FINAL DRAFT

EUROPEAN
TELECOMMUNICATION
STANDARD

pr **ETS 300 617**

March 1996

Source: ETSI TC-SMG

Reference: DE/SMG-061206P

ICS: 33.060.50

Key words: Digital cellular telecommunications system, Global System for Mobile communications (GSM)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Digital cellular telecommunications system (Phase 2); GSM Network configuration management (GSM 12.06)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

* Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Special Mobile Group (SMG) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

This final draft ETS describes the Configuration Management (CM) aspects of Network Elements (NEs) within the Digital cellular telecommunications system. This ETS corresponds to GSM technical specification, GSM 12.06, version 4.1.0.

NOTE: TC-SMG has produced documents which give technical specifications for the implementation of the Digital cellular telecommunications system. Historically, these documents have been identified as GSM Technical Specifications (GSM-TSs). These specifications may subsequently become I-ETSs (Phase 1), or European Telecommunication Standards (ETSs)(Phase 2), whilst others may become ETSI Technical Reports (ETRs). These ETSI-GSM Technical Specifications are, for editorial reasons, still referred to in this ETS.

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

Configuration Management (CM), in general, provides the operator with the ability to perform effective network management as the PLMN evolves. CM is initiated by the operator in various network elements of the PLMN to meet the operator objectives.

CM actions may be requested as part of an implementation programme (e.g. additions and deletions), as part of an optimisation programme (e.g. modifications), and to maintain the overall Quality of Service. The CM actions are initiated either as a single action on a network element of the PLMN or as part of a complex procedure involving actions on many network elements.

Clause 4 provides a brief background of CM while Clause 5 explains CM services available to the operator. Clause 6 breaks these services down into individual CM functions which will support the defined services. Clause 7 describes the application of these services and functions to the BSS NE in a GSM PLMN. In Annex A there are informative examples to illustrate the application of CM functions to complete scenarios.

Blank page

1 Scope

This final draft European Telecommunication Standard (ETS) describes the Configuration Management (CM) aspects of Network Elements (NEs) which constitute a PLMN with initial emphasis on the Base Station System (BSS) management. This is described from a management perspective being decomposed into constituent functionalities, which in turn will allow the construction of a management object model using the object oriented paradigm to support open systems management (see GSM 12.20 (ETS 300 622) [14]). The ETS follows the methodology described in GSM 12.00 (ETS 300 612-1)[10].

This ETS defines a set of controls to be employed to effect set-up and changes to a PLMN, in such a way that operational capability, network integrity and inter working co-operation are ensured. In this way, this ETS describes the interface behaviour for the management of PLMN NEs in the context of the described management environment. The context is described for both the Operation System (OS) and NE functionality. The standardisation of specific controls is outside of the scope of this ETS.

2 Normative references

This ETS incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references subsequent amendments to, or revisions of, any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] GSM 01.04 (ETR 100): "Digital cellular telecommunication system (Phase 2); Abbreviations and acronyms".

[2] GSM 04.06 (ETS 300 555): "Digital cellular telecommunication system (Phase 2); Mobile Station - Base Station System (MS - BSS) interface Data Link (DL) layer specification".

[3] GSM 04.08 (ETS 300 557): "Digital cellular telecommunication system (Phase 2); Mobile radio interface layer 3 specification".

[4] GSM 05.02 (ETS 300 574): "Digital cellular telecommunication system (Phase 2); Multiplexing and multiple access on the radio path".

[5] GSM 05.05 (ETS 300 577): "Digital cellular telecommunication system (Phase 2); Radio transmission and reception".

[6] GSM 05.08 (ETS 300 578): "Digital cellular telecommunication system (Phase 2); Radio subsystem link control".

[7] GSM 08.08 (ETS 300 590): "Digital cellular telecommunication system (Phase 2); Mobile Switching Centre - Base Station System (MSC - BSS) interface Layer 3 specification".

[8] GSM 08.52 (ETS 300 593): "Digital cellular telecommunication system (Phase 2); Base Station Controller - Base Transceiver Station (BSC - BTS) interface Interface principles".

[9] GSM 08.58 (ETS 300 596): "Digital cellular telecommunication system (Phase 2); Base Station Controller - Base Transceiver Station (BSC - BTS) interface Layer 3 specification".

[10] GSM 12.00 (ETS 300 612-1): "Digital cellular telecommunication system (Phase 2); Objectives and structure of Network Management (NM)".

[11] GSM 12.01 (ETS 300 612-2): "Digital cellular telecommunication system (Phase 2); Common aspects of GSM Network Management (NM)".

[12] GSM 12.03 (ETS 300 614): "Digital cellular telecommunication system (Phase 2); Security management".

[13] GSM 12.04 (ETS 300 615): "Digital cellular telecommunication system (Phase 2); Performance data measurements".

[14] GSM 12.20 (ETS 300 622): "Digital cellular telecommunication system (Phase 2); Base Station System (BSS) Management Information".

[15] CCITT Recommendation X.721 (ISO/IEC 10165-2): "Information technology - Open Systems Interconnection - Structure of management information: Definition of management information".

[16] CCITT Recommendation X.731 (ISO/IEC 10164-2): "Information technology - Open Systems Interconnection - Systems Management: State management function".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply.

data: Is any information or set of information required to give software or equipment or combinations thereof a specific state of functionality.

equipment: Is one or more hardware items which correspond to a manageable or supervisable unit or is described in an equipment model.

firmware: Is a term used in contrast to software to identify the hard-coded program which is not downloadable on the system.

hardware: Is each and every tangible item.

network element: Is a discrete telecommunications entity which can be managed over a specific interface e.g. the BSS.

network resource: Is a component of a Network Element which can be identified as a discrete separate unit e.g. BSC, BTS or TRX .

operator: Is either

- a human being controlling and managing the network; or,
- a company running a network (the PLMN operator).

optimisation: Of the network is each up-date or modification to improve the network handling and/or to enhance subscriber satisfaction. The aim is to maximise the performance of the system.

re-configuration: Is the re-arrangement of the parts, hardware and/or software that make up the PLMN. A re-configuration can be of the parts of a single NE or can be the re-arrangement of the NEs themselves, as the parts of the PLMN.

reversion: Is a procedure by which a configuration, which existed before changes were made, is restored.

software: Is a term used in contrast to firmware to refer to all programs which can be loaded to and used in a particular system.

up-dates: Generally consist of software, firmware, equipment and hardware, designed only to consolidate one or more modifications to counter-act errors. As such, they do not offer new facilities or features and only apply to existing NEs.

up-grades: Can be of the following types:

- enhancement - the addition of new features or facilities to the PLMN;

- extension - the addition of replicas of existing entities.

3.2 Symbols

None

3.3 Abbreviations

For the purposes of this ETS ,the following abbreviations apply.Further abbreviations used may be found in ETR 100 [1].

BSIC	Base Station Identification Code
BSS	Base Station System
CM	Configuration Management
FM	Fault Management
FW	Firmware
HW	Hardware
MIB	Management Information Base
MOC	Managed Object Class
NE	Network Element
NR	Network Resource
OS	Operation System
SW	Software
TRX	Transceiver

4 Network configuration management

4.1 General

In the development of a PLMN, three general phases can be described which represent different degrees of stability. Once the first stage is over, the system will cycle between the second and the third phases. This is known as the network life-cycle and includes:

1) the PLMN is installed and put into service;
2) the PLMN reaches certain stability and is only modified (dynamically) to satisfy short term requirements, e.g. by (dynamic) re-configuration of resources or parameter modification; this stable state of a PLMN cannot be regarded as the final one because each equipment or SW modification will let the PLMN progress to an unstable state and require optimisation actions again;
3) the PLMN is being adjusted to meet the long term requirements of the network operator and the customer, e.g. with regard to performance, capacity and customer satisfaction through the enhancement of the network or equipment up-grade.

During these phases, the operators will require adequate management functions to perform the necessary tasks.

4.1.1 Installing a PLMN

When a PLMN is installed and initialised for the first time, all NEs need to be introduced to the OS, the data for initialisation and SW for proper functioning need to be provided. All these actions are carried out to create NEs and to initialise them.

4.1.2 Operating a PLMN

Whilst in service, the operator needs to react to short term incidents such as traffic load requirements which are different from the current network capabilities, NEs/NRs need to be re-configured and parameters need to be adapted to follow these day-to-day requirements.

4.1.3 Growing/pruning a PLMN

As the PLMN grows and matures new equipment is installed and understanding of system behaviour increases. Subscriber requirements/wishes may demand that operators modify their system. In addition manufacturers improve the infrastructure components and add features to their products hence the operator will start modifying the PLMN to profit from these changes and to improve subscriber satisfaction. Additionally, the PLMN configuration will be modified (i.e. it will be up-dated or up-graded) to cope with a need for increasing or decreasing network capacity. These actions are carried out for the long term strategy of the operators to optimise the network.

4.1.3.1 System up-date

Whenever the PLMN needs to be improved for reasons of reducing failures, the system will be up-dated. In this case SW or equipment will be replaced without adding new functionalities or resources to the network. The basic function required is:

> the modification of existing SW/equipment; it may be necessary to introduce a different set of data to cope with the modified SW/equipment.

For system up-date the network shall not be disturbed in its function until the required modification is activated. This requires mechanisms to

- do SW/data downloading in parallel with on-going traffic;
- isolate the affected NEs/NRs from traffic before the actual modification is done.

4.1.3.2 System up-grade

System up-grade may affect all areas of PLMN activities and can be described as enhancements, whereby either new features or new facilities are implemented. Also extensions, reductions or further replications of existing facilities are covered by this CM aspect. The CM functions employed are:

- Creation of NEs and/or NRs;
- Deletion of NEs and/or NRs; and,
- Modification of NEs and/or NRs.

The following requirements are to apply:

- to support expeditious handling of SW and data while minimising impact on ongoing traffic;
- to follow a required sequence of up-grades: e.g. the new SW depends upon the availability of the new equipment functionality;
- to provide the capability to create an additional logical NE/NR without having installed the physical resource supporting it: for example it should be possible to create a cell in a BSS without the physical equipment present or connected. However, additional mechanisms should be in place to prevent any service connection to any physically non-existent NE/NR or reporting failures from non-existing NE/NR;
- to provide the capability to prevent the erroneous taking into service of a NE/NR which is not fully installed and initialised: whenever a NE/NR is modified (extension or reduction) it shall be taken out of service until the logical part of the procedure is finished. An extended NE/NR cannot be placed into service until all needed parameters and equipment are initialised. Likewise, a reduced NE/NR cannot be placed back into service until the applicable re-configuration is performed.

When the network is up-graded by the addition of NEs or NRs or a change in the configuration, it is essential that the NE/NR can be restored to the configuration which existed before the changes were made. This procedure is called "reversion" and is useful in maintaining service if any difficulty should arise from a network up-grade.

4.2 Operational context for configuration management

The CM functions available to the operator need to address various aspects beyond that which might strictly be regarded as management of the network. These include:

- assisting the operator in making the most timely and accurate changes thus avoiding lengthy waiting periods or complex scenarios;
- ensuring that CM actions will not have any secondary effects on the network other than the specified ones;
- providing mechanisms to protect the telephony-related traffic from effects due to CM actions, it shall be possible to inhibit traffic if a traffic affecting CM action is expected and to gracefully release calls prior to the closure of the resource;
- providing mechanisms to overcome data inconsistency problems by logging the modifications for reversion reasons, or to recover through data update from a second source.

4.2.1 Administrative aspects of configuration management

When managing the network by creating, deleting or modifying NEs/NRs, the operator should ensure that there is no uncontrolled impact on the network. The network management system therefore needs to support the following set of management functionalities when addressing various administrative aspects:

- Security;
- Data Validity;
- Data Consistency; and,
- Resource Administration.

4.2.1.1 Security aspects

It is up to the operator to ensure the network security by employing the appropriate mechanisms for control of logical and physical access.

4.2.1.2 Data validity

It is also up to the operator to ensure that data used in CM is valid given the particular network configuration. Thus, the operator is responsible for the data setting in a given context.

4.2.1.3 Data consistency

The NE-OS relationship employs an object model abstraction of the NE's physical and logical resources to be managed by the OS which is the agreed MIB between NE and OS. The NE local representation of those physical and logical instantiated resources to be managed, as well as their accurate mapping onto the agreed object model abstraction, is a pure matter of the NE manufacturer. Thus the consistency between the actual local representation of physical and logical resources to be managed within an NE, and the corresponding view of the OS, totally relies on:

- which information is exchanged between NE and OS; this is mainly a matter for the GSM 12 series, defining object models for various functional areas and/or of agreements between the network operator and his manufacturer(s);
- how such information is exchanged between NE and OS; this is also a matter for other GSM 12 series documents, refer to GSM 12.01 [11];
- how information is locally represented and treated by an NE and by its associated OS(s); this is left to the manufacturers of NEs and OSs.

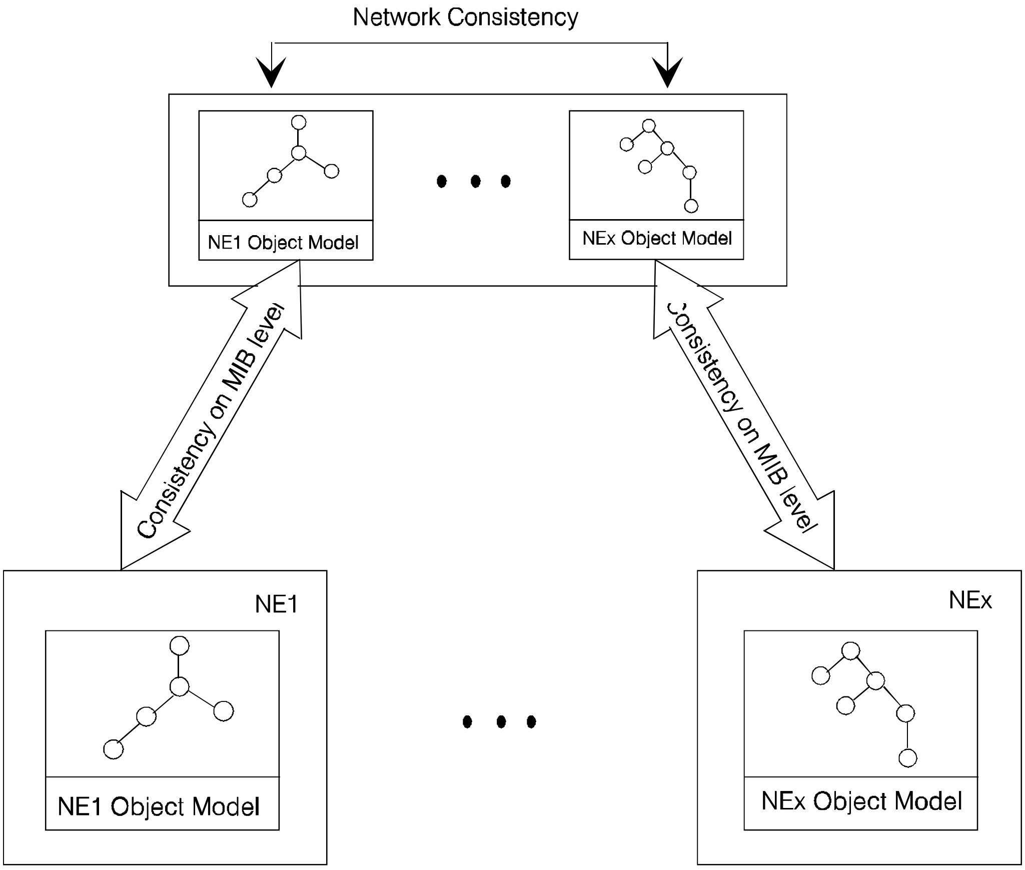

Figure 1: NE - OS data relationship.

A peer-to-peer data consistency between NE and OS does not guarantee overall data consistency from a network point of view. Consistency between related data is restricted to the information level offered by the information abstraction common to both the NE and the OS, and thus may be better called consistency on the MIB level.

While complete data consistency may not be possible, it is up to the operator and manufacturer to define and support an appropriate set of procedures to ensure that the required Quality of Service is maintained.

In order to promote data consistency, the following operational procedures are recommended:

- always use confirmed services:
  all types of OS-NE information exchange leading or possibly leading to modifications of the NE's database or the OS's database should be confirmed;
- control of autonomous NE/NR re-configuration:
  local NE/NR re-configuration, for example partial or full reversion mechanisms (either triggered autonomously or by a local operator), should be reported;
- define appropriate audit procedures on the NE - OS Interface to support NE - OS data re-synchronisation, for example:
  - the OS shall be able to retrieve all management information from the NE accessible via the NE - OS management interface by applying appropriate data retrieval methods (periodically or on request);
  - the OS shall be able to compare the retrieved information with its own data;
  - the OS shall be able to report any deviations between the NE's view and the OS's view to the operator;
- maintain the OS view: As far as possible operational concepts for data manipulation should employ the OS(s) as the only managing instance(s) for an NE to be managed. If however access to local NE data is given to maintenance personnel quasi data consistency is achieved by:
  - applying a remote OS terminal for the local access to the NE under consideration rather than directly modifying NE data without any control of the OS;
  - changes made locally shall be notified to the managing OS(s) as defined in the appropriate information model.

4.2.1.4 Resource administration

Within this document state handling shall follow the rules set by the ISO nomenclature (refer to CCITT Recommendation X.721 [15]) but this shall not imply any implementation requirements.

Before a resource is re-configured by the operator, it may be necessary that the resource supporting the service which is being modified, is taken out of service. This is to minimise any difficulties experienced by subscribers. The means to provide that functionality to the operator is called resource administration.

The operator should be able to take out of service a resource without disrupting the traffic (e.g. if maintenance needs to be done on the network). This can be achieved by not allowing new traffic on the resource, but giving the current users the chance to finish their calls. This operator action is called "SHUT_DOWN" which puts the system into the "SHUTTING_DOWN" state. The SHUTTING_DOWN state will eventually lead to the "LOCKED" state as soon as the last user has finished the call. It might be that some resources cannot be SHUT_DOWN and need to be isolated without an intermediate state. This action is termed "LOCK". Once the configuration is completed by the operator, the "UNLOCK" action is used to put the resource into the "UNLOCKED" state.

It is common that, within the network, resources have functional inter-dependencies, so that when taking a resource out of service, some others also should be taken out of service. This process may have several levels of ripple effects, resulting in a complex procedure. To avoid any mistake, or damage to the operation of the network, the operator will indicate the major resource to be taken out of service; the state propagation, and how the subsequent resources will be affected by this, is dependent on the system architecture.

Additionally, the state of the resource may be qualified with (refer to CCITT Recommendation X.731 [16]):

- Alarm status;
- Procedural status;
- Availability status;
- Control status;
- Standby status;
- Unknown status.

4.2.2 Configuration management triggers

There are various sources which can trigger CM actions. For example an operator may wish to modify the current structure or to set parameters for quality of service improvements.

Alternatively, the system, or a particular part of it, can automatically trigger system modification actions because it needs to recover from faults or to escape overload situations (GSM 04.08 [3], GSM 08.08 [7], GSM 08.58 [9]). This ETS only considers the operator triggered re-configurations. The autonomously triggered re-configurations are not within the scope of this document, neither are the mechanisms employed.

An operator initiated re-configuration may be required for the optimisation of the PLMN or NE. This may result from an analysis of traffic. Under-utilised equipment may be better employed in another way to cater for extra load, either temporarily or permanently.

Some typical CM triggers are the performance measurement results, obtained from measurements defined in GSM 12.04 [13]. GSM 12.04 covers not only typical network configuration evaluation related performance measurements such as hand-over success and failure and the use of power controls on up-link and down-link connections, but also traffic measurements and measurements concerning resource access, resource availability and Quality of Service. These measurements support network configuration evaluation on a short as well as a long term basis.

Other CM triggers may be generated internally to the PLMN administrations which may e.g. determine that the maximum capacity of an HLR, EIR or AUC is reached.

5 Configuration management service components

While a GSM network is first installed and brought into service, and following installation the PLMN operator will enhance and adapt the network to short and long term requirements. In addition, it will be optimised to satisfy customer needs. To cover these aspects of CM, the system will provide the operator with the following capabilities:

- initial system installation to establish the network;
- system operation to adapt the system to short term requirements;
- system up-date whenever it is necessary to modify the system to overcome SW bugs or equipment faults;
- system up-grade to enhance or extend the network by features or equipment respectively.

These capabilities are provided by the management system through its service components:

- system modification to change the network to meet the operators requirements;
- system monitoring to gain an overview on the present SW, equipment and data situation of the network.

The service components will be explained in more detail in the following subclauses.

5.1 System modification service component

Whenever it is necessary to adapt the system data to a new requirement due to optimisation or new network configurations, it will require an operator action to introduce new or modified data into the system. The data will be distributed to:

- either one NE when dealing with a locally limited modification; or,
- to each NE concerned when the change affects multiple NEs; and,
- to the other OSs in the case where multiple OSs exist in the same management domain.

This implies the necessity of mechanisms to ensure data integrity and to maintain system data consistency.

To be able to control the operation of the network, the OS should have all data for each node it is controlling. The detailed definitions of these data items are specified in GSM 12.20 [14].

The concept of system modification includes the following aspects:

- normally, before subscriber impacting data modifications are performed, the NEs/NRs concerned are cleared from traffic in a controlled way;

  NOTE: In the case of "frequency re-definition" it is not necessary to clear the affected NRs from traffic, because a synchronisation mechanism is implemented between MS and NE to prevent any subscriber impact (refer to GSM 04.06 [2]).

- only once all needed data is given to the system, are the concerned NEs/NRs put back into traffic again;
- when the data modification is performed, the affected NEs and the controlling OS will up-date their local data to ensure data consistency within the system;
- safeguards shall be available within the NEs to prevent changes to configuration affecting service(s) in use. In emergencies, it shall be possible to override these safeguards.

On occasion, modifications may not be stable or not fulfil the operator intentions. In these cases, reversion to the previous stable configuration may be necessary. Occasionally there will be changes to the network that create a new configuration which cannot revert to any previous network status for protection. Such changes may involve major equipment modification to the core elements of the network or re-distribution of traffic across interconnected nodes to other Operators. In these cases it is necessary to implement the changes and to manage the consequences of any problems or failures without the protection of 'reversion', as equipment may have been removed or the work programme may be complex, time limited and expensive.

