Technical Specification Group Services and System Aspects
Meeting #8, Düsseldorf, Germany, 26-28 June 2000

TSGS#8(00)0248

Source: **SA5 (Telecom Management)**

Title: **32.111 CR, "Split of TS - Part 1: Main part of spec – Merge Clause X into Clause 4" (S5-000329)**

Document for: **Approval**

Agenda Item: **6.5.3**

SA5 has split TS 32.111 into a multi-part TS as identified below:

Part 1: **"3G Fault Management Requirements";**

Part 2: "Alarm Integration Reference Point: Information Service";
Part 3: "Alarm Integration Reference Point: CORBA Solution Set";
Part 4: "Alarm Integration Reference Point: CMIP Solution Set".

Six (6) CRs are submitted to SA#8 for approval; the present one is highlighted in yellow:

Spec	CR	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
32.111	001	R99	Split of TS - Part 1: Main part of spec – Requirements	F	3.0.1	3.1.0	S5-000328
32.111	002	R99	Split of TS - Part 1: Main part of spec - Merging of Clause X into Clause 4, etc.	F	3.0.1	3.1.0	S5-000329
32.111	003	R99	Split of TS - Part 1: Main part of spec – Alignment of FM requirements with IRP, etc.	F	3.0.1	3.1.0	S5-000331
32.111	004	R99	Split of TS - Part 2: Alarm IRP Information Service (IS)	F	3.0.1	3.1.0	S5-000332
32.111	005	R99	Split of TS - Part 3: Alarm IRP CORBA Solution Set (SS)	F	3.0.1	3.1.0	S5-000333
32.111	006	R99	Split of TS - Part 4: Alarm IRP CMIP Solution Set (SS)	F	3.0.1	3.1.0	S5-000334

Scope

This TS 32.111-1 ~~The present document~~ specifies the overall requirements for 3G Fault Management as it applies to the NE, EM and NM.

Clauses 4 ~~and 5~~ 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. 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~~ EM as a consequence of faults will not be subject of the present document, these are described in [1].

~~Clauses 6 and 7 of the present 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~~5 of the present document defines the functional requirements for the standard Itf-N, for the purpose of Fault Management of 3G networks, as seen from the Network Manager (NM). The Itf-N is fully standardised so as to connect systems of any vendor to the NM via this interface.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

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

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

[4] 3G TS 32.104~~6~~: "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".

[13] TS 32.111-2 Alarm Integration Reference Point: Information Service

[14] TS 32.111-3 Alarm Integration Reference Point: CORBA Solution Set

[15] TS 32.111-4 Alarm Integration Reference Point: CMIP Solution Set

3 Definitions and abbreviations

3.1 Definitions

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

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

ADAC Faults = faults that are “Automatically Detected and Automatically Cleared” by the system when they occur and when they are repaired

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

Alarm: an alarm is an abnormal network entity condition which categorises an event as a fault

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

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

Event: this is a generic term for any type of occurrence within a network entity. A notification or event report may be used to inform one or more OS(s) about the occurrence of the event

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

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

~~**Steady fault:** a steady 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 network entity~~

~~**Unsteady fault:** an unsteady 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 network entity~~

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
CCITT	The International Telegraph and Telephone Consultative Committee
~~CM~~	~~Configuration Management~~
CMIP	Common Management Information Protocol
~~CMIS~~	~~Common Management Information Service~~
~~CMISE~~	~~Common Management Information Service Element~~
~~EIR~~	~~Equipment Identity Register~~
EM	Element Manger
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
NM	Network Manager
~~NMC~~	~~Network Management Centre~~
~~OA&M~~	~~Operation, Administration and Maintenance~~
~~OMC~~	~~Operation and Maintenance Centre~~
OS	Operations System
~~OSI~~	~~Open System Interconnection~~
~~O&M~~	~~Operations and Maintenance~~
QO~~o~~S	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 and requirements

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

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

4.1 Faults and alarms

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

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

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

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

4.1.1 Fault detection

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

The network entities accomplish this task using autonomous self-check circuits/procedures, including, in the case of ~~Nes~~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 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 the present document as a ~~steady~~ ADAC fault. The network entities ~~must~~ should be able to recognise when a previously detected ~~steady~~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 ~~unsteady~~ 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 will always be necessary to clear ~~unsteady~~ 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 an 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, quality of service) according to [9];
- the severity of the fault (indeterminate, warning, minor, major, critical), as defined in [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, i.e. ~~steady~~ ADAC or ~~unsteady~~ADMC;
- any other information that will help understanding the cause and the location of the abnormal situation (system/implementation specific).

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

4.1.2 Generation of alarms

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

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

In case a network entity is not able to recognise that a single fault manifests itself in different ways, the single fault is detected as multiple faults and originates multiple alarms. In this case however, when the fault is repaired the network entity ~~must~~ 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 will detect the fault as described in subclause 4.1.1 and generate its own associated communication alarm toward the managing OS. In this case it is the responsibility of the OS to correlate alarms received from different NEs/OSs and localise the fault in the best possible way.

