3GPP TR 32.819 V8.0.0 (2008-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Element management layer - Operation System Function (E-OSF) definition (Release 8)

Keywords
UMTS, GSM, management

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 Report has been produced by the 3rd Generation Partnership Project (3GPP).

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

In the Logical Layered Architecture (LLA) of TMN [1], Network-OSFs (N-OSF) are concerned with the management function on Network Management Level (NML), and Element-OSFs (E-OSF) with the management function on Element Management Level (EML).
These two logical layers respectively play the role of Network Management Function (NMF).

This report provides Element Management Layer (EML) operation system functions and function sets.
The content is associated with the 3GPP TS 32.xyz-series.

1 Scope

The present document identifies and defines the needs in the E-OSFs.
The intention is not to define new requirements for the eventual standardization of new Interface IRP or NRM IRP and/or System Context.

The present document proposes to define the E-OSFs including the following main aspects:

- Define functional scope of Element-OSF (E-OSF)
- Define functional requirement of Elements-OSF (E-OSF)

The present document identifies a set of functions require by operators to operate mobile networks.
By identifying these functional capabilities and then comparing them with the 3GPP IRP capabilities, widely used functions and omissions in the 3GPP set of IRPs are indicated.
Change Requests and new IRPs are expected to be created in order to narrow the functional gap.

2 References

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

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

[1] ITU-T Recommendation M.3010 (2000): "Principles for a Telecommunications management network".

[2] 3GPP TS 32.111-1: "Telecommunication management; Fault Management; Part 1: 3G fault management requirements".

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

[4] ITU-T Recommendation M.3400: "TMN management functions".

3 Abbreviations

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

BML	Business Management Layer
B-OS	Business Management Layer-Operations Systems
B-OSF	Business Management Layer-Operations Systems Function
EML	Element Management Layer
E-OS	Element Management Layer-Operations Systems
E-OSF	Element Management Layer-Operations Systems Function
FM	Fault Management
LLA	Logical Layered Architecture
NE	Network Element
NEF	Network Element Function
NEL	Network Element Layer
NML	Network Management Layer

NMS	Network Management System
N-OS	Network Management Layer-Operations Systems
N-OSF	Network Management Layer-Operations Systems Function
O&M	Operations & Maintenance
OS	Operations System
OSF	Operations Systems Function
SML	Service Management Layer
SMS	Short Message Service
S-OS	Service Management Layer-Operations Systems
S-OSF	Service Management Layer-Operations Systems Function
TMN	Telecommunication Management Network

4 TMN Logical Layered Architecture (LLA)

To deal with the complexity of telecommunications management, the management functionality could be considered to be partitioned into logical layers (see [1]). The LLA is a concept for the structuring of management functionality which organizes the functions into a grouping called "logical layers" and describes the relationship between layers. A logical layer reflects particular aspects of management and implies the clustering of management information supporting that aspect.

The grouping of management functionality implies grouping OSFs into layers. A specialization of OSFs based upon different layers of abstraction is business, service, network and element. Some TMN implementations may include business OSFs that are concerned with a total enterprise (i.e. all services and networks) and carry out overall business coordination. Service OSFs are concerned with services offered by one or more networks and should normally perform a customer interfacing role. Network OSFs are concerned with the management of networks, and Element OSFs with the management of individual elements.

Four (4) specializations of the OS physical block are defined to support a physical realization of function blocks in logical layers:

1. Business-Operations Systems (B-OS),
2. Service-Operations Systems (S-OS)
3. Network-Operations Systems (N-OS)
4. Element-Operations Systems (E-OS).

These physical blocks are named according to the predominant functional block they contain. Specifically, B-OS, S-OS, N-OS and E-OS predominantly contain B-OSF, S-OSF, N-OSF and E-OSF respectively.
When physical blocks contain more than one kind of specialized OS functional block that provide substantial functionality to the physical block, thus spanning more than one logical layer, the physical block is named according to the highest hierarchically layered function block. For example, a physical block containing both N-OSF and E-OSF, providing substantial network functionality is called an N-OS.

5 Functional scope of E-OSF and N-OSF

5.1 Element Management Layer (EML)

The EML manages each Network Element on an individual or group basis and supports an abstraction of the functions provided by the Network Element Layer (NEL).

The EML has one or more element OSFs and/or MFs that are individually responsible, on a devolved basis from the Network Management Layer (NML), for some subset of Network Element Functions (NEF).
As an objective, a vendor independent view should be provided to the NML.

The EML has the following three (3) principle roles:

1) Control and coordination of a subset of Network Elements on an individual NEF basis. In this role, the element OSFs support interaction between the NML and the NEL by processing the management information being exchanged between network OSFs and individual NEFs. Element OSFs should provide full access to NE functionality.

2) The EML might also control and coordinate a subset of Network Elements on collective basis. In this role, element OSFs may also provide a single entity view of a group of NEFs.
In addition, these element OSFs may manage the relationships (e.g. connectivity) between NEFs.

3) Maintaining statistical, log and other data about elements within its scope of control.

OSFs in the EML interact with OSFs in the same or other layers within the same TMN through a q3 reference point and in other TMNs through an x reference point.

Figure 5.1-1 show the reference point related E-OS, q reference point between E-OSF, TF and NEF.f Class between OSF and a WSF.x reference point between E-OSFs and the S-OSF of a TMN or the equivalent.

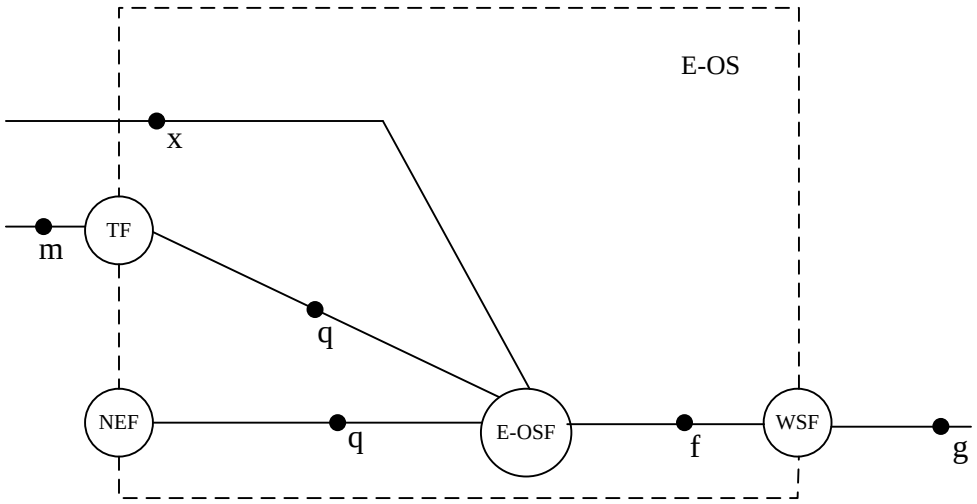


Figure 5.1-1: E-OS reference point

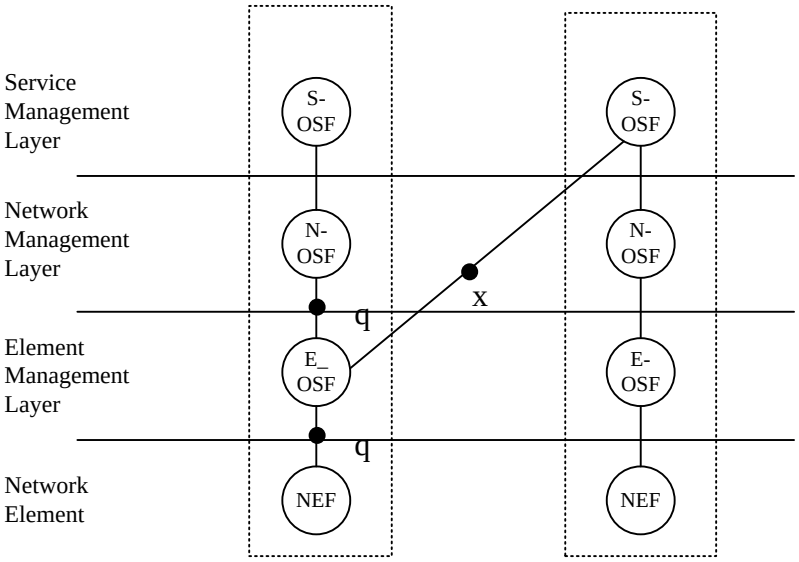
Logical Layered Architecture (LLA) is a concept for the structuring of management functionality which organizes the functions into groups called "logical layers" and describes the relationship between layers.

A logical layer reflects particular aspects of management arranged by different levels of abstraction. Functional interactions between OSF function blocks within different logical layers are described by the reference point.

The EML manages each Network Element on an individual or group basis and supports an abstraction of the functions provided by the Network Element layer. The EML has one or more element OSFs that are individually responsible, on a devolved basis from the NML, for some subset of NEFs.

Interactions between E-OSF and NEF or N-OSF within a TMN take place at the q reference points. And the interactions between E-OSF and S-OSF in the other TMN take place at the x reference.

Figure 5.1-2 shows the case.



NOTE: All mediation functions, including those physically located elsewhere (e.g. in a network element), are logically located in the element management layer.

Figure 5.1-2: E-OSF reference point

5.2 Network Management Layer (NML)

The NML has the responsibility for the management of a network as supported by the EML, includes the management aspects of any management entity which implements E-OSF.

At this layer, functions addressing the management of a wide geographical area are located. Complete visibility of the whole network is typical and, as an objective, a technology independent view should be provided to the SML.

The NML has the following four principal roles:

1) Control and coordination of the network view of all Network Elements within its scope or domain.

2) Provision, cessation or modification of network capabilities for the support of service to customers.

3) Maintenance of network capabilities.

4) Maintaining statistical, log and other data about the network and interact with the SML on performance, usage, availability, etc.

Thus, the NML provides the functionality to manage a network by coordinating activity across the network and supports the "network" demands made by the SML. It knows what resources are available in the network, how these are interrelated and geographically allocated and how the resources can be controlled. It has an overview of the network. Furthermore, this layer is responsible for the technical performance of the actual network and should control the available network capabilities and capacity to give the appropriate accessibility and Quality of Service (QoS).

OSFs in the network management layer interact with OSFs in the same or other layers within the same TMN through a q3 reference point and in other TMNs through an x reference point.

6 Functional requirement of E-OSF

6.1 Fault Management (FM)

According to 3GPP TS 32.111-1 [2], the FM focus on fault detection, isolation and correction of abnormal operation of the telecommunication network and its environment. However, some other function should also be included in E-OSF.

6.1.1 Alarm surveillance function set

6.1.1.1 Overview

E-OSF should support following function set:

- Alarm view function set;
- Alarm status function set;
- Alarm presentation function set;
- Alarm filter function set.

6.1.1.2 Alarm view function set

Management entity that implements E-OSF should provide the following alarm views at least. Any problematic equipment in the network can be detected from the topological view. In addition, any problematic board should be detected from the locating view (optional).

In this view, alarms should be displayed in topological way and O&M operator can browse, analyze and operate on the alarms. It should display summary of alarm information, including the number of alarms, number of alarms with different levels, specific network status and the physical network equipment.

Topological alarm view should support the display of alarms that meet the filtering criteria. The alarms on the topological alarm view should be updated in real-time, so as to reflect the active network status in time.

6.1.1.3 Alarm status function set

Alarms can be divided into current alarm (active alarm) and history alarm. Current alarms refer to the alarms that has not been cleared and which is active until the fault that caused the alarm is corrected and a "clear alarm" is generated. The alarms that have been cleared are called history alarms, which should be saved in history alarm database for future query. History alarm should accurately record "all the alarms that have been reported in real time"

E-OSF should support the following alarm status, which should be associated with 3GPP TS 32.111-2 [3]:

- Unacknowledged active alarm: unacknowledged and not cleared alarms;
- Acknowledged active alarm: acknowledged and not cleared alarms;
- Unacknowledged history alarm: unacknowledged but not cleared alarms;
- Acknowledged history alarm: acknowledged and cleared alarms.

6.1.1.4 Alarm prompt customization function set

E-OSF should support the following way to customize the alarm prompt.- Customization of alarm prompt colourManagement entity that implements E-OSF should display the alarm level in different colour. In addition, the colour of the alarm severity can be customized in specific case.

For example,

1) In the topological map, when multiple alarms happened at the same time in the same NE, only the colour that indicate the highest severity alarms among these alarms on the same NE should be displayed. When highest severity alarms are cleared, colour that indicates the next level severity alarm in the remained alarms should be displayed.

2) In the alarm list, the alarm should be sorted in the order of severity of alarms.

3) Customization of audible alarm

For newly received alarm, management entity that implements E-OSF should generate audible prompt that could be customized by the O&M operator.

6.1.1.5 Alarm filter function set

Management entity that implements E-OSF should support the filtering of alarms submitted by NEs. Those comply with the filtering criteria should not be displayed on the active alarm window, but it should not affect the report and the storage of alarms.

Management entity that implements E-OSF should provide functional modules so that O&M operator can set the filtering criteria and control the alarm presentation. The filtering criteria include but are not limited to the following attribute or combination of attribute:

- Alarm equipment
- Time of the alarm generation
- Type of the alarm
- Level of the alarm
- Possible reason

6.1.1.6 Suppress alarm function set

It should be possible to suppress all alarms from one or more NEs during a specified period. This might be needed when maintenance work is a heavy burden or "re-homing" of an NE. All logging as well as reporting should be suppressed, but the suppressed alarms should be stored. Even though notification is subscribed through Itf-N for one NE, this NE can not send notification to NMS when suppress alarm function is enabled. In the case of no NMS for operators, there is no alarm prompt, but the suppressed alarm must be found in storage.

6.1.2 Fault localization function set

6.1.2.1 Overview

E-OSF should support fault localization function set [4];

Fault localization policy function set:

- Verification of parameters and connectivity function set.
- Network fault localization function set.
- Running of diagnostic function set.

6.1.3 Alarm operation function set

6.1.3.1 Overview

E-OSF should support alarm operation function set:

- Alarm query function set
- Alarm synchronization function set

- Alarm confirmation function set
- Alarm severity change function set

6.1.3.2 Alarm query function set

Management entity that implements E-OSF should support flexible active alarm and history alarm query, but the conditions for the combined query include but not limited to the following:

- Alarm equipment
- Alarm generation time
- Alarm type
- Alarm level
- Possible alarm reason

On the fault management GUI, the detailed alarm information queried can be displayed on the fault management GUI, also exported and printed.

6.1.3.3 Alarm synchronization function set

Management entity which implements E-OSF should support alarm synchronization, including:

1) Automatic synchronization

Management entity that implements E-OSF can automatically synchronize NE alarms, and it is applicable to the following cases:

- When management entity that implements E-OSF is establishing management connection with NE;
- When there is a communication failure between management entity which implements E-OSF and NEs, it is restored;
- When there is an management entity which implements E-OSF failure, it is recovered;
- When active management entity that implements E-OSF is being swapped to backup Management entity which implements E-OSF.

2) Periodical synchronization

Management entity that implements E-OSF can periodically synchronize NE alarms during operation, the synchronization interval can be defined by users.

3) Manual synchronization

Refer to management entity which implements E-OSF support O&M operator to manually synchronize when needed.

6.1.3.4 Alarm acknowledgement function set

Management entity that implements E-OSF should support the alarm acknowledgement, and can record the acknowledgement reason, the time when the acknowledgement happened. Management entity that implements E-OSF should distinguish alarms acknowledgement from alarms un-acknowledgement. Alarm acknowledgement refers to alarm IRP definition.

1) Alarm acknowledgement

The acknowledgement of an alarm is a maintenance function that aids the operators in his day-to-day management activity of his network. The E-OSF should acknowledge an alarm to indicate some activity have been started to resolve this specific problem.

2) Cancel alarm acknowledgement

Management entity that implements E-OSF should support the cancellation of alarms acknowledged. The alarms acknowledged should only be cancelled by user who acknowledges the alarm.

3) Clear alarm

Management entity that implements E-OSF should support to clear alarms, including automatic clear and manual clear.

Automatic clear function means the active alarm should change to history alarm automatically when alarm clear message is received from NE.

Manual clear function means the active alarm should change to clear alarm manually, and which should not affect NEs. If the failure of NE is not recovered, the alarms should be reported in real-time.

For cleared but not acknowledged alarms, management entity that implements E-OSF should mark it in some way to remind operator.

4) History alarm statistics and report generation

Management entity which implements E-OSF should provide history alarm statistics function and can generate and export related report.

5) History alarm storage time

Management entity that implements E-OSF should save the history alarm for some period and delete expired alarms automatically.

6.1.3.5 Alarm severity function set

Management that implement the E-OSF should provide the capability to change the alarm severity for certain alarms and the alarm should be reported or logged with severity updated, severity available has been listed in 3GPP TS 32.111-2 [3]. This function does not affect the original alarm severity within NE.

EXAMPLE: The severity of alarm for some circuit boards is "Warning" predefined by vendors. From an operator's perspective, the possibility that this circuit board in trouble leads to traffic break is greatly increased. Therefore, the operator would decide to change the severity of alarm for these circuit boards from "Warning" to "Major" or "Critical".

6.1.4 Alarm forwarding

6.1.4.1 Overview

Management entity that implements E-OSF should provide external interface that can support alarm forwarding. Alarm forwarding includes the following functions set:

- Alarm EMAIL notification function set
- Alarm SMS notification function set
- Alarm light and voice notification function set
- Alarm smoothing function set

6.1.4.2 Alarm EMAIL notification

Management entity that implements E-OSF should support the email notification function of the alarms. For certain alarms, when the user has confirmed the person to be notified from the FM interface, management entity which implements E-OSF should automatically send the alarm information and the related contents to the email box of the registered person to be notified. In the meanwhile, Management entity that implements E-OSF should provide Email address management function.

6.1.4.3 Alarm SMS notification

Management entity that implements E-OSF should support the SMS notification function of the alarms. For certain alarm, when the user has confirmed the person to be notified from the FM interface, management entity which implements E-OSF should automatically send the alarm information and the related contents to the mobile phone of the registered person to be notified.

In the meantime, management entity that implements E-OSF should provide mobile phone number management function for the SMS delivery.

6.1.4.4 Alarm light and sound notification function set

Management entity that implements E-OSF should support the interface that is used to connect the external equipment that can display the problematic NE with light and sound.

6.1.4.5 Alarm smoothing

Alarm smoothing is used to deal with alarms that is often happened and cancelled automatically. When this kind of alarm is happened, it should be forwarded after smooth. The alarm is smoothed by the method of alarm forwarding delay. It means that the operator can set the delay time to forward the alarms on management entity which implements E-OSF. During the period of delay, if the alarm has automatically been cancelled, there is no need to forward the notification by email or SMS, otherwise forwarding should be implemented.

6.2 Performance Management (PM)

6.2.1 Overview

PM is an important function of network management, requiring management entity which implements E-OSF to define the measurement tasks of NE performance and collect, save and display the performance data in a proper way. Through the collection, real time observation, storage and analysis, it should provide basic data and give recommendations on how to improve the network service quality and how to allocate/plan of network resources, so as to monitor and optimize the NE performance.

Management of measurement includes the following function sets:

- Definition of measurement task function set
- Query of the measurement tasks function set
- Modification of measurement function set
- Delete measurement task function set
- Activation of measurement task function set
- Hang up of measurement task function set
- Figure of measurement task status change function set

6.2.2 The management of measurement task function set

6.2.2.1 Definition of measurement task function set

Management entity which implements E-OSF allows user to define the following properties of the NE performance measurement:

- Measured object: list of certain type of NEs that need to be measured.
- Performance indicator set: Performance indicator set corresponds to measurement indicator set. The counter in the set can be self-defined. One measurement task can include one or several performance indicator sets.
- Measurement start time: If it is not assigned, it means start immediately, and time is in year/month/day/hour/min.
- Measurement stop time: If it is not assigned, it means keep monitoring, and time is in year/month/day/hour/min.
- Measurement period: It refers to the periods in a day that need to be measured, and the start time of each period is exactly xx'clock.
- Measurement schedule: It is divided into weekly schedule or monthly schedule. Weekly schedule defines in which days the measurement is done in a week, and monthly schedule defines in which days the measurement is done in a month. The combination of measurement plan and measurement periods defines measurement time.
- Granularity of the measurement: it refers to the interval between measurement data collections. The required granularity is 15 min.
- Interval between reports: interval between reports should be a multiple of the interval between measurement data collections.

After measurement task is finished, the initial status is "inactive". The measurement task should be activated before it becomes valid. When several measurement tasks request the measuring of the same Counter in the same NE, the task can be accepted. The actual periods that management entity that implements E-OSF obtained the statistics of the Counter is the combination of these measurement tasks.

6.2.2.2 Query of the measurement task function set

Management entity which implements E-OSF provides functions for querying parameters and status of the measurement tasks. The parameters of measurement tasks definition refer to clause 8.2.1. The value for the measurement status can be: "inactive" and "active".

6.2.2.3 Modification of measurement task function set

Management entity which implements E-OSF should enable the user to modify measurement parameter before user modify the measurement task, the task should be confirmed by user in "inactive" status, and if it is activated, user need to hang up the task first; I.e. the user can only modify parameters of measurement tasks which are "inactive".

6.2.2.4 Delete measurement task function set

Management entity which implements E-OSF should enable the user to delete measurement task before user delete the measurement task, the task should be confirmed by user in "inactive" status, and if it is activated, user need to hang up the task first; I.e. the user can only delete measurement tasks which are "inactive".

6.2.2.5 Activation of measurement task function set

The activation of measurement task refers to management entity which implements E-OSF can activate measurement task which is in "inactive" status through the activation action. After the activation is done, measurement task should change from "inactive" status to "active" status. Then collect and submit performance data according to the measurement task defined start time, stop time, measurement period, measurement plan, collection granularity and report granularity.

6.2.2.6 Hang up of measurement task function set

Through hang up operation, change measurement task from "active" status to "inactive" status. From user's point of view, in this status management entity which implements E-OSF can not collect or report performance data.

6.2.2.7 Figure of measurement task status change

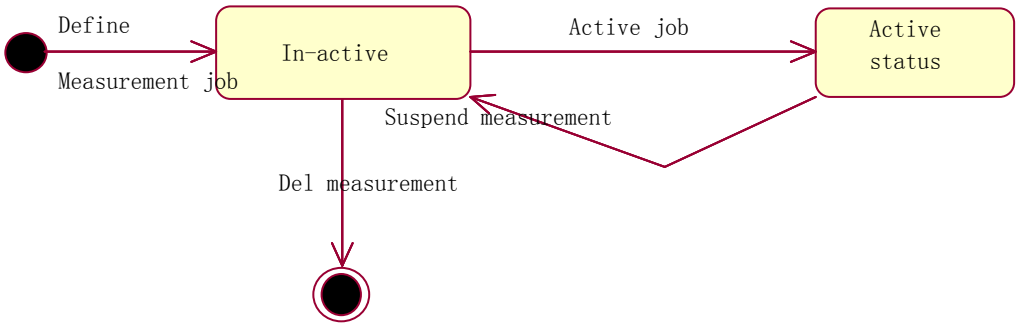


Figure 6.2.2.7: Measurement task status change

6.2.3 Performance data management function set

Performance data management refers to management entity which implements E-OSF effectively collect, store, query and generate report of performance data.

6.2.3.1 Collection of performance data function set

Management entity which implements E-OSF obtains performance data in file format, and this file is called performance data file. Performance data file is organized by NEs.

NOTE: Performance data file is not organized by measurement tasks because several measurement tasks can send measurement requests to the same counter. The measurement time can be overlapping.
So if the file is organized in this way, it may cause the statistics of the same counter in the same period to appear in the performance data files of different tasks.

The delay of performance data entrance (into the database) should be less than 30 min. For example the data of 10:00—11:00 should be entered into the Management entity which implements E-OSF database by 11:30 at the latest.

If the assigned Counter does not finish the entrance after the maximum delay threshold, Management entity which implements E-OSF should trigger an alarm indicating the performance data collection is overdue.

6.2.3.2 Storage of performance data function set

Management entity which implements E-OSF obtained performance data should be stored in database and management entity which implements E-OSF should storage the performance data for at least 2 months. The performance data file management entity which implements E-OSF obtained from NEs should be saved for at least 24 hours THIS CLAUSE DOES NOT EXIST.

6.2.3.3 Query of performance data function set

Management entity which implements E-OSF can query the performance data according to NE, time, performance data etc, and the result can be exported as a file (XML or TXT or Excel format).

6.2.3.4 Generation of performance data report function set (optional)

Management entity which implements E-OSF can generate statistic report of performance data, and display the information with line, column or pie charts.

Management entity which implements E-OSF can self-define the statistics report, management entity which implements E-OSF should be able to print out the statistics.

6.2.4 Performance threshold management function set

Performance threshold management can automatically compare the current performance indicator or the calculation result of performance indicators with the pre-defined threshold. If the value is above the threshold, it should generate relative performance alarm. Once the value is returned back to normal, this alarm should be deleted automatically.

Performance threshold management include the creation, modification, query, deletion, hang up and restoration of performance threshold.

Performance alarm and alarm clear operation should follow the rules in the fault management part of this document.

6.2.4.1 Creation of performance threshold function set

The performance threshold can be defined according to needs. It is setting threshold for performance measurement items (independent counter or the combination of multiple counters). Management entity which implements E-OSF should monitor performance measurement items defined by performance threshold, generate alarm when the performance data have passed threshold. The alarm type is service quality alarm (over the threshold alarm).

The parameters need to be defined:

- The monitored performance measurement item can be a single counter or the calculation result of combined counters.
- The level of alarms which generate performance alarm (see the FM part of the present document for requirements on performance alarm information and operation)
- The NE scope which the performance alarm should apply.

6.2.4.2 Query and modification of performance threshold function set

Management entity which implements E-OSF can query current performance threshold list and performance threshold status (active, hang up), and can modify the threshold.

6.2.4.3 The deletion of performance threshold function set

Management entity which implements E-OSF can delete defined performance threshold. After deletion, management entity which implements E-OSF should not report related performance alarm.

6.2.4.4 The hang up and restore of performance threshold function set

Management entity which implements E-OSF can switch the performance threshold between active and inactive by hang up and restore operations.

When the performance threshold is active, management entity which implements E-OSF should monitor the performance data and generate performance alarms. When performance threshold is in hang up status, management entity which implements E-OSF should stop monitoring the performance data, and should not generate related performance alarms.

6.3 Configuration Management (CM)

The CM function is mainly responsible for overall management of all the NE hardware and software configuration data or the exchange data, displaying the equipment's working status by figures or texts.
The information is displayed in different layers, and it can integrate, query, edit, delete, preset, backup, authenticate and rollback configuration data.

6.3.1 General management function

6.3.1.1 NE/network resource configuration management

The NE objects that can be managed by the system

- CN_CS: the parameter configuration of MSC, VLR, HLR/AUC etc;
- UTRAN: the parameter configuration of RNC, NodeB and that of related ATM;
- CN_PS: the parameter configuration of GGSN, SGSN, DNS, FW and that of related ATM;
- Management entity which implements E-OSF: can query the configuration information of NMS equipment (including database server, application server, WEB server, work station, PC, LAN switch, router, printer etc) including host name, IP, port, operating system and software version etc.

6.3.1.1.1 Creation, modification and deletion of NE

The creation, modification and deletion of NE refer to create, modify and delete the logical definition of NE in management entity which implements E-OSF, defining the NEs to be managed by management entity which implements E-OSF.

1) Create NE

After management entity which implements E-OSF installation, it does not have NE data of the network but management entity which implements E-OSF should provide NE creation function. When creating NEs, user should input the following contents:

- NE type
- NE name
- NE address: refers to the physical address which can locate the NE
- The vendors that provide the NE equipments

With the above information, management entity which implements E-OSF can find the NEs which comply with the above information in the managed network, establishing the communications between management entity which implements E-OSF and NEs. When NE is created, management entity which implements E-OSF can establish the connection with NEs, and through the connection, it can configure the NEs.

2) Delete NE

User can delete an NE which does not exist or has been modified but still exist in management entity which implements E-OSF, including the related configuration data.

3) Query/modify NE

User should be able to query or modify the properties of the NE, which were listed when the NE was created.

6.3.1.1.2 NE management software

- Query the version, status, activation time of the NE software package and patch;
- Patch backup of the NE software package and patch;

- The download of the NE software package and patch;
- The activation and handover of the NE software package and patch;
- The log function of the NE software package and patch;
- The management of multiple of NE software package and patches.

6.3.1.2 The management of configuration data

1) Query of configuration data

Management entity which implements E-OSF should be able to query the current configuration data of the NE.

2) Synchronization of configuration data

Synchronization of configuration data refers to management entity which implements E-OSF collects and the current configuration data and save it.

3) Download and activation of configuration data

Management entity which implements E-OSF downloads the configuration data to NE and activates them.

4) Rollback of configuration data

When management entity which implements E-OSF have downloaded the configuration data to NE and activated them, it can rollback to the original status if necessary (for example, configuration of exchange data).

6.3.2 Configuration of the managed objects

6.3.2.1 The configuration of radio access network

1) RNC data configuration

Signalling data configuration, hardware data configuration, ATM exchange configuration, data configuration between RNCs, data configuration between NodeB and RNC, data configuration between RNC and MSC, data configuration between RNC and SGSN etc.

2) NodeB configuration

Data configuration of NodeB and that between NodeB and RNC

6.3.2.2 Configuration of core network

1) MSC/VLR data configuration

Including data configuration of system, data configuration of signalling, data configuration of services, data configuration of pre-analysis, signalling data, circuit data, GT analysis, BTS related exchange data configuration, data configuration of ATM, number analysis (calling number analysis, called number analysis, call transfer, roaming number analysis, handling of calling number display), routing analysis, EOS analysis etc.

2) SGSN data configuration

Including data configuration of system, data configuration of signalling, GT analysis, Gb interface configuration, routing data configuration, DNS configuration, Iu-PS interface configuration, ATM data configuration, loading sharing management etc.

3) GGSN data configuration

Including APN configuration, address pool configuration, Gi interface configuration, Gn configuration, RADIUS configuration, loading sharing management etc.

4) HLR data configuration

HLR system data configuration, signalling data configuration, HLR user data configuration, user capacity data configuration, HLR physical data configuration, HLR capacity data configuration, system parameter configuration, GT analysis, roaming VLR data configuration, call forwarding number, data configuration of local MSC/VLR, load sharing management, HLR service support etc.

5) DNS and Firewall data configuration

To be decided.

6.4 Security Management

Security management provides effective control mechanism that can limit the user access and operation over the NEs in the management entity which implements E-OSF, guaranteeing each legal user can login normally, use the software module he is authorized to use, get access to NE he is allowed to visit, make use of commands he is entitled to use and prevent overstepping. This should ensure the security of network equipment and the secure operation of NMS, making records of the authentications and authorizations in the system so that the operations are undeniable.

6.4.1 Security management mechanism

Security management mechanism should be implemented through user management, user group management, authorization management, authentication, billing. Management entity which implements E-OSF should support multiple user management and manage user in groups. One user should belong to one or more user groups.

User privilege is given based on the user groups, but not on single user.

System administrator can make relative security management policy according to needs, flexibly add or delete user accounts or give relative privileges. Management entity which implements E-OSF should make a record of user login or authentication.

6.4.2 User management, user group management, privilege management

Management entity which implements E-OSF has and only has one super administrator group, in which there is a default super administrator. The super administrator group and the default super administrator can not be deleted. Only members in super administrator group can do user management, user group management, privilege management.

6.4.2.1 User management

1) Add a user

Add a new user needs to give the user name, password, and assign the user group that the user is in.

2) Delete a user

Delete an existing user and it should no longer exist.

3) Lock a user

Lock an existing user. The user should not be able to visit management entity which implements E-OSF until he is unlocked.

4) Unlock a user

Unlock a locked user, and he should be able to visit management entity which implements E-OSF again.

5) Query user information

Query user information, including, user name, the lock status, and user privilege etc.

6) Modify user password

User can modify his own password, member of super administrator group can modify any user password which can not be saved or transmitted in plain text.

Management entity which implements E-OSF user should not be bound to operating systems on the management entity which implements E-OSF Client end.

6.4.2.2 User group

1) Add a user group

Add a new user group, need to give the name of the user group and can assign the privilege of this user group.

2) Modify user group

Modify an existing user group, need to give the name of the user group and can modify the privilege of this user group.

3) Delete user group

Delete an existing user group and it should no longer exist. If a user only belongs to this group, it should be deleted.

4) Lock a user group

Lock an existing user group, meaning lock the related privileges of the users under this group.

5) Unlock a user group

Unlock a user group and the users under this group should regain the privileges.

6) Query the user group information

Query user group information, including: user group name, the lock status of user group, users in the user group, privilege of the user group etc.

6.4.2.3 Privilege management

Privilege management can assign the contents of the privilege and the given of privileges to user groups.

The privilege includes the following parameters:

- Allow or prohibit the use of software module
- Allow or prohibit the access of NE or NE groups
- Allow or prohibit the operation on NE.

Overlapping of privileges: when a user belong to several groups at the same time, different privilege can be given to the same user group, the same privilege can be given to different user groups.

6.4.3 Identification, authentication, billing

6.4.3.1 Identification

When a user is login to management entity which implements E-OSF, send its identification information to management entity which implements E-OSF security management system and management entity which implements E-OSF security subsystem should check the information according to management entity which implements E-OSF local identification information so that the system should know if the user is legal.

6.4.3.2 Authentication

When a user is using management entity which implements E-OSF software module, the system should authenticate its privilege.

6.4.3.3 Accounting

For all the authentications and identifications, account should be done so that the operations are undeniable. Accounting information includes the user's information, time and operation result etc. The accounting management requirements refer to "log management".

6.5 Software system Management

6.5.1 Function overview and work division

The chapter lists the requirements from management entity which implements E-OSF software management and system maintenance points of view.

6.5.2 Management entity which implements E-OSF software management

The software management of management entity which implements E-OSF system refers to managing management entity which implements E-OSF system software configuration, running status, file backup and system security etc. to ensure that the system can securely run management entity which implements E-OSF.

6.5.2.1 Software version management

The system should make a record of all the software modules, patch version and the function remarks etc running on managed entity which implements E-OSF in detail.

6.5.2 Management entity which implements E-OSF software management

The software management of management entity which implements E-OSF system refers to managing management entity which implements E-OSF system software configuration, running status, file backup and system security etc. to ensure that the system can securely run management entity which implements E-OSF.