Progress of these changes should be sequential through an agreed milestone plan which includes effective tests to prove network functionality with only one action, or a coherent series of actions, completed at a time. The decision points, beyond which there is no return, should be clearly identified.

"Automatic re-configuration" shall not be dealt with in this document as it is dependent on the implementation. However, if an automatic re-configuration occurs, the operator shall be informed of the result.

5.2 System monitoring service component

The system monitoring service component provides the operator with the ability to receive reports (on request or spontaneously) on the configuration of the entire network or parts of it from managed NEs. These consist of structure, states, versions employed and data settings. Spontaneous reports are sent by the NE if there was an autonomous change of, for example, the states or other values due to fault management actions. Also, the OS may ask the managed NE to send the information required to the OS at any time.

For example the following data will be provided by the NE on request:

- structure and state of the equipment managed by the OS:
  the information as such is important for the operator to gain a consistent view on the system availability;
- information about the currently installed equipment, FW, SW versions and which combinations are compatible with each other;
- frequencies used in each cell;
- performance data related to cell coverage (refer to GSM 12.04 [13]);
- cell configuration data:
  such as cell power, protocol timers or cell identity.

Any inconsistencies found during system monitoring by the OS should be reported to the operator, and it is left to the operator to take appropriate actions.

6 Configuration management functions

6.1 System modification functions

The requirements of CM and their usage lead to basic CM functions to be defined for the network. These describe the required actions on managed elements (NEs or NRs) and the expected reactions. The system modification functions described are:

- Creation of Network Elements and Resources;
- Deletion of Network Elements and Resources;
- Conditioning of Network Elements and Resources.

For each of these areas there are example scenarios given in Annex A to explain the described CM functions. This illustrates possible ways of combining management functions to achieve the required processes. They are not intended to represent any specific implementation. The scenarios have been developed based on the major requirements for the system:

- minimum disturbance of the network by taking the affected resources out of service if needed;
- physical modifications should be independent of the related logical modifications;
- all the required actions to satisfy a defined task should be completed correctly before the resources can be brought into service;
- data consistency checks shall be performed as described in subclause 4.2.1.3.

There are three aspects of NE and NR management which can be distinguished:

1) Management of the physical aspect (equipment);
2) Management of the executable aspect (SW and FW); and,
3) Management of the logical aspect (data).

All three management aspects are addressed, but not all aspects of equipment and SW management are covered by this standard because of their implementation dependencies.

6.1.1 Creation of network elements and network resources

The creation of a NE or NR is used to initially set up a PLMN or to extend an already existing network. The action of creation is a combination of installation, initialisation and introduction of the newly installed equipment to the network and to the OS which will control it. The creation can affect equipment, SW and data.

Whenever a PLMN or parts of it are installed, the created NEs/NRs requires to be:

- physically installed and tested and initialised with a possible default configuration;
- logically installed by means of introduction to the network possibly involving changes to existing NE/NR configurations (e.g. neighbour cell descriptions);
- allowed to be put into service.

The sequence of physical and logical installation may vary depending on the specific PLMN operator strategy. In case the logical creation takes place before the physical creation no related alarms shall be reported to the operator.

6.1.2 Deletion of network elements and network resources

If a network is found to be over-equipped, the operator may wish to reduce the scale of the network or to re-use the spare equipment elsewhere. This can occur when an operator over-estimates the traffic in one area and, for example, under-estimates the load in a different one.

The deletion of a NE or NR requires:

- taking the affected NEs or NRs out of service;
- logical removal from the network (possibly involving changes to other NE or NR configurations, for example, neighbour cell description);
- if necessary, the physical dismantling of the equipment;
- return of other affected NEs or NRs to service.

The sequence of logical and physical removal will not matter if the affected NEs are taken out of service prior to their removal. This will help to protect the network from error situations.

6.1.3 Conditioning of network elements and network resources

There are three categories of modifications to be regarded with respect to NEs or NRs. It is possible to either modify SW, equipment or data or a certain combination of them. Which aspects are affected by any particular modification is implementation dependent.

When a NE or NR is to be modified the following actions shall be performed:

- logical removal;
- required modification; and,
- logical re-installation.

This sequence is recommended to provide protection to the network against fault situations which may occur during the modification process.

The result of conditioning should be able to be determined by the operator by employing the appropriate mechanisms provided through performance measurements (see GSM 12.04 [13]).

A modification to data which has a controlling influence on some resources could influence the resource throughput or its capability to originate new traffic during the modification time. This distinction is made because, for particular modifications, the capacity of the NR can be decreased without influencing the ongoing traffic. Before deciding to perform an action, the operator should consider the effects that a modification might have on capacity, throughput and current activity of a resource.

6.1.3.1 Considerations on conditioning mechanisms

The data which characterise a PLMN will not all be subject to the same rate of change or need to be modified using the same mechanism. Changes to the logical configuration may also need to be applied across multiple NEs. These aspects are described in the following subclauses.

Whenever the configuration of the network requires modification, the following questions will be important to the operator:

- What will be the influence on the ongoing traffic?
- What will be the impact on the capacity of the network?
- How difficult and time-consuming will the modification procedure be?

The answer to these questions will give an idea as to when the modification can be best performed with the aim to keep traffic disturbance as low as possible and to require the modification process itself to cause as little disturbance as possible. On the other hand, it does not seem to be reasonable to invent a "low disturbance" modification algorithm for each single parameter, especially those which are only modified once or twice during the life time of the network. These rare modifications could be performed with an acceptable level of interruption to traffic. Therefore, the system data elements may be classified by:

- modification once or twice during the life time of the system (e.g. protocol supervision timers);
- modification required seldom (e.g. BSIC);
- modification is expected frequently and/or for a short term (telecom parameters).

Depending on this rating the requirements on the modification mechanism for certain data elements should vary.

6.1.3.2 Network traffic considerations

As stated previously, different types of modification mechanisms can be distinguished with regard to their impact on traffic and their extent:

For the impact regarding traffic, the following types can be identified:

- no impact on the traffic at all:
  the modified data values have no relation to the traffic capability;
- impact on traffic:
  the data modification causes for example a change in the volume of allowable traffic without affecting existing traffic; e.g., the set/reset of the ´cell barred´ bit on BCCH for the cell/BTS.

For the impact regarding extent, the following types can be identified:

- impact on only the NR or NE:
  the modification of either SW, equipment or data is effective for a NR, (e.g. one cell/BTS) or a complete NE;
- impact on more than one NE or different NRs of one NE:
  certain modifications on SW, equipment or data will require changes to be performed upon more than one NR in one NE or more than one NE; such changes will require consideration of data consistency, data integrity and network integrity, e.g. it should be distinguished between the NR directly affected by a modification and other impacted NRs; the relationships and dependencies between data values should be described and a mechanism defined to protect the system against inconsistency.

The description of the different mechanisms is detailed in the following clause and illustrative examples can be found in Annex A.

6.2 System monitoring functions

A major aspect of CM is the ability of the operator to monitor the operation of the network. This monitoring capability is necessary for the operator to determine the current operational state of the network as well as to determine the consistency of information among various NEs. The monitoring capability requires three functions to support it: the information request function, the information report function and the response/report control function.

6.2.1 Information request function

In order to support the operator's need to monitor the network, the OS needs to be able to gather information on request from the various NEs. The information request function should support the capabilities of the OS to be able to request information for any single attribute defined in the management information base. In addition, the OS should be able to gather large amounts of information in a single request by providing appropriate scope and filtering constructs in the request.

On receipt of a valid request, the addressed NE shall respond with the current values of the specified data elements. This response will be immediate if so requested by the OS. However, in cases where very large amounts of data are concerned and where the OS and the NE support the capabilities, the OS may request the NE to store the information in a file and transfer it using a file transfer mechanism (refer to GSM 12.00 [10]).

6.2.2 Information report function

In addition to being able to provide information on request, the NE is required to have the capability of reporting information autonomously. Generally this will be performed when some information on the state or operation of the system has changed. For appropriate events in the system the NE should be able to identify the notification as an alarm and be able to indicate the severity and cause of the condition in the report (see also GSM 12.01 [11]). Notifications may be logged locally. Logged notifications may be requested by the OS to be transferred from the NE. Transfer mechanisms may be by file transfer or using messages (refer to GSM 12.00 [10]).

6.2.3 Response/report control function

For responses to information requests and for information reports, it should be possible for the operator to specify where and when the information should go. The OS and NE should provide a capability to configure the response/reporting capabilities such that the following requirements are met:

- information forwarding shall be able to be enabled and disabled;
- information shall be able to be forwarded to the OS as soon as it is available;
- information shall be able to be directed to any of various OSs;
- information shall be able to be logged locally by the NE and, optionally by the OS; and,
- information shall be able to be retrieved from logs using appropriate filtering specifications.

7 BSS configuration management

This clause concentrates on describing the system aspects that can be managed using the management functions defined in clause 6. The particular emphasis is on managing the configuration of the BSS but much of the described functionality can be associated with the CM of other NEs.

This clause describes the management of features, grouped according to the aspect of the configuration to which they refer. They are:

- physical aspect (Equipment):
  - defined by manageable items, for example:
    - Transceivers,
    - Transcoder,
    - etc.;

- executable aspect:
  - defined as the intangible items:
    - SW,
    - FW;

- logical aspect:
  - defined by service , functional and application items, such as:
    - BCCH,
    - "time slot",
    - power control,
    - etc.;

- relational aspect:
  the relationships between the logical, physical and executable aspects.

7.1 Equipment management

This subclause describes the requirements for the management of the physical aspects of a PLMN implementation.

7.1.1 Definition of equipment

For the purposes of this description, HW is taken to mean the physical implementation of the infrastructure. Typically this represents cabinets, racks, shelves, circuit boards, power supplies, cooling systems, etc. In a radio environment it may also include aspects such as antennae, feeder cables, etc. Equipment is HW which is manageable. Some equipment may be monitored and controlled by a remote management system whereas other equipment may be described in an equipment model only because faults or failures need to be reported.

Actual implementations to support the same functionality will differ depending on the approach adopted by manufacturers. A unit of equipment may support one or more functions and one function may be supported by one or more units of equipment. The ability of equipment to be managed and the range of management functions available will depend on the manufacturer.

7.1.2 Equipment management functions

The range of, or necessity for, equipment management functions will vary depending on the nature of the implementation. The following are typical functions for the management of equipment by a remote managing system:

- Equipment Availability Management;
- Equipment Utilisation Management;
- Equipment Identification;
- Equipment Redundancy;
- Overload Protection;
- Replaceability;
- Compatibility.

The list is not exhaustive.

NOTE: The standardisation of this function remains for further study and is dependent on further studies by other standardisation groups.

7.1.2.1 Equipment availability management

Some types of equipment, e.g. Transcoder or Transceiver, may be able to be managed in terms of their availability for use. Putting such an equipment type into service, i.e. making it available, may involve powering up the equipment and the loading of any necessary SW but would not necessarily start the execution of that SW until the supported functionality was made available for service.

Conversely, taking such equipment types out of service may cause the SW to stop executing on all supported processors and, possibly, removal of power from that equipment.

7.1.2.2 Equipment utilisation management

In a system where there is replication of functionality spread across multiple equipment units, it may be possible to manage the mapping of specific functionality to specific equipment units. This can provide a manageable mapping between the equipment and the supported functionality.