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

4.1.3 Clearing of alarms

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

- the equipment faults are repaired by replacing the faulty units with working ones;
- the software faults are repaired by means of partial or global system initialisations, by means of software patches or by means of updated software loads;

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

It is also possible that a ~~steady~~ 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 ~~steady~~ 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 ~~unsteady~~ ADMC faults, manual intervention by the operator is always necessary to clear the fault. Practically, various methods exist for the system to detect that a fault has been repaired and clear alarms and the faults that triggered them. For example:

- The system operator implicitly requests the NE to clear a fault, e.g. by initialising a new device that replaces a faulty one. Once the new device has been successfully put into service, the NE will clear the fault(s). Consequently, the NE will clear all related alarms.
- The system operator explicitly requests the clearing of one or more alarms. Once the alarm(s) has/have been cleared, the NE will detect that the fault condition has ceased.
- The NE detects the exchange of a faulty device by a new one and initialises it autonomously. Once the new device has been successfully put into service, the NE will clear the fault(s). Consequently, the NE will clear all related alarms.
- The NE detects that a previously reported threshold crossed alarm is no longer valid. It will 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.
- ~~Unsteady~~ 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 ~~unsteady~~ ADAC alarms/faults in the NE. Once an ~~unsteady~~ ADMC alarm/fault has been cleared, the NE will clear the associated ~~unsteady~~ ADAC fault/alarm.

Details of these mechanisms are system/implementation specific.

Each time an alarm is cleared the NE shall generate an appropriate clear alarm event. A clear alarm is defined as an alarm, as specified in subclause 4.1.2, except that its severity is set to "cleared". The relationship between the clear alarm and the active alarm is established:

- by re-using a set of parameters that uniquely identify the active alarm (cf. subclause 4.1.2); 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 will be limited. The storage capacity will be Operator and implementation dependent. If the number of delayed notifications exceeds the storage space then an alarm synchronisation procedure shall be run when the communication capability has been restored.

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

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

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

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

- the NE that generated the alarm, i.e. all alarm messages for that NE 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 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 purposes, each NE will 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 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. Further "buffer full" behaviours, e.g. those defined in [11], may be implemented as an option. The storage capacity itself, and thus the duration for which the data can be retained, will 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:

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

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

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

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

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

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

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

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

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

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

If the faulty resource has redundancy, the NE shall perform action a), c) and d) above and, in addition, the recovery sequence that is specific to that type of redundancy. Several types of redundancy exist (e.g. hot standby, cold standby, duplex, symmetric/asymmetric, N plus one or N plus K redundancy, etc.), and for each one, there is a specific sequence of actions to be performed in case of failure. The present document specifies the Fault Management aspects of the redundancies, but it does not define the specific recovery sequences of the redundancy types.

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

The detailed definition of the management of the redundancies is out of the scope of this document.~~strictly related to the way they are modelled in the MIM of the NE. For the modelling of the redundancies, the relationships shall be defined among the objects, which participate in each redundancy. This will identify the objects and the roles that they have in the redundancy. By defining the relationships, also the role of the objects participating in the relationships are implicitly defined by the relationships' attribute values.~~

~~The NE shall provide the OS with the capability to monitor and control any redundancy of the NE. The control of a redundancy by the OS (which means the capability to trigger a changeover or a change-back) can be achieved by means of state management, cf. subclause 4.2.~~

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 Support of Maintenance Action~~

4.1.8 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 must have the same severity.

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

4.2 State management

The State Management is a common service defined within Configuration Management (TS 32.106) 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 must be notified to the relative manager(s) as specified in TS 32.106.

When a state change is originated by a failure, the alarm notification and the related state change notifications must 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 must 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) must be checked and, in case they are "enabled" they shall be changed to "disabled". In this process, also the secondary status must 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 must 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 4.3 Test management

~~x Fault management requirements~~

~~This clause defines the FM requirements from the OS's perspective. According to the concept described in clause 4, the NEs shall maintain alarm and state change information. 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. clause 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 subclauses, are optional in the OMC, which means they may or may not be implemented, but if implemented, they shall comply with the present document. Details of these considerations are a matter of vendor/operator agreement.~~

~~x.y Alarm and state management~~

~~x.y.z 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 clause 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, the present document 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. subclauses 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.~~

~~x.y.z 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. subclause 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 clause 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 subclause 5.1.1, plus the "cleared" alarm severity level.~~

~~x.y.z 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 (Node B - 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.~~

~~x.y.z 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.~~

~~x.y.z Communication failure~~

~~If forwarding of alarms or state change events by a 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.~~

3GPP TSG-SA5 (Telecom Management)
Meeting #12, Rome, 5–9 June 2000

SA5#12(00)0329

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

32.111 CR 002 Current Version: 3.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ ↑ *CR number as allocated by MCC support team*

For submission to: SA#8
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG use only)*
for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM □ ME □ UTRAN / Radio ☒ Core Network □
(at least one should be marked with an X)

Source: SA5#12 **Date:** 20 June 2000

Subject: Split of TS - Part 1: Main part of spec – Merge Clause X into Clause 4

Work item: 32.111 3G Fault Management

Category:
(only one category shall be marked with an X)

F	Correction	☒	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change:

The following changes are proposed to be introduced in TS 32.111 Ver 3.0.1

1. Merging on Clause X into Clause 4 (this change was already announced when the previous version was forwarded to SA plenary)

2. Editorial and error corrections.

Clauses affected: Scope, References, Definitions, Abbreviations, 4, 4.1.* (but 4.1.3), 4.2, 4.3, x.y.z,

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	
Other GSM core specifications	□	→ List of CRs:	
MS test specifications	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments: