronization' or 'Itf-N distribution of comments associated to faults'.	3.2.0	4.0.0
Mar 2002	SA_15	--	--	--	Automatic upgrade to Rel-5 (no Rel-5 CR)	4.0.0	5.0.0
Sep 2002	SA_17	SP-020477	004	--	Add requirements for new clearAlarms() operation in Alarm IRP	5.0.0	5.1.0
Dec 2002	--	--	--	--	Updated references & cosmetics	5.1.0	5.1.1
Dec 2003	SA_22	SP-030631	005	--	Add retrieval of alarm history information requirement	5.1.1	6.0.0
Jun 2005	--	--	--	--	Foreword, Introduction update : added 32.111-5 new TS-family member	6.0.0	6.0.1
Jun 2007	SA_36	--	--	--	Automatic upgrade to Rel-7 (no CR) at freeze of Rel-7. Deleted reference to CMIP SS, discontinued from R7 onwards. Cleaned-up references.	6.0.1	7.0.0
Mar 2009	SA_43	SP-090207	006	--	Include reference to SOAP Solution Set specification	7.0.0	8.0.0
Dec 2009	SA_46	--	--	--	Upgrade to Rel-9	8.0.0	9.0.0
Mar 2011	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
Sep 2011	SA_53	SP-110534	007	-	Add concepts for Alarm Correlation and Root Cause Analysis	10.0.0	10.1.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.1.0	**11.0.0**
2013-06	SA_60	SP-130272	008	1	Addition of criteria for critical and major alarms (compliance Top OPE)	11.0.0	**12.0.0**
			010	1	Addition of requirements on repair actions (compliance Top OPE)		
2014-12	SA_66	SP-140801	011	1	Alarm quality improvements, new definitions and concepts for alarm handling	12.0.0	**12.1.0**
2015-03	SA_67	SP-150060	016	1	Replacement of obsolete term “N interface”	12.1.0	**12.2.0**
2016-01					Update to Rel-13(MCC)	12.2.0	**13.0.0**

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	SA#75					Promotion to Release 14 without technical change	14.0.0
2018-06	-	-	-	-	-	Update to Rel-15 version (MCC)	**15.0.0**
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	**16.0.0**
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	**17.0.0**

History

Document history		
V17.0.0	April 2022	Publication