Modification to this mapping may be dependent on the ability of the equipment to provide the required functionality.

7.1.2.3 Equipment identification

Equipment can be identified by various techniques. Commonly, these include location (both site and location within a containing equipment - rack location, shelf location, etc.), part number, functional identity and upgrade status. These identities are normally, but not necessarily, fixed for the lifetime of the particular equipment item. The management function required which involves equipment identity is to be able to perform an audit of the equipment to retrieve these various forms of identification.

7.1.2.4 Equipment redundancy

Where essential functionalities are supported by particular equipment types it may be advisable to provide redundant equipment which can take over the role if the first choice equipment suffers a failure. Redundancy may be provided by:

- **hot standby**: a second, separate equipment item is mirroring the activities of the first and can take over immediately when a failure is detected without loss of usage;

- **cold standby**: the second equipment item takes over from the primary equipment but all existing usage is lost.

The unit(s) providing the redundancy may support more than one primary unit. Once the redundant unit has replaced a failed unit in service then that redundancy is lost.

It should be possible to identify redundancy in an equipment configuration and to nominate specific units to act as redundant units to other defined units. Some implementations, especially where "hot standby" is provided, i.e. a one-to-one redundancy exists, will automatically re-configure as the redundancy is a feature of the architecture rather than a manageable function.

When a redundant unit is brought into service this should be notified to the manager system indicating which unit has been replaced. The loss of redundancy should also be notified to the manager.

7.1.2.5 Overload protection

During busy hour periods there is a possibility of overflow situations, i.e. too much traffic for the current network configuration. The system may be able to provide some mechanism to prevent the network from, or to react to, overload situations during this period to cater for the excess traffic.

Overload protection may be provided by:

- **Re-configuration**: the system may be re-configured using existing equipment by automatic or operator controlled increase/decrease of the coverage area of a cell, via power control, handover thresholds, etc. Automatic re-configuration however is implementation dependent and optional.

- **Additional Equipment**: the operator may enhance the capacity of the network through the use of additional equipment already available to the network but not currently in use i.e. the NE is over equipped. The additional equipment should be known to the system as part of the MIB. This additional equipment will be used to provide the extra capacity needed to cover the overload situations.

- **Restricting Traffic**: it will be possible to prevent new traffic from using the cell through mechanisms such as access class barring whilst existing calls will be unaffected (refer to GSM 04.08 [3]).

7.1.2.6 Replaceability

It is important, when deriving a maintenance policy, to know which equipment items are replaceable (e.g. to effect a repair following a fault, or to install a new version of the equipment) and the impact of the replacement action - does the system require power to be removed; is hot insertion allowed?

Since this information is a physical characteristic of the equipment implementation it needs to be associated with the definition of the equipment items.

7.1.2.7 Compatibility

The various equipment units which make up, for example a BTS, may change over time. Upgrades may become available which incorporate new features, or new developments in equipment components may improve capacity. Not all the individual equipment units used in the implementation may work in an ensemble. This is also true of on-board FW which may not be compatible with the parent board on which it is mounted or the SW with which it may be expected to execute.

Information should be available to allow the management of compatibility between equipment components.

7.2 Software management

Centralised management of a highly distributed network, like a PLMN, needs to allow for the continued enhancement and improvement of the installed NE base. One way of implementing new features or improvements is through the delivery from a manufacturer of new SW.

7.2.1 Definition of software

In the context of this description, SW is considered to be comprised of a file or files containing executable instructions or related data which are meaningful only to the host on which it is to execute. An entire system of executable SW may be comprised of multiple files which are related. This may be necessary at a processor, sub-system or system level (e.g. a whole BTS SW load may be comprised of the respective loadable SW packages for each processor or sub-assembly). The extent to which individual processors or sub-systems are manageable independently from the NE or as an integrated part of that NE management will depend on the specific implementation, but the general concept should be applicable to all implementations.

New SW deliveries may include: modifications to the existing SW to correct problems (bug fixing); support of new features; enhancements to existing features; consolidation of base SW and its corrections. Whatever the reason for the delivery of the new SW, it is likely to come in the form of a package. The exact constituents of the package will depend on the manufacturer's strategy and capabilities for SW generation and the distributed or centralised nature of the NE implementation.

7.2.2 Software management functions

In order to control the roll out of a SW delivery, it will be necessary to support one or more of the following SW management functions:

- Receive the SW delivery from source;
- Transfer the SW to the NE for local storage;
- Manage the identification and role of the SW version;
- Construct a loadable/executable form of the SW;
- Load the SW and execute it;
- Manage the local storage of SW.

The following subclauses describe, in more detail, the various aspects of SW management listed above.

7.2.2.1 Receive the software delivery

As mentioned previously, a SW delivery may be comprised of one or more files of executable code and associated data. The method of delivery to the PLMN Operator will be a matter for local negotiation. It is expected that, given the type of technologies involved in the implementation of a PLMN, there will be certain dependencies between the loadable SW delivered as a package of files and the equipment on which it is to execute. There may also be dependencies with any executable code stored in the form of FW within the NE implementation. These dependencies may need to be maintained and correlated by the PLMN Operator before and/or in conjunction with the loading of the SW for execution. Local procedures in the NEs may also perform version compatibility checks before attempting a load or execution. These matters are not considered applicable to the standardisation of SW management in this ETS.

7.2.2.2 Transfer the software to the network element

It may be required to transfer the SW by means of communication over the NE management interface. This can be achieved by using file transfer mechanisms with a specific file designator of "SW". The transfer of the SW file(s) will be under the control of the manager, while the actual mechanisms to be employed for local storage will be under the control of the agent. For more detailed information on the specific technique to be employed refer to GSM 12.00 [10].

Other transfer methods may be applicable depending on the use of access devices local to the NE (e.g. by means of a local maintenance terminal, whether this is connected directly or by means of a remote communications link). These procedures are not the subject of standardisation in this specification. However, it is important that the managing system is informed of local actions which affect the loaded and/or executing SW.

7.2.2.3 Identification of the software package

Both before and after the files which make up the delivery have been transferred to the target NE, it will be necessary to identify the SW version. This identification will take a number of forms, as follows:

- the identity of the component parts as supplied;
- the absolute identity of the SW version as defined by the creator of the delivery;
- a designator for the role of the SW as to be used in the system.

These forms of identity will enable the operator to maintain a (potential) library of SW versions which may support various configurations and requirements.

The role of the SW may be indicated as a function of the NE (or component) on which it is to be loaded. Four roles are considered. These are:

- **running:**
  this is the SW version which is currently executing on the NE (or component);
- **back-up:**
  this is the SW version which is to be executed if the running version fails and a reload is required. The reloading may be manually or automatically executed;

  NOTE: the degree or extent of a failure attributable to the SW load itself which causes the "back-up" version to be loaded and executed will be an implementation matter and not a subject for this standardisation. If the failure causes a corruption of the locally executing code version of the SW then the "back-up" version should be used.

- **new:** this is a SW version which is to be loaded under, possibly, controlled conditions. The designation 'new' in this description is not to infer that the version is necessarily a new version as delivered from the manufacturer but that it is newly introduced to the NE. The extent and scope of failure tolerance when a 'new' SW version is executing (i.e. is also the 'running' version) may vary on a manufacturer or Operator basis;
- **fall-back:**
  this is a version of the SW which is considered to be well tested and reliable and one which can be loaded if problems with the current version are found to be intolerable. The usefulness of this designation in practice will depend on the compatibility of successive SW releases with the supporting technology and data values (and data formats). The designation of a SW version as fall-back, and the initiation of its load and execution, will be under operator control.

7.2.2.4 Construct a loadable form of the software

The transfer of files (either electronically or manually) to the NE may or may not deliver the entire SW load package depending on the structure of the delivered SW. If the whole package is comprised of a number of components then these will be associated within the NE in order to produce a coherent entire load (if this is necessary). The whole package will then need to be manageable as a single entity.

The process of constructing the whole package may be achieved in a number of ways; the exact process is not a matter for this standardisation. If the association of multiple packages is supported under the control of a managing system then the agent shall support the necessary mechanisms.

7.2.2.5 Load the software and execute

It shall be possible for the managing system to control the execution of the SW in the agent system. Whether the level of management is able to be exercised on a processor, sub-assembly or sub-system basis will be determined by the implementation. The management controls shall include:

- **disable:** the SW is stopped from executing;

- **initialise:** the SW is loaded from local storage and begins execution from the entry point (typically after having first been disabled);

- **restart:** the SW is stopped and restarted from the entry point;

- **reset:** the SW is stopped, reloaded from source and restarted (this is a combination of disable and initialise).

The extent of the management action to be executed will depend on the target object within the relevant object hierarchy to which the action is addressed as SW versions can be associated to a specific equipment or associated to a defined function, refer to GSM 12.20 [14].

7.2.2.6 Manage the local storage of software

It will be necessary, to preserve storage capacity in the NE, to be able to manage the storage capability local to the NE. Direct management of files held in a local file store is outside of the scope of this standardisation. It will, however, be possible to delete SW version identities. The SW version identity provides an indication of which 'files' belong to the software version. Deletion of the version identity may or may not delete the associated files, and so free the associated file space, depending on the implementation and the local management capabilities for file manipulation. If a file is to be deleted which is still referenced by a valid version identity, then the manager should be informed. (If 'files' are used in the composition of more than one SW version, their deletion will cause problems when these versions are requested to be executed.)

7.3 Logical configuration management

The third component of the configuration of a NE is the logical aspects. It is necessary to construct and maintain the data which characterises the specific use of the NE, both locally and in its relationship to other NEs. This is the data which describes the functional environment of the NE.

This subclause describes the general requirements for the management of this data.

7.3.1 Definition of logical configuration

The logical configuration, in the context of this specification, means the data - in terms of relationships and values - which describe the operational characteristics of the NE. Typically, this data represents the use to which the physical resources will be put and the operating constraints of the functionality.

7.3.2 Logical parameter management requirements

The data which is utilised by a NE can be classified, in terms of its ability to be managed, by its origin of definition. The origins can be:

- GSM-defined characteristics;
- other telecommunications function characteristics; or,
- network element-specific characteristics.

Some data elements will be manageable while others will be pre-defined by the manufacturer (and, therefore, not manageable in the context of this specification). This clause describes the general management function requirements for the management of data elements defined by GSM.

NOTE: These requirements may be equally applicable to the management of other data elements which describe other, related telecommunications functionality, e.g. the configuration of signalling system No. 7, but as the definition of these data elements is outside of the scope of GSM their management cannot be defined in the 12-series. See also GSM 12.00 [10].

7.3.2.1 Create initial data elements and values

Typically, a single NE requires a large number of individual data elements to be established before it can perform the task for which it was designed. It should be possible to create the data elements (i.e. the definitions or locations within the required data structures) and set initial values. Each data element may be created individually through management action or be provided in bulk form to the NE.

Bulk provision may be by means of a file transferred from a managing system. The file may represent the actual data structures (i.e. a database) or contain a set of data element creation management commands.

Requirements related to the loading of the data elements and values locally to the NE are outside of the scope of this specification.

In order to maintain data consistency between the manager and agent systems, it is required that NEs report the successful and unsuccessful creation of the data elements. In addition, the manager can request the information - through individual read requests or a database "audit" mechanism - as appropriate.