6.5.2.1 Software version management

The system should make a record of all the software modules, patch version and the function remarks etc running on managed entity which implements E-OSF in detail.

6.5.2.2 Software patch management

6.5.2.2.1 Load of patch

The system should provide function by which the software patch can be loaded to management entity which implements E-OSF, and the patch loading progress can be shown. If the patch loading process has any problem, the system should provide roll back function so that the system to go back to the status before the patch is loaded. If the patch loading is finished, update the new patch number.

6.5.2.2.2 Activation of the patch

The system should provide patch activation function, so that the patch application can work properly.

6.5.2.2.3 Deactivation of patches

If the software patches can not work normally in the management entity which implements E-OSF, the system should provide deactivation function.

6.5.2.2.4 Unload patches

The system should provide management entity which implements E-OSF software patch unload function.

6.5.2.2.5 Patch number and record

The system should have detailed version record and function description of all the patches on the management entity which implements E-OSF.

6.5.3 Maintenance E-OSF implementation system

Maintenance function of management entity which implements E-OSF system mainly include the monitoring and management of related file system resource, memory, CPU resource, data storage room etc. The sampling time and threshold of the indicators can be set by users. It can also view the system process, the process name, status of progress, start time, stop time, running host as well as process type etc. It should also be able to break and activate some processes.

6.5.3.1 Database maintenance function

The database maintenance function of management entity which implements E-OSF system provides the following means to database maintenance for the user:

- Monitor the space occupied by database
- Automatically record the increase of database everyday;
- User can conveniently check the status of the database connection progress
- Provide user interface through which user can query and modify database.

System should provide a limit function for each level of threshold for database space. When there is a threshold overflow, there should be an alarm of the relevant level which should prompt the maintenance to backup history data, clear useless data or add more storage space.

6.5.3.2 System log function

The log management function of management entity which implements E-OSF is mainly used to query, count and document the system log, include to start, exit, stop and restart Management entity which implements E-OSF database and application process. It also manages the system information generated in important operational process and help management entity which implements E-OSF maintenance.

6.5.3.3 System backup function

The purpose of system backup is to recover the management entity which implements E-OSF to the original status before the failure according to the file system backup and database backup.

Management entity which implements E-OSF system backup includes file system backup and database backup. The backup mode required by management entity which implements E-OSF system includes:

- Manual backup and manual backup on a regular basis,
- Online backup and offline backup,
- Full backup and incremental backup.

The configuration of backup parameter: the user selects backup method, backup contents, backup time and backup media.

Data recovery: when the data is corrupted, management entity which implements E-OSF can restore the correct data. The recovery can be done through backup or obtain the information from NEs.

System recovery: When the system is corrupted, it can be recovered to normal according to backup data.

6.5.3.4 Remote access function (optional)

Provide relative dial up access or VPN access, and guarantee the normal and secure operation of the access modes, prevent illegal users so as to protect the normal operation of NMS, ensure the data security and business confidentiality.

6.5.4 High system availability (optional)

In order to increase the system availability, management entity which implements E-OSF should provide redundancy configuration so that when one management entity which implements E-OSF failed, the system can still handle alarms and maintain the NEs with commands. An effective redundancy system should at least provide fault management function and configuration management function.

6.5.5 System expandability

In order to adapt to the ever-increasing information of NEs and the handling the change information, management entity which implements E-OSF system software and hardware should be expandable.

Annex A:
E-OSF and 3GPP IRP set comparison

A.1 Fault management and AlarmIRP

Table:

Functional Requirements			Satisfied by AlarmIRP	Importance
FM	Alarm surveillance function set	Alarm view function set	getAlarmList(M) getAlarmCount(O)	Should Have
		Alarm status function set	getAlarmList(M) AcknowledgeAlarm(M) unacknowledgeAlarms (O)	Should Have
		Alarm prompt customization function set	NA	Should have
		Alarm filter function set	getAlarmList(M)	Should have
	Fault localization function set	Fault localization policy function set	NA	Should have
		Verification of parameters and connectivity function set	NA	May have
		Sub-Network fault localization function set. see	NA	May have
		Running of diagnostic function set	NA	May have
	Alarm operation function set	Alarm query function set	getAlarmList(M)	Should Have
		Alarm synchronization function set	getAlarmList(M)	Should Have
		Alarm confirmation function set - Cancel alarm confirmation	unacknowledgeAlarms (O)	Should Have
		Alarm confirmation function set - Clear the alarm	clearAlarms (O)	Should Have
		Alarm confirmation function set - History alarm statistics and report generation	getAlarmList(M) getAlarmCount(O)	Should Have
		Alarm confirmation function set - History alarm storage time	NA	Should have
		Alarm severity function set	NA	Should Have
	Alarm forwarding	Alarm EMAIL notification function set	NA	Should have
		Alarm SMS notification function set	NA	Should have
		Alarm light and sound notification function set	NA	Should have

Annex B:
Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Cat	Old	New
Mar 2008	SP-39	SP-080075	--	--	Submitted to SA#39 for Information	--	1.0.0	
Apr 2008	SP-40	SP-080447	--	--	Submitted to SA#40 for Approval	--	2.0.0	8.0.0