Technical Specification Group SA #6
Nice, France, 15 - 17 December 1999

TSGSA#6(99)598

Source: SA5

Presentation of Specification to TSG SA

Presentation to:	TSG SA Meeting #6
Document for presentation:	3G TS 32.111 V1.1.0 *3G Fault Management*
Presented for:	information

Abstract of document:

This document specifies the overall requirements for 3G Fault Management as it applies to the NE, EM and NM. The first part of the specification defines the fault management 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.

It also describes the specific aspects of the Fault Management for the UTRAN and the CN, respectively, with particular emphasis on the exact fault definitions and alarm information to be generated, the definition of the test procedures and the relationship with the UTRAN resp. CN management architecture as defined in [3].

Finally, 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.

Changes since last presentation to TSG-SA Meeting # 5

- Alarm management;
- Fault management capability requirements over N-interface

Outstanding Issues:

See list of outstanding R99 issues on the following page

Contentious Issues:

none identified

Release 1999 Submission form

Work Area / Item:	32.111 "3G Fault Management"			
Affects:	**UE/MS:**	**CN:**	**UTRAN:**	**Compatibility Issues: Yes: No:**
Expected Completion Date:	June 2000 for the R99 issues mentioned below			
Services impacted:				
Specifications affected:				
Tasks within work which are not complete:	1. Complete the discussion and agreement of all existing contributions with a target to provide the body of TS 32.111 (without appendices) 2. The body of the document will contain the FM concepts and requirements that apply to all the TM interfaces, and the specific requirements that apply to the Itf-N interface. 3. IRP Alarm Information Service 4. CORBA Alarm Solution Set 5. CMIP Alarm Solution Set 6. Review some IRP framework issues; 7. Clarification of management capability requirements over N-interface; 8. IRP alarm information service; 9. Solution sets for notification IRP.			
Consequences if not included in Release 1999:				
Accepted by TSG: SA #6 for late inclusion in Release 1999:				

3G TS 32.111 V1.1.0 (1999-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Fault Management
(3G TS 32.111 version 1.1.0)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Reference

3TS/TSGS-0532111U

Keywords

Fault Management, Alarms

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 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 this TS, 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 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 specification.

Introduction

This Technical Specification (TS) 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 and 3G TS 32.102.

A 3G system is composed of a multitude of network elements (NE) of various types and, typically, different vendors which interoperate in a co-ordinated manner in order to satisfy the network users' communication requirements. The occurrence of failures in a network element 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 NE. In order to minimise the effects of such failures on the quality of service 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 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 encompasses all of the above functionalities except commissioning/decommissioning of NEs and potential operator triggered reconfiguration (these are a matter of Configuration Management, cf. [1]). It also includes associated features in the 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 as it applies to the NE, EM and NM.

Sections 4 and 5 define the fault management 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 to be specified in this part of the 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 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 OMC as a consequence of faults will not be subject of this document, these are described in [1].

Clauses 6 and 7 of this document describe specific aspects of the Fault Management for the UTRAN and the CN, respectively, with particular emphasis on the exact fault definitions and alarm information to be generated, the definition of the test procedures and the relationship with the UTRAN resp. CN management architecture as defined in [3].

Finally, Clause 8 of this TS 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

editor' note: to be updated/ completed (e.g. RFCs for FTP etc.)

[1] 3G TS 32.106 "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 32.106 "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] ISO 8571: "File Transfer, Access and Management".

3 Definitions and abbreviations

3.1 Definitions

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

Alarm: an alarm is a specific → event category used to categorise an event as a fault.

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

Event: this is a generic term for the occurrence of a specific condition within a managed element. A → notification or event report may be used to inform an OS about the occurrence of the event.

Fault: a deviation of a system from normal operation. This deviation may result in the loss of the specified operational capabilities of the element or the loss of redundancy in case of a redundant configuration.

Initial alarm: an → alarm where the severity is set to any value except "cleared".

Notification: information emitted from an NE to an OS or from one OS to another OS on a higher management level. It is used to inform the recipient about the occurrence of an → event. More specifically, an → alarm notification may be used to inform the recipient about the occurrence of a → fault. In OSI terms, the sender of a notification is referred to as the agent, while the recipient is termed the manager.

Permanent fault: a permanent fault is characterised by well-defined conditions for the declaration of its presence or absence, i.e. fault occurrence and fault clearing conditions. This implies that the fault can be both detected and cleared automatically by the fault management functions of the NEs.

Transient fault: a transient fault is characterised by a defined condition for the declaration of the fault, but no clearing condition exists. This implies that the fault can be detected but not cleared automatically by the fault management functions of the NEs.

Editor's note: to be completed

3.2 Abbreviations

For the purposes of this TS, the following abbreviations apply:

Editor' note: these must be updated/completed

CCITT	The International Telegraph and Telephone Consultative Committee
CM	Configuration Management
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FTAM	File Transfer Access and Management
FTP	File Transfer Protocol
HLR	Home Location Register
ISO	International Standards Organisation
MMI	Man-Machine Interface
MML	Man-Machine Language
MOC	Managed Object Class
MOI	Managed Object Instance
MS	Mobile Station
MSC	Mobile Services Switching Centre
NE	Network Element
NMC	Network Management Centre

Editor's note: this term is used for OSs on the network management level, pending the definition of terminology in [2] and [3]

OA&M	Operation, Administration and Maintenance
OMC	Operation and Maintenance Centre

Editor's note: this term is used for OSs on the network element management level, pending the definition of terminology in [2] and [3]

OS	Operations System
OSI	Open System Interconnection
O&M	Operations and Maintenance
QoS	Quality of Service
RNC	Radio Network Controller
TFTP	Trivial File Transfer Protocol
TMN	Telecommunications Management Network
TS	Technical Specification
VLR	Visitors Location Register

4 Fault Management concept

Any evaluation of the network elements' and the overall network health status will require the detection of faults in the network and, consequently, the notification of alarms to the OS (OMC and/or NMC). 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 pending alarms in the network and operational state information as well as alarm/state history data shall be made available to the system operator for further analysis. Additionally, test procedures are required in order to obtain more detailed information if necessary, or to verify an alarm or state or the proper operation of NEs and its logical and physical resources.

The following subsections explain the detection and NE internal handling of faults, alarms and states and the execution of tests.

4.1 Faults, alarms and states

Faults that may occur in the network can be grouped into one of the four 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; or,
- loss of some or all of the NE's specified capability due to overload situations.

Each occurrence of a fault shall be detected by the affected NE(s) using autonomous self-check procedures or by the observation of thresholds. In any case, as a consequence of the fault, appropriate alarms and, possibly, associated state changes, related to the physical or logical resource affected by the fault, shall be generated by the NE.

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

4.1.1 Fault detection

Any deviation from the specified behaviour of a NE, including but not limited to

- failures of physical or logical resources,
- loss of capability due to overload,
- unavailability of some or all of the NE's functionality, and
- disruption or loss of traffic or signalling connections to other NEs

shall be detected by the affected NEs. The NEs accomplish this task using autonomous self-check mechanisms or measurements for the observation of 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 OMC, cf. [4]. The fault detection mechanism as defined above shall include both active and standby components of the NEs.

The majority of the faults will 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 this TS as a permanent fault. The NEs shall recognise when a previously detected permanent 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. Manual intervention by the system operator, either locally or at the OMC, may be necessary for the NE to declare the clearing of a permanent fault, e.g. re-initialisation of equipment after replacing a faulty device.

For some faults, no clearing condition exists. For the purpose of this TS, these faults shall be referred to as transient faults. An example of this is when the NE has to restart a software process due to some inconsistencies, and normal operation can be resumed afterwards. Manual intervention by the system operator will always be necessary for the NE to clear transient faults since these, by definition, cannot be cleared by the NE itself.

For each fault, the following information shall be supplied by the fault detection process:

- for hardware faults, the smallest replaceable unit that caused the fault;
- for software faults, the corrupted file(s) or data bases;
- 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, whether the specified operational capability of the resource was reduced due to the fault;

- the nature of the fault, i.e. transient or permanent;
- any other information that will help understanding the cause of the abnormal situation (system/implementation specific).

Each new fault shall be entered into an internal list of pending faults by the NE. Each fault that is cleared shall be removed from the pending faults list. Note that the pending faults list is only a notion for the purpose of describing the fault management concept specified in this TS, and does not constitute a requirement. An implementation of the pending faults list may be used by the NE for internal housekeeping, however, it is not required to be visible outside of the NE, i.e. to the system operator. Instances of faults shall only be visible to the system operator by virtue of associated alarms and state changes, see following subsections for details.

4.1.2 Generation of alarms

For each fault that enters the pending faults list, appropriate alarms shall be generated by the NE, regardless of whether it is a transient or permanent fault. Such alarms shall contain the following information:

- the device/resource/file/functionality/smallest replaceable unit as defined in subsection 4.1.1 above;
- a description of the loss of capability of the affected resource, if applicable;
- the type of the alarm (communication, environmental, equipment, processing error, quality of service) according to [9];
- the severity of the alarm (indeterminate, warning, minor, major, critical), as defined in [9];
- the probable cause of the alarm;
- whether or not the alarm can be cleared by the network element, i.e. whether it is associated with a permanent or a transient fault;
- the time at which the alarm was generated in the NE; and
- any other information that will help understanding the problem (system/implementation specific).

For certain faults, additional manual procedures may be necessary in order to obtain the required level of alarm detail. For that case, appropriate test/diagnosis routines shall be available in the system (cf. sections 4.2, 6 and 7).

More than one alarm may be generated by an NE as a consequence of a fault, since a single fault may create problems in more than one physical or logical resource within the network element. 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. The system shall, as far as applicable, indicate all effects of the fault by an appropriate number of hardware/software/function/load related alarms, and an indication of the correlation between these alarms (i.e. they are all caused by the same fault) shall be included in each of the alarms. On the other hand, only the number of alarms necessary to notify the system operator of all effects of the fault on physical and/or logical resources shall be generated, in order to avoid excessive numbers of alarms.

All alarms generated by the NE shall be input into a list of pending alarms. The NE shall keep track of the relationship between alarms and faults, similarly as described above for the correlated alarms.

NOTE: the concept described above will, in principle, also apply if a system does not distinguish between alarms and faults. In that case, the relationship between faults and alarms is always 1:1, i.e. no correlation information is required.

4.1.3 Clearing of alarms

Various methods exist for the system to clear alarms, and the faults that triggered them, from the pending alarms list and the pending faults list. 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 will clear the fault(s). Consequently, all related alarms will be cleared by the NE.

- The system operator implicitly requests the clearing of one or more alarms by initialising a new device that replaces a faulty one. Once the new device has been successfully put into service, the NE will clear the alarm(s). Consequently, once all related alarms have been cleared, the NE will clear the associated fault.

- The system operator explicitly requests the clearing of one or more alarms. Once all alarms related to the same fault have been cleared, the NE will clear the associated fault.

- 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 will clear the fault. Consequently, all related alarms will be cleared by the NE.

- 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 will clear all related alarm(s). Consequently, once all alarms have been cleared, the NE will clear the associated fault.

- The NE detects that a previously reported threshold crossed alarm is no longer valid. It will then clear the corresponding initial 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 is implementation specific and depends on the definition of the threshold measurement, see also subsection 4.1.1.

- Transient 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 transient alarms from the pending alarms list. Once all alarms related to the same fault have been cleared, the NE will clear the associated transient fault.

- .... ffs

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 subsection 4.1.2, except that its severity is set to "cleared". The relationship between the clear alarm and the initial alarm is established

- by re-using a set of parameters that uniquely identify the initial alarm (cf. subsection 4.1.2), or

- by including a pointer to the initial alarm in the clear alarm.

The clear alarm shall result in the deletion of the corresponding initial alarm from the pending alarms list. When all alarms corresponding to a fault are cleared, then this fault shall be cleared as well, which results in its removal from the pending faults list, cf. subsection 4.1.1.

4.1.4 Generation of state change events

At any given point in time, NEs and their components (hardware/software) will be either in service, which means they operate at their full specified capability or some fraction thereof, or out of service, which means none of the specified capabilities are available. The reason for a NE/component to change its availability for service may be administrative commands (i.e. triggered by the system operator) or the occurrence resp. elimination of a malfunction, i.e. in conjunction with alarms. In the latter case, the behaviour of the NE/component can be described in terms of the operational state, as defined in [8]. The value of the operational state is defined as "disabled" if the NE/component is completely out of order, and "enabled" otherwise.

For each device/resource/functionality or other component (including the complete NE) that has an operational state defined, any change to the operational state shall be recorded in the NE. Such state change records shall contain the following information:

- the device/resource/functionality whose state changed;

- the new value of the operational state;

- the reason why the state change occurred:

  - ▪ due to one or more (cleared) alarms, and, if yes, an indication of the correlated alarms;

  - because of dependency on some other resource(s) that went out of or back into service, and, if yes, an indication of the state change events of the other resource(s);

Editor's note: should the state change events of the other resource(s) be indicated or just the other resource(s)?

- the time at which the state change was detected in the NE; and,
- any other information that will help understanding the cause of the problem (system/implementation specific).

4.1.5 Storage of alarms and states in the NE

For fault management purposes, each NE will have to store and retain the following information:

- a list of all pending alarms generated as a result of the pending faults, i.e. all alarms currently contained in the pending alarms list;
- alarm history information, i.e. occurrence of new alarms and clearing of alarms that are no longer pending (introduction into/removal from the pending alarms list);
- the values of the operational state for all its components (hardware/software/functional) that have an operational state defined; and,
- state change history, i.e. history of changes of the operational state values as defined above.

The storage space for alarm and state change history in the NE will be 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. The NEs shall be capable of storing at least three days worth of alarm and state change history.

4.1.6 Fault Recovery

Once a fault has been detected, the affected NE shall be capable of recovering from the malfunction. This entails that the NE's normal operation shall be maintained to the highest level possible, i.e. operation according to its specified behaviour shall only be reduced by the capability that was lost because of the fault. In order to achieve this, the NE shall perform the following functions:

- isolate the fault by putting faulty devices/resources/functions out of service, i.e. allowing no side effect of the fault;
- minimise the effect of the fault by automatic reconfiguration. Some examples of this are:
  - ffs
- automatic change over to redundant equipment, if equipped/configured.

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.

Upon elimination of the fault, the NE shall automatically return to its initial configuration. Manual intervention may be necessary to support this feature, e.g. initialisation of repaired equipment to kick off the automatic return to initial configuration. It shall be possible to verify the proper operation of the repaired device/resource/function prior to putting it back into service.

4.2 Tests

ffs

5 Fault management requirements

This section defines the FM requirements from the OS's perspective. According to the concept described in section 4, alarm and state change information shall be maintained by the NEs. This information shall then be forwarded to one or more OS(s), i.e. the OMC and/or NMC. The OMC's role to play in this environment depends on implementation options chosen by the vendor and the network operator.

- the NMC interface (cf. section 8) may be implemented in the NEs or the OMC. This means that the OMC may not be involved in the forwarding of alarm and state information to the NMC, if the NMC interface is implemented in the NE. In contrast, the OMC may have to act as a mediation device if the interface to the NMC is implemented in the OMC and the interface between OMC and the NEs uses a different (proprietary) technology.

- the network operator may choose to operate his network, in terms of FM, mainly from the NMC. This implies that functions for the forwarding and retrieval of alarms and states as well as the processing and user interface presentation of this information may not be required in the OMC, but the NMC. As a consequence, all of these functions, as described in the following subsections, are optional in the OMC, which means they may or may not be implemented, but if implemented, they shall comply with this TS. Details of these considerations are a matter of vendor/operator agreement.

5.1 Alarm and state management

5.1.1 Alarm/state change forwarding and filtering

Alarm and state change events shall be forwarded by the NE, in the form of unsolicited notifications, according to the following scheme:

- as soon as an alarm is entered into or removed from the pending alarms list;

- immediately when an operational state change event is recorded in the NE.

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.

If the NMC interface is implemented in the NE, then the destination of the notifications is the NMC, and the interface shall comply with the stipulations made in section 8. If the NMC interface resides in the OMC, proprietary means may be employed to forward the notifications to the OMC. Note that, even if the NMC interface is implemented in the NE, the OMC may still also receive the notifications by one of the above mechanisms, however, this TS does not explicitly require the NEs to support the OMC as a second destination.

The event report shall include all information defined for the respective event (cf. subsections 4.1.2, 4.1.3 and 4.1.4), plus an identification of the NE that generated the report. This NE identification shall be identical to the identifiers defined within the CM domain, see [1].

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

- the NE that generated the alarm, i.e. all alarm messages of that NE will 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 same functionality and criteria, as far as applicable, shall also be available for state changes, as follows:

- the NE that generated the state change event, i.e. all state change messages of that NE will be suppressed;
- the device/resource/function to which the state change relates;
- the time at which the state change occurred; 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.

5.1.2 Retrieval of alarm and state information

The NEs shall offer a facility for an OS to retrieve alarm and operational state information stored in the NE (cf. subsection 4.1.5). If the interface to the NMC is implemented in the NEs, then this facility shall be implemented according to the stipulations given in section 8. If the NMC interface resides in the OMC, then proprietary means may be employed on the NE-OMC interface, however, a bulk data retrieval based on existing protocols, such as FTP, TFTP, or FTAM, is anticipated. Note that either of the two above mechanisms may still be used by the OMC even if the NMC interface resides in the NEs.

The alarm retrieval facility shall entail the following features:

- read alarms from the alarm history;
- read state changes from the state change history;
- retrieve the pending alarms from the NE; and,
- read current values of the operational state.

It shall be possible to apply filters to each of the above operations as defined in subsection 5.1.1, plus the "cleared" alarm severity level.

5.1.3 Support of Maintenance Action

In order to facilitate maintenance of the network, the system shall support the following OMC commands:

- request isolation of device for maintenance. Ongoing calls shall be allowed to be terminated by the users.
- request clearing of calls for maintenance. This will isolate the device addressed by the command, and ongoing calls using the device will be cleared.
- clear device from control channels (NodeB - per channel, per carrier, per cell). It shall be possible to specify an alternate device to take over the channel(s), otherwise automatic reconfiguration shall be performed.
- establish priorities for automatic reconfiguration. This will force the NE's automatic reconfiguration after a fault to follow a scheme predefined by the system operator.

The NE shall confirm the result of the command to the requesting system operator.

5.1.4 Configuration of Alarms

It shall be possible to configure the alarm actions, thresholds and severities through OMC commands, according to the following requirements:

- upon detection of a fault, certain actions will be carried out by the NE, e.g. putting the defective device/resource/function out of service. It shall be possible to change these activities for each individual fault.

- 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, in the NE, the severity of each alarm defined in the system, e.g. from major to critical.

The NE shall confirm the result of any such alarm configuration command to the requesting system operator.

5.1.5 Communication failure

If forwarding of alarms or state change events by an NE is not possible due to communication breakdown, then the notifications shall be sent as soon as the communication capability has been restored. The recipient of the notifications, i.e. the OMC and/or NMC, shall notice the communication failure and generate appropriate internal alarms in order to alert the system operator of the problem.

5.2 Test management

ffs

6 UTRAN aspects

ffs

7 CN aspects

ffs

8 N interface

8.1 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.

As pointed out in chapter 5, the N interface (Itf-N) may connect the network management system either to EMs or directly to the NEs. In the following, the term "subordinate entities" defines either EMs or NEs , which are in charge of supporting the N interface.

This chapter describes the properties of an interface enabling an 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 [1]). This is, however, not part of the FM functionality.

Therefore, for the purpose of fault management the subordinate entities send notifications to an 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.

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 must be able to initiate the communication.

8.2 Management of alarm and state change event reports

8.2.1 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 as follows:

- *managedObjectClass* It defines the object class according to the information model of the Itf-N.
- *managedObjectInstance* It defines the object instance, which models on the Itf-N the network resource generating the alarm / state change report.
- *eventType* It identifies the type of the event (e.g. different alarm type in accordance with ISO/IEC 10165-2 / X.721).
- *eventTime* It defines the time of generation of the event.
- *probableCause*: This parameter defines further qualification as to the probable cause of the alarm.
- *specificProblems*: It may contain detailed manufacturer-specific 3G systems information related to the alarm cause.
- *perceivedSeverity*: This parameter defines severity levels, which provide an indication of how it is perceived that the capability of the managed object has been affected.
- *trendIndication*: This parameter, when present, specifies the current severity trend of the managed object.
- *thresholdInfo*: This parameter shall be present when the alarm is a result of crossing a threshold.
- *notificationIdentifier*: It is a value generated by the mediation function, which unambiguously identifies (in the context of a specific Itf-N) an alarm / state change report.

- *correlatedNotification*: It is an unambiguous value generated by the mediation function for the correlation between alarm and/or state change reports (e.g. in an alarm report with perceived severity "cleared to indicate the clearing of those alarms whose notification identifiers are included in this parameter).

- *proposedRepairActions*: It may contain detailed manufacturer-specific 3G systems information related to the alarm cause.

- *additionalText*: It may contain detailed manufacturer-specific 3G systems information related to the original alarm / state change report.

- *additionalInformation*: It may contain detailed manufacturer-specific 3G systems information related to the original alarm / state change report.

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 correspondent ("equivalent") functional object at the Itf-N. If the functional object generating the original alarm notification has not a direct correspondent 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 correspondent ("equivalent") functional object at the Itf-N. If the functional object generating the original state change notification has not a direct correspondent 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 correspondent equipment-related resource. If present, the parameters *specificProblems, proposedRepairActions*, *additionalText* and *additionalInformation* shall contain the detailed (manufacturer-specific) information needed on NM level for maintenance purposes.

Note

In some cases a failure or the locking of an equipment-related object implies also the change of the operational state of its correspondent functional object within the NE or EM (if EM is available). The mapping of this state change notification to an alarm of the correspondent functional object at the Itf-N is subject of further study.

On the Itf-N the correlation between functional related and the generic logical objects (modeling equipment-related network resources) is performed explicitly by means of a relationship attribute in the functional object class definition.

With regard to the multi-vendor capability of the Itf-N, this mapping concept combines the following requirements:

- Precise information about manufacturer-specific, equipment-related failures for the NM operator in charge of network maintenance (this information is provided in some parameters of alarm reports mapped to the generic logical objects)

- If functionality is affected, an additional alarm report concerning the related functional object is provided for the NM operator in charge of network's quality of service.

The two types of alarm reports generated by the mediation function are correlated by means of the parameters *notificationIdentifier* and *correlatedNotifications* respectively.

8.2.2 Real-time forwarding of event reports

If the Itf-N is in normal operation (the NM connection to the subordinate entities is up), alarm and related state change event 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 must have an own filter within every subordinate entity which may generate notifications.

The semantics of alarm and state change reports forwarded to the NM are in accordance with [7], [8] and [9] respectively.