7.3.2.2 Modify data values

Changes to the logical configuration will require modifications to be made to the values of the data elements present in the NE. Changes may be necessary to single data elements or to multiple data elements as part of a single change operation, depending on the nature of the change action to be performed. General requirements, for the control of data modification, are summarised as follows:

- the manager needs to be informed of the success or otherwise of any requested change;
- if the change involves the modification of multiple data elements, the manager needs to be informed of the success or failure of the whole change operation;
- modifications to data values shall be checked, when necessary, to be valid, e.g. within an allowable range of values or consistency with other data elements;
- validity checks may be performed either in the manager application, the protocol machine or the agent application, depending on the circumstances;
- the agent should be aware when multiple change commands form part of a single operation so as to synchronise the change and to allow a degree of inconsistency to exist while the whole change is being performed.
- notifications of failures to modify data values should describe accurately the reason for the failure;
- if a failure to modify a data value occurs when more than one modification has been requested in a single change operation, mechanisms shall exist to recover the original data values and re-establish data integrity within the NE; if data integrity cannot be maintained, the agent system shall report the discrepancy to the manager;
- modifications to data values may be rejected by the agent system if the change to the particular data element is defined as requiring a particular condition (or state) to apply to the NE before the change will be allowed;
- changes to data values made locally, either autonomously by the agent or through local operator intervention shall be reported to the managing system;
- in a multiple manager system environment, changes to data values made by one manager shall be reported to all other managers where that data element is represented in the relevant management information model (it is not necessary that the new value is reported to the manager which requested the change independently from the notification of the success of the change).

7.3.2.3 Delete data elements

Changes to the configuration of the NE may require that certain data elements are removed from the containing data structure. It shall be possible to delete these data elements in a consistent and predictable manner. Where dependencies exist between data elements, it shall be possible either to allow all related data elements to be deleted using a single change command from the manager or to reject the delete request until all dependent data elements have been first deleted.

Any specific environmental conditions (e.g. the NE removed from service from the mobile user population) which may be required before a delete can be effected will need to be checked before the delete can be allowed to proceed.

7.3.2.4 Read data values

It shall be possible for a manager system to retrieve data values from an agent on demand. This process may require the retrieval of a single data value, multiple values for a single system aspect, single values across multiple system aspects or multiple values for multiple system aspects.

All reports of values supplied by the agent system shall identify the data element being reported, the current obtained value or a failure reason if the request was unable to be fulfilled.

If the volume of data requested by the manager system exceeds that which is considered to be suitable for transfer across the management interface as a message, the manager may request and the agent may agree to provide the required information in a bulk transfer of the data. The agent is responsible for notifying the manager of the readiness of the bulk transfer.

7.3.3 Logical functionality management requirements

There are some functions which characterise GSM which are optional. This optionality may be of the form that it can be optionally supported by a PLMN Operator. This implies that it may or may not be supplied by the manufacturer, depending on the requirements of the Operator. Secondly, it may take the form of being mandatory to be supplied but optional in its use. For example, a particular facility may be intended to assist in providing additional capacity in densely populated areas - urban environment - but is of little or no value in low density areas - rural environments. The PLMN Operator should, therefore, have the ability to control the availability and use of such functionality depending on the local environment and use of the NE concerned.

This clause looks at the requirements necessary to manage the functional configuration of a NE (concentrating on the BSS) for those functions which characterise GSM.

NOTE: As before, these requirements may be equally applicable to other functionality but their use in that context is outside of the scope of the 12-series specifications to define.

The properties which characterise the logical functionalities of a GSM BSS can be formed into functional groups like Power Control, Handover Control etc. In order to control and influence the functional behaviour of the BSS, during initialisation and its lifetime, it should be possible to manage control algorithms, processing, comparison and decision making parameters.

The following groups are defined to provide control over the BSS functionalities:

- Cell Configuration Management Function;
- Adjacent Cell Configuration Management Function;
- Power Control Management Function;
- Handover Control Management Function;
- Frequency Control Management Function;
- Protocol/Timer Control Management Function;
- Functional Building Block Management.

For each of these management functionalities the parameters as defined in the GSM core specifications are identified as being modifiable by the PLMN operator (refer to subclauses 7.3.3.3 to 7.3.3.9 for further details).

NOTE: GSM defines a basic handover algorithm and RF power control process. The manufacturer has the option of extending these basic algorithms hence the management of these parameters is implementation dependent. In this case, it is the manufacturers responsibility to ensure that the data is manageable from an OS.

7.3.3.1 Enabling functionality

If the system allows the enabling of a previously disabled functionality then this shall be possible by means of management action. The context for the enabling will depend on the specific functionality. Whether existing users of the system will commence using the new functionality during the current use of the system will depend on the implementation. For example, enabling encryption on the air interface of a BTS may only affect subsequent call starts; existing calls will remain unencrypted.

If enabling a functionality is likely to cause disturbance to existing call traffic then the system should be removed from service prior to its being enabled and returned to service subsequent to the enabling operation completing.

7.3.3.2 Disabling functionality

If the system allows the disabling of a previously enabled functionality then this should be possible by means of management action. The context for the disabling of a functionality will depend on the implementation. Any effect on existing users of the functionality should be considered before invoking the disable operation.

Defence mechanisms may be employed to ensure that all existing users of the functionality have stopped use before the functionality is disabled. These defence mechanisms may include preventing any new use of the functionality while allowing existing use to continue until a natural conclusion or removing all traffic from the affected NE before performing the disable operation. The particular choice of mechanism will depend on the likely disturbance which may be caused to user traffic.

7.3.3.3 Cell configuration management function

Cell CM is concerned with the management of data which determine the operating characteristics of the cell.

Cell CM will consist of:

- (re-)defining cell identification and location area of the cell;
- (re-)defining the set of radio frequencies allocated and available to a cell;
- (re-)defining the receiver RF signal strength hysteresis, (CELL_RESELECT_HYSTERESIS), required for cell reselection as defined in GSM 05.08 [6];
- (re-)defining the Network Colour Code for an accessing MS, refer to GSM 05.08 [6];
- (re-)defining the properties of the common control channels of the cell;
- (re-)defining threshold and control parameters for RACH measurements as defined in GSM 08.58 [9];
- (re-)defining radio link timers, (RADIO_LINK_TIMEOUT), to detect radio link failures, refer to GSM 05.08 [6];
- (re-)defining the minimum received level at the MS required for access to the cell, (RXLEV_ACCESS_MIN), refer to GSM 05.08 [6];
- (re-)defining the maximum transmit power level a MS may use when accessing the cell, (MS_TXPWR_MAX_CCH), refer to GSM 05.08 [6];
- (re-)defining the number of TDMA frames reserved for the Access Grant channel during a multiframe, (BS_AG_BLKS_RES), refer to GSM 05.02 [4];
- (re-)defining the number of multiframes between two transmissions of the same paging message to mobiles of the same paging group;
- (re-)defining whether the IMSI attach/detach procedure and call re-establishment is used in the cell, refer to GSM 04.08 [3];
- (re-)defining whether a MS may camp on a cell, (CELL_BAR_ACCESS), refer to GSM 05.08 [6];
- (re-)defining access class barring, (Access Control Class), refer to GSM 04.08 [3];
- (re-)defining the availability of DTX downlink or uplink mode as defined in GSM 04.08 [3];
- (re-)defining the interval for the MS periodic location updates;
- (re-)defining the logical channel combination mapped onto the physical channel, refer to GSM 05.02 [4];
- (re-)defining the training sequence code of a radio channel;
- (re-)defining the effective transmit power of the carrier, refer to GSM 05.05 [5];
- other related items for further enhancements of future phases.

7.3.3.4 Adjacent cell configuration management function

This group is concerned with the management of data which affects the adjacency control within a NE in a manufacturer independent way.

Adjacent Cell CM will consist of:

- identification of adjacent cells for both handover and reselection purposes;
- (re-)defining reselection related, adjacent cell specific parameters, i.e. the ARFCN of the BCCH channel, see GSM 04.08 [3] and GSM 05.02 [4];
- other related items for further enhancements of future phases.

7.3.3.5 Power control management function

This group is concerned with the management of data which affects the RF power control usage within a NE. The implementation of RF power control in the MS is mandatory, whereas RF power control may optionally be implemented in the BSS as specified in GSM 05.08 [6]. Measurement processing, threshold comparison and decision making are allowed to be configured to take place either in the BTS or in the BSC.

Power control management will consist of:

- (re-)defining maximum and minimum threshold values for such items as signal strength and signal quality on uplink and down link, as defined in GSM 05.08 [6];
- (re-)defining power control parameters for processing, comparison and decision making sufficient to manage the example algorithm in the Annex A of GSM 05.08 [6] or the management of operator or vendor specific algorithms;
- (re-)defining the location where measurement processing, threshold comparison and decision making for power control is supported to take place, see GSM 05.08 [6];
- (re-)defining the support of the optional BS RF power control process, see GSM 05.08 [6];
- other related items for further enhancements of future phases.

7.3.3.6 Handover control management function

This group is concerned with the management of data which affects the handover control within a NE. Measurement processing and threshold comparison are allowed to be configured to take place either in the BTS or in the BSC.

Handover control management will consist of:

- operations to enable/disable the allowed optional BSS handover types, as described in GSM 08.08 [7];
- operations for forced handovers to clear a TRX or BTS;
- (re-)defining maximum and minimum threshold values for such items as signal strength, signal quality and interference level on uplink and downlink as defined in GSM 05.08 [6];
- (re-)defining the maximum permitted absolute distance between MS and serving BTS ;
- (re-)defining parameters to be used to prevent repetitive handovers between adjacent cells;
- (re-)defining priority levels of adjacent cells for handover;
- (re-)defining the maximum transmit power level a MS may use in the specified adjacent cells;
- (re-)defining the minimum required received power level for the specified adjacent cells;
- (re-)defining handover control parameters for processing, comparison and decision making sufficient to manage the example algorithm in the Annex A of GSM 05.08 [6] or the management of operator or vendor specific algorithms;
- (re-)defining the location where measurement processing and threshold comparison for handover determination is supported to take place;
- other related items for further enhancements of future phases.

7.3.3.7 Frequency control management function

This group is concerned with the management of data which affects the radio frequency control within a NE in a manufacturer independent way.

Frequency control management will consist of:

- (re-)defining the frequency band used by the BCCH;
- (re-)defining the ARFCN(s) that the carrier uses;
- (re-)defining the set of radio frequencies allocated and available to a cell (CA) and to a hopping group (MA);
- (re-)defining the order in which the allocated frequencies are to be used (HSN);
- (re-)defining the values of the index offset (MAIO) which the hopping physical channels on the same time slot with the same MA and the same HSN shall use;
- operations to perform a dynamic modification of the radio definition of a BTS. These operations are optional. They are used on-line for frequency redefinition and modification of any other parameter which gives the frequencies related to the channels;
- other related items for further enhancements of future phases.

7.3.3.8 Protocol/timer control management function

This group is concerned with the management of data which affects protocol and timer control within a NE in a manufacturer independent way.

Protocol/Timer control management will consist of:

- (re-)defining maximum queue lengths if queuing is implemented;
- priority handling in queues if queuing is implemented;
- (re-)defining maximum values for such items as the maximum time a handover/call attempt may wait for a traffic channel to be released, if queuing is implemented;
- (re-)defining BSSMAP timers as defined in GSM 08.08 [7];
- (re-)defining LapDm timer (T200) to be used on the different control channels as defined in GSM 04.06 [2];
- (re-)defining Layer 3 timers (T31xx) to be used on the air interface as defined in GSM 04.08 [3];
- other related items for further enhancements of future phases.

7.3.3.9 Functional building block management

This group manages the functional building blocks as defined by GSM 08.52 [8] (e.g. BTS, BSC, TRX, ...) and is concerned with the handling of data, state and mapping information which is necessary to manage the BSS.

Functional Building Block Management will consist of:

- (re-)defining, for a particular functional building block, the maximum and minimum number of blocks allowed in the BSS;
- (re-)defining the relationships between functional building blocks i.e. how the operation of one part of a system affects the operation of another part;
- (re-)defining whether a functional block can be switched on or off, e.g. LOCK or UNLOCK a BTS;
- (re-)defining user-friendly functional block names and/or locations if appropriate;
- (re-)defining relationships between the functional block, the real physical equipment and the SW package;
- other related items for further enhancements of future phases.

7.4 Modelling notes

General guidelines on the definition of a management information model using object oriented techniques are described in GSM 12.00 [10] and other publications.

The object model which supports the CM of the BSS is defined in GSM 12.20 [14]. The requirements described in the preceding subclauses can be modelled in a number of different ways depending on the overall objectives of the model and the consideration of the dependencies between data elements being modelled.

Data elements which describe the operating environment of the BSS or a component functionality will normally be modelled as attributes of managed object classes. The managed object classes may represent functionality, or groups of related functionalities. Control of the functions may be modelled either as an inherent behaviour of the object class or as a modifiable attribute (or set of attributes) contained within the object class.

Each characteristic of the BSS, defined by GSM to be manageable, should be included in the management model. The concept of optionality, as described previously, also needs to be taken into account.

Annex A (informative): Examples of management procedures

The scenarios given for the Network and NE Management Examples will follow a set of basic rules:

- the descriptive methods employed are derived from "Petri Nets":
  one distinguishes actions (drawn as box or bar) and processing conditions (circles) which are input or output conditions; the process sequence is driven using tokens, those left over in a scenario will disappear when the scenario (process) is finished properly (deleted); the process modelled through a Petri net follows certain rules:

  - all input conditions shall to be completed/fulfilled before the next action;
  - when an action is completed, it will complete all output conditions with tokens (actions can produce and delete tokens);
  - the token flow models the timing sequence for the process;
  - Petri nets therefore allow parallel, partly independent processes which require synchronisation at a particular point in time to be expressed within a mathematical model;
  - the scenario will end when all those conditions without follow-up actions will contain a token;
  - the end of a scenario is reached when all tokens are in conditions without any following action;

- the level of detail is down to self-contained actions as "SHUT_DOWN" or "UNLOCK".

Whenever "severely affected NEs/NRs" are referred to, the reader should bear in mind that there may be NEs/NRs in the network which are affected by a modification so that the telecommunication function cannot be supported properly anymore; but this is not necessarily true for all implementations or modifications.

The creation, deletion and conditioning of NRs can be further divided into modifications which directly affect the NE, for example the modification of a BTS, or modifications which indirectly affect the NE, for example the addition of a TRX to a BTS; These different types of modifications will require the management functions to be combined in different ways to achieve the required processes, as can be seen below.

A.1 Network element and network resource management examples

The scenario for Element Extension (subclause A.1.1) is explained in detail to provide a better understanding of the method.

A.1.1 Network resource creation scenario (TRX)

In case, a NR shall be enhanced by additional resources (e.g. a BTS is enhanced by an additional TRX), the physical and the logical installation of the new NR could be done independent of each other. The **example** presented allows to:

- completely separate the logical from the physical modification:

  - the logical re-configuration of the enhanced BTS can be processed only when the SHUT_DOWN was finished and the BTS reached the LOCKED state; the UNLOCK following the re-configuration can not be processed until all severely affected NRs were SHUT_DOWN and LOCK'ed for the needed modifications;
  - while in SHUTTING_DOWN the operator can decide to UNLOCK the BTS directly without modification; then the re-configuration is not allowed anymore until the BTS is SHUT_DOWN and LOCKED again;
  - the physical modification allows the extension/installation without disturbing the traffic on the network (hot insertion of equipment) and can be performed without the BTS being LOCKED and independently of the logical re-configuration;

- the process is only finished when both, logical and physical modifications are performed;
- when the operator has re-configured the enhanced BTS it is necessary to finish the process first until the next re-configuration can be performed on the enhanced BTS.

To give a clear view of what the scenario is showing, a "flow chart" is described which explains the token flow and the actions allowed to be performed (refer to Figure A.1). The enumerated conditions in the flow chart are used to give the momentarily reached state in the scenario. The sequence of the separated actions (e.g. "SHUT_DOWN the BTS to be enhanced") in the flow chart is not the only one possible, the actions could also be processed in a different sequence.

The flow chart is indicating in the first column the transition of the tokens from the input conditions to the output conditions. Second column is listing the input conditions which contain tokens after the transition and third column is listing all the actions, which can be performed next.

from condition/to condition	**completed conditions**	**actions ready to be performed**
start of Element Extension		
Start condition --> 0, 1, 14	0, 1, 14	affected NEs/NRs can be SHUT_DOWN;

0 --> 2, 6	1, 2, 6, 14	affected NEs/NRs can be SHUT_DOWN;
		physical extension can be performed;
		enhanced BTS can be SHUT_DOWN;

SHUT_DOWN enhanced BTS		

2 --> 5, 9	1, 5, 6, 9, 14	affected NEs/NRs can be SHUT_DOWN;
		enhanced BTS can be configured;
		enhanced BTS can be UNLOCK'ed (Operator command)
		physical extension can be performed

operator UNLOCK on enhanced and LOCKED BTS (put: 10)		
9, 10 --> 11	1, 5, 6, 11, 14	affected NEs/NRs can be SHUT_DOWN; physical extension can be performed;

5, 11 --> 2	1, 2, 6, 14	affected NEs/NRs can be SHUT_DOWN;
		enhanced BTS can be SHUT_DOWN;
		physical extension can be performed;

SHUT_DOWN severely affected NEs/NRs		
1 --> 3, 7	2, 3, 6, 7, 14	affected NEs/NRs can be re-configured; enhanced BTS can be SHUT_DOWN; physical extension can be performed;
physical extension is performed		
6 --> 13	2, 3, 7, 13, 14	affected NEs/NRs can be re-configured; enhanced BTS can be SHUT_DOWN;
enhanced BTS is SHUT_DOWN		
2 --> 5, 9	3, 5, 7, 9, 13, 14	enhanced BTS can be configured; affected NEs/NRs can be re-configured;
enhanced BTS is configured		
5, 9 --> 8, 12	3, 7, 8, 12, 13, 14	affected NEs/NRs can be re-configured;
7, 8 -- > 9	3, 9, 12, 13, 14	enhanced and configured BTS can be UNLOCK'ed; affected NEs/NRs can be re-configured;
affected NEs/NRs are re-configured and UNLOCK'ed		

3 --> 4	4, 9, 12, 13, 14	severely affected and LOCK'ed NEs/NRs can be UNLOCK'ed;
		enhanced and configured BTS can be UNLOCK'ed;

4 --> 15	9, 12, 13, 14, 15	enhanced and configured NE/NR can be UNLOCK'ed;
enhanced BTS is UNLOCK'ed (put: 10)		
9, 10 --> 11	11, 12, 13, 14, 15	enhancement of NE/NR can be finished;
finish enhancement of BTS and up-date OS accordingly		
11, 12, 13 --> 16	14, 15, 16	OS can be updated
14, 15, 16 --> end condition		Element Extension is finished

Figure A.1: Detailed flow chart on Network Resource Creation

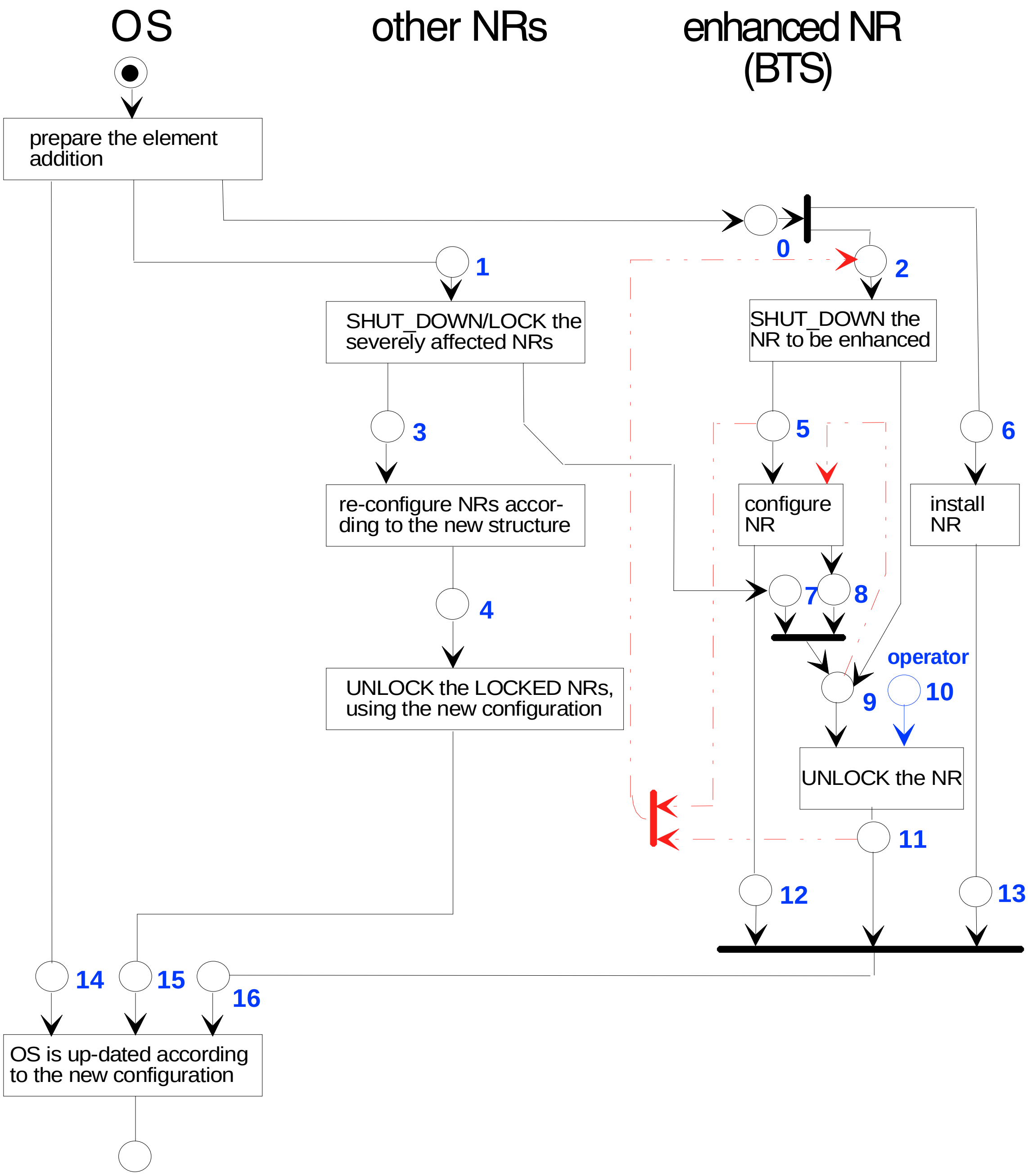
OS
other NRs
enhanced NR (BTS)
prepare the element addition
0
1
2
SHUT_DOWN/LOCK the severely affected NRs
SHUT_DOWN the NR to be enhanced
3
5
6
re-configure NRs accor-ding to the new structure
configure NR
install NR
4
7
8
operator
9
10
UNLOCK the LOCKED NRs, using the new configuration
UNLOCK the NR
11
12
13
14
15
16
OS is up-dated according to the new configuration

Figure A.2: Network Resource Creation (TRX)

A.1.2 Network resource creation scenario (BTS)

Whenever the operator decides to enhance the network by an additional NR, e.g. he is adding a BTS to a BSS, it is necessary to make the new BTS known to the already existing NRs. This can be done independently of the installation of the new BTS as it remains LOCKED until the complete installation is performed. The only synchronisation needed is when SHUT_DOWN and LOCK'ing is finished for all the severely affected NRs, before the new BTS is UNLOCK'ed. This is to prevent the network from data inconsistency and unexpected reactions on the new but still unknown BTS.

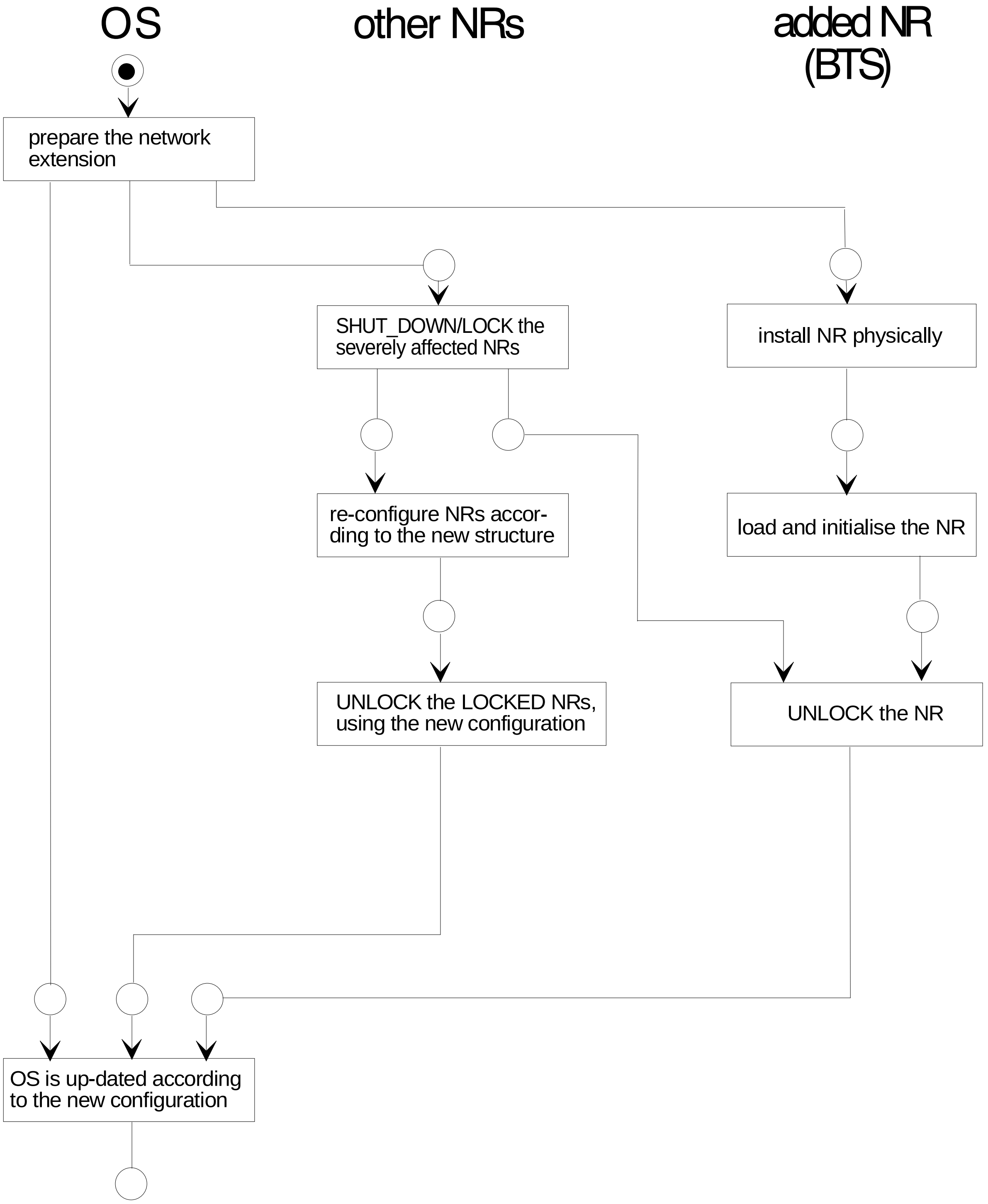
OS
other NRs
added NR (BTS)
prepare the network extension
SHUT_DOWN/LOCK the severely affected NRs
install NR physically
re-configure NRs accor-ding to the new structure
load and initialise the NR
UNLOCK the LOCKED NRs, using the new configuration
UNLOCK the NR
OS is up-dated according to the new configuration

Figure A.3: Network Resource Creation (BTS)

A.1.3 Network resource deletion scenario (TRX)

If it is necessary to minimise subscriber impact, the operator may reduce the capacity of an existing NR (e.g. remove a TRX from a BTS). The reduced NR shall be SHUT_DOWN and shall have reached the LOCKED state before the affected and re-configured NRs in the network are taken into service, this prevents the network from any inconsistency.

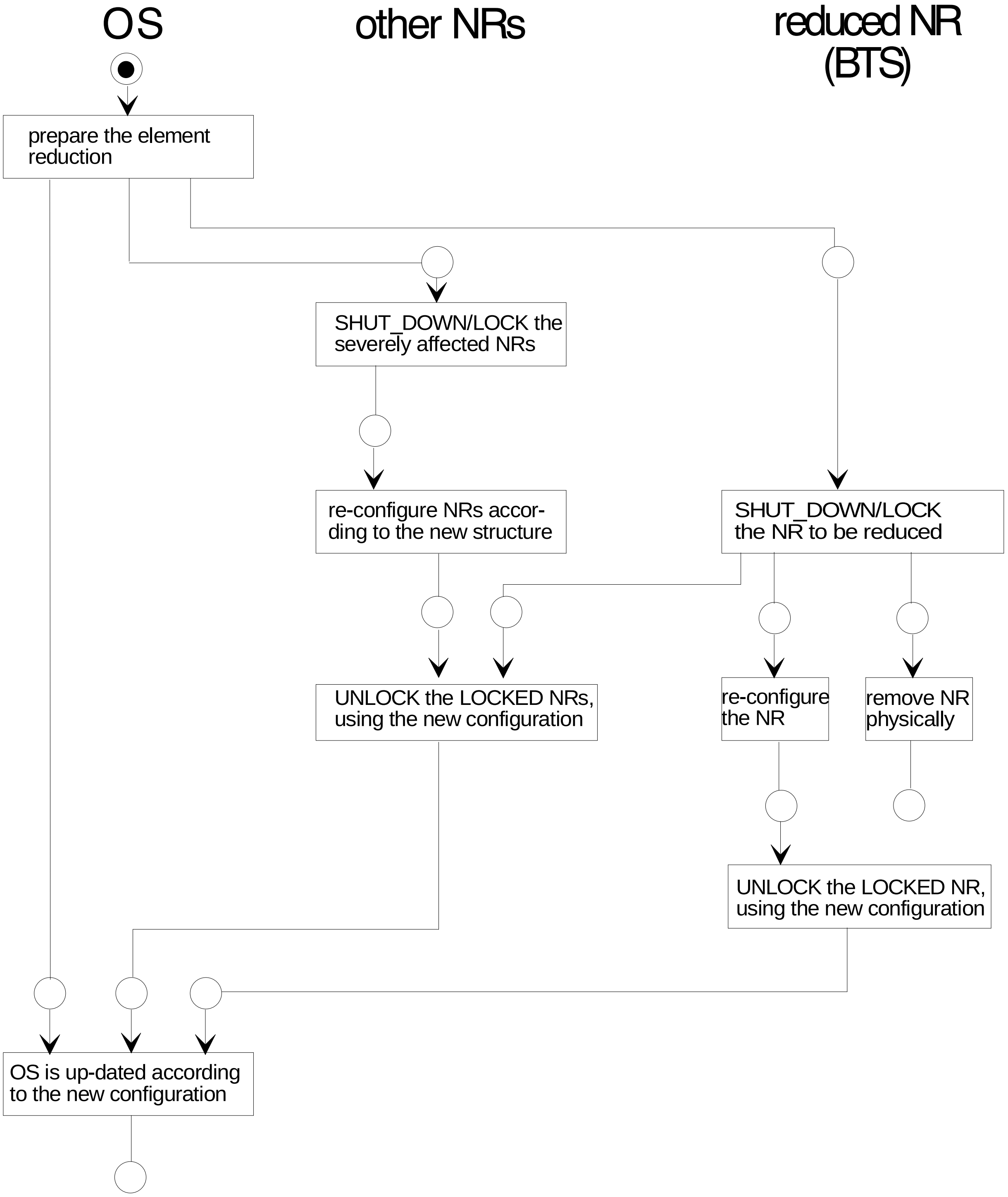
OS
other NRs
reduced NR (BTS)
prepare the element reduction
SHUT_DOWN/LOCK the severely affected NRs
re-configure NRs according to the new structure
SHUT_DOWN/LOCK the NR to be reduced
UNLOCK the LOCKED NRs, using the new configuration
re-configure the NR
remove NR physically
UNLOCK the LOCKED NR, using the new configuration
OS is up-dated according to the new configuration

Figure A.4: Network Resource Deletion (TRX)

A.1.4 Network resource deletion scenario (BTS)

To delete a NR from the network, e.g. he is deleting a BTS from a BSS, all severely affected NRs should be SHUT_DOWN/LOCK'ed before the re-configuration can be performed. The NR to be removed should also be SHUT_DOWN and have reached the LOCKED state before the severely affected NRs can be UNLOCK'ed.