At the Itf-N the optional parameters *specific problems*, *proposedRepairActions*, *additionalText* and *additionalInformation* may be used to forward manufacturer-specific information to the NM.

8.2.3 Alarm clearing

Via Itf-N, an alarm report containing the value "cleared" of the parameter *perceivedSeverity* indicates the clearing of those previous alarm reports whose *notification Identifier*s are included in the *correlatedNotifications* attribute.

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.

8.3 Retrieval of alarm and state information

The retrieval of alarm and state information comprises two aspects:

a) Retrieval of current information

This mechanism shall ensure data consistency about the current alarm / state change 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 / state change information stored within the subordinate entities for later evaluation.

8.3.1 Retrieval of current alarm information on NM request

This specification 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.

  Note: This requirement is for further investigation.

- 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.

This requirement is for further investigation.

8.3.2 Retrieval of current state change information on NM request

The requirements defined above for the alarm synchronisation procedure are valid analogously for the retrieval of current state change information as well.

Nevertheless the state change synchronisation procedure takes into account only the object instances whose state information is different from a combined default state. As combined default state the following values (according to ITU-T X.721) shall be used:

- Operational state: enabled
- Administrative state: unlocked
- Usage state: idle.

8.3.3 Logging and retrieval of alarm and state change history information on NM request

The alarm / state change history information may be stored in the subordinate entities in dependence on the NM requirements. The NM is able to create logs for alarms / state change event reports and to define the criteria for storage of alarm / state change information according to [11].

The subsequent retrieval of stored information is possible on NM request in two different ways:

- via a read command with appropriate filtering
- via bulk data transfer, using standardised file transfer procedures, as mentioned in chapter 5.1.2.

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

8.4 Co-operative alarm acknowledgement on the Itf-N

In case the Itf-N connects the NM with EMs, the fault management and - as consequence - also the acknowledgement of alarms may take place on both management layers, depending on the operational concept.
A co-operative alarm acknowledgement means that the acknowledgement performed on one network management level is notified to all the partner OS on the other management layer, thus the acknowledgement-related status of this alarm is the same within the whole management hierarchy. In case of multiple NMs, if the acknowledgement takes place on one NM, the EM informs all other NMs.

In case the co-operative alarm acknowledgement is supported, the 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. This information consists of the *notificationIdentifier* value of a previous active alarm.
  - *Acknowledgement history* data, including the current alarm state (active | cleared), the time of alarm acknowledgement, the management system (EM | NM) and optionally the operator in charge of acknowledgement (the parameter operator name or, in case of auto-acknowledgement, a generic system name).
  - *Possible filtering criteria*, as optional information to be used only in the acknowledgement messages sent by the EM towards the NM, in order to discriminate also the acknowledgement message, if the related alarm report is filtered out by NM-related discriminator in EM). As filter criteria the perceived severity, probable cause and specific problems shall be supported.

- The alarm acknowledgement procedure on the Itf-N must cope with different customer requirements concerning the acknowledgement competence between operators working at EMs and NM. This matter may be managed by means of a "competence type" information, which may be controlled by every connected EM.
  Every time the communication between the two management systems is established, the NM is able to get the "competence type" information and to handle accordingly the alarm acknowledgement. A specific value of the "competence type" information allows the acknowledgement of alarms according to the individual authorisation profiles.

- 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 chapter 8.3.1, this extended synchronisation procedure relates not only to the active, but also to the "cleared and not acknowledged" alarms, which have to be still managed by the EM.

History

Document history		
0.0.1	01/09/99	Initial draft
1.0.0	10/10/99	Submitted to TSG-SA #5 (11-13 October, 1999) for information. Identical to v0.0.1
1.0.1	10/12/99	Includes changes agreed in SA5 meetings #6, #7, #8(partial) and FM ad-hoc meeting
1.1.0	14/12/99	Submitted to TSG-SA #6 (15 - 17 December, 1999) for information