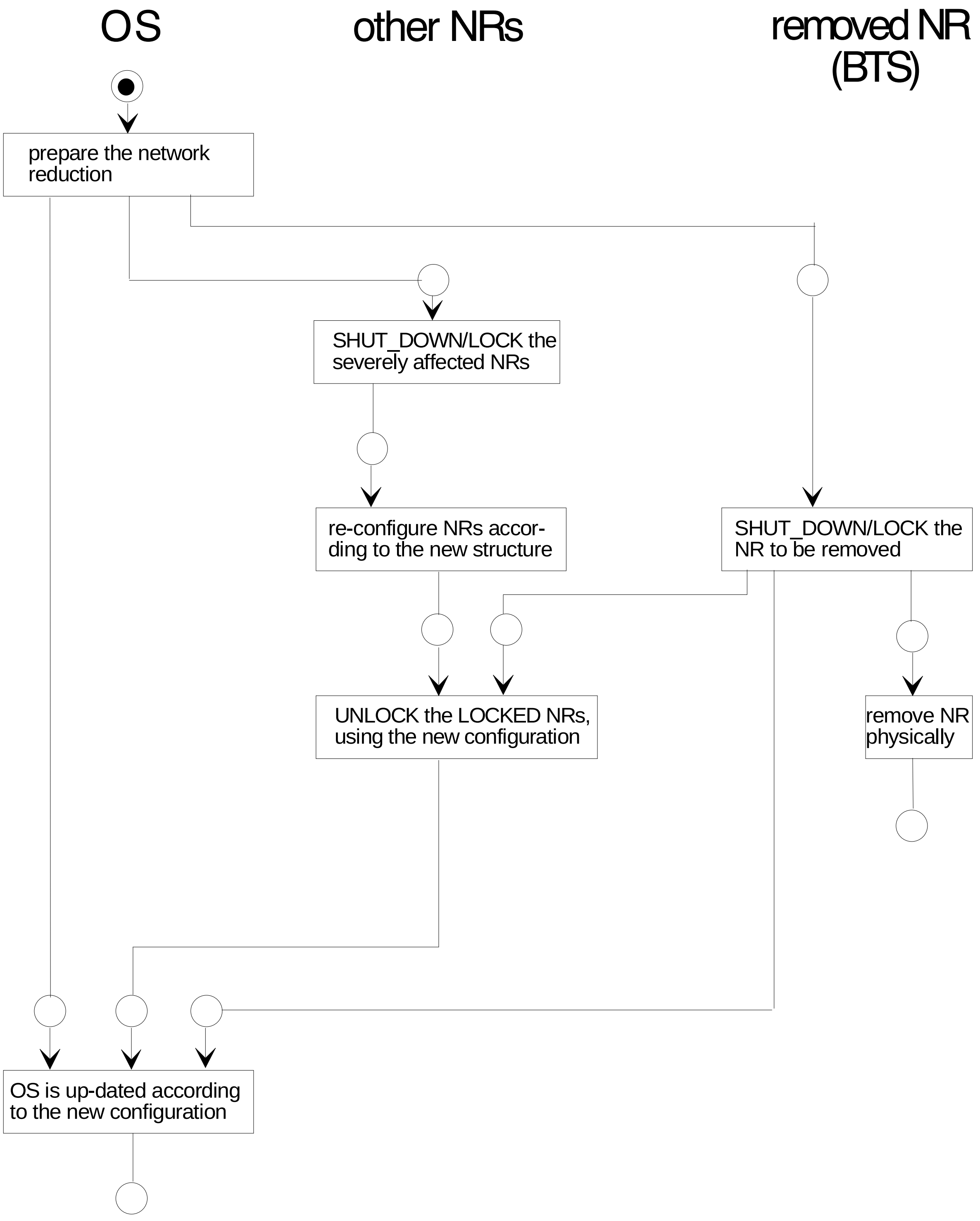
OS
other NRs
removed NR (BTS)
prepare the network reduction
SHUT_DOWN/LOCK the severely affected NRs
re-configure NRs according to the new structure
SHUT_DOWN/LOCK the NR to be removed
UNLOCK the LOCKED NRs, using the new configuration
remove NR physically
OS is up-dated according to the new configuration

Figure A.5: Network Resource Deletion (BTS)

A.2 Network element and network resource conditioning examples

A.2.1 Network element/network resource conditioning scenario without traffic impact

The operator may frequently modify telecom parameters which have no impact on the traffic carrying capability e.g. Layer 2 timers. This type of modification will not involve the SHUT_DOWN of the NE/NR concerned as the traffic is not affected.

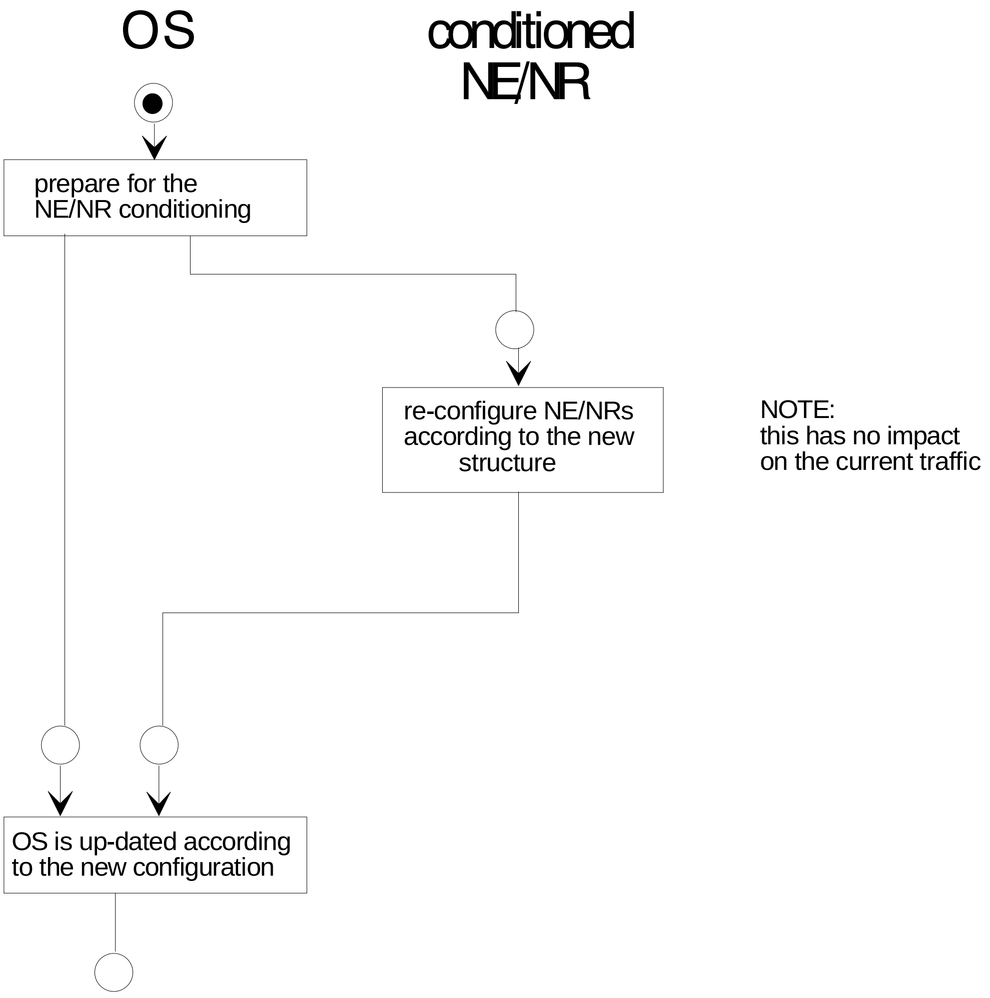
OS
conditioned NE/NR
prepare for the NE/NR conditioning
re-configure NE/NRs according to the new structure
NOTE: this has no impact on the current traffic
OS is up-dated according to the new configuration

Figure A.6: NE/NR Conditioning Scenario without traffic impact

A.2.2 Network element/network resource conditioning scenario with capacity impact

It may be necessary to modify data which affect the volume of allowable traffic without affecting existing traffic, for example, changing the state of the cell barring parameter. This type of modification will not involve the SHUT_DOWN of the NE/NR concerned as the traffic is not affected.

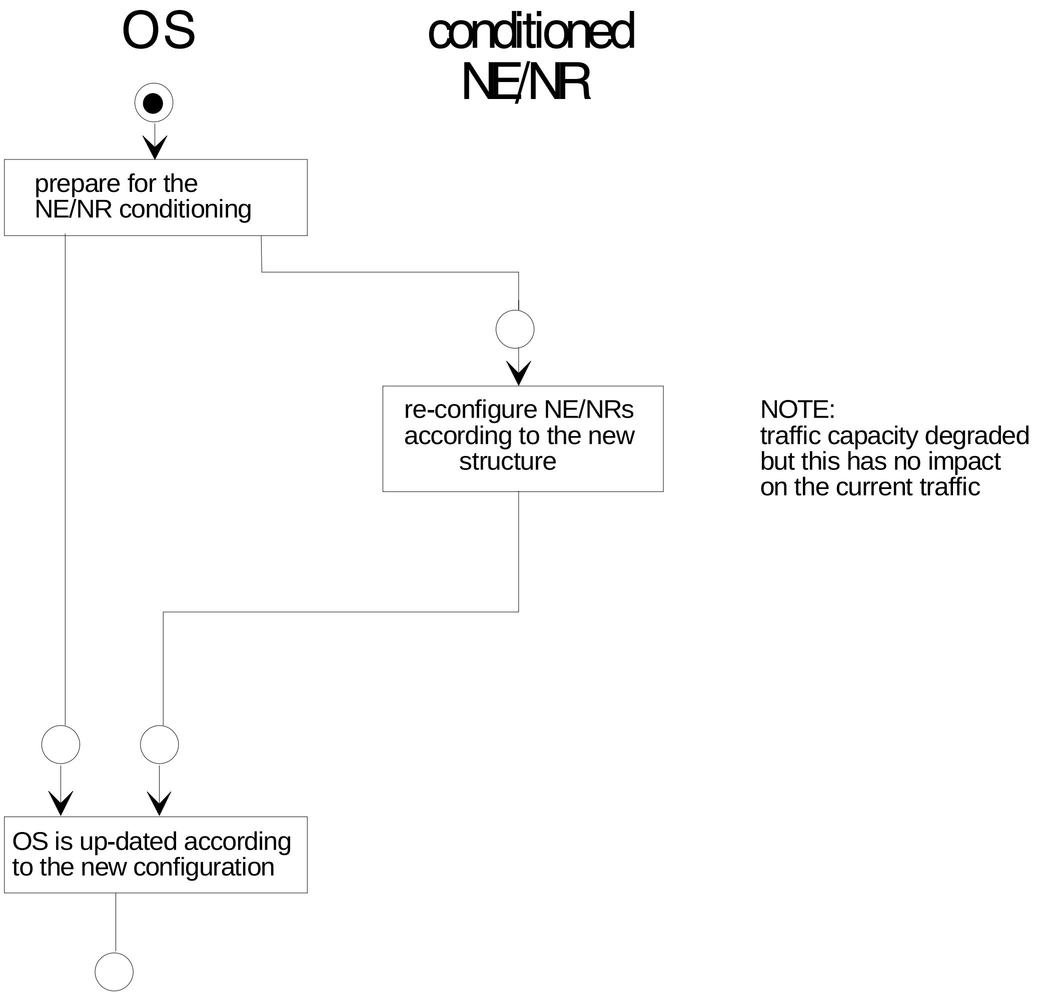
OS
conditioned NE/NR
prepare for the NE/NR conditioning
re-configure NE/NRs according to the new structure
NOTE:
traffic capacity degraded but this has no impact on the current traffic
OS is up-dated according to the new configuration

Figure A.7: NE/NR Conditioning Scenario with capacity impact

A.2.3 Network element/network resource conditioning scenario with traffic impact on one network element/network resource

Modification of SW, HW or data which affects part or all of a NE when traffic is expected to be affected will require the traffic to be removed from the NE before the re-configuration can occur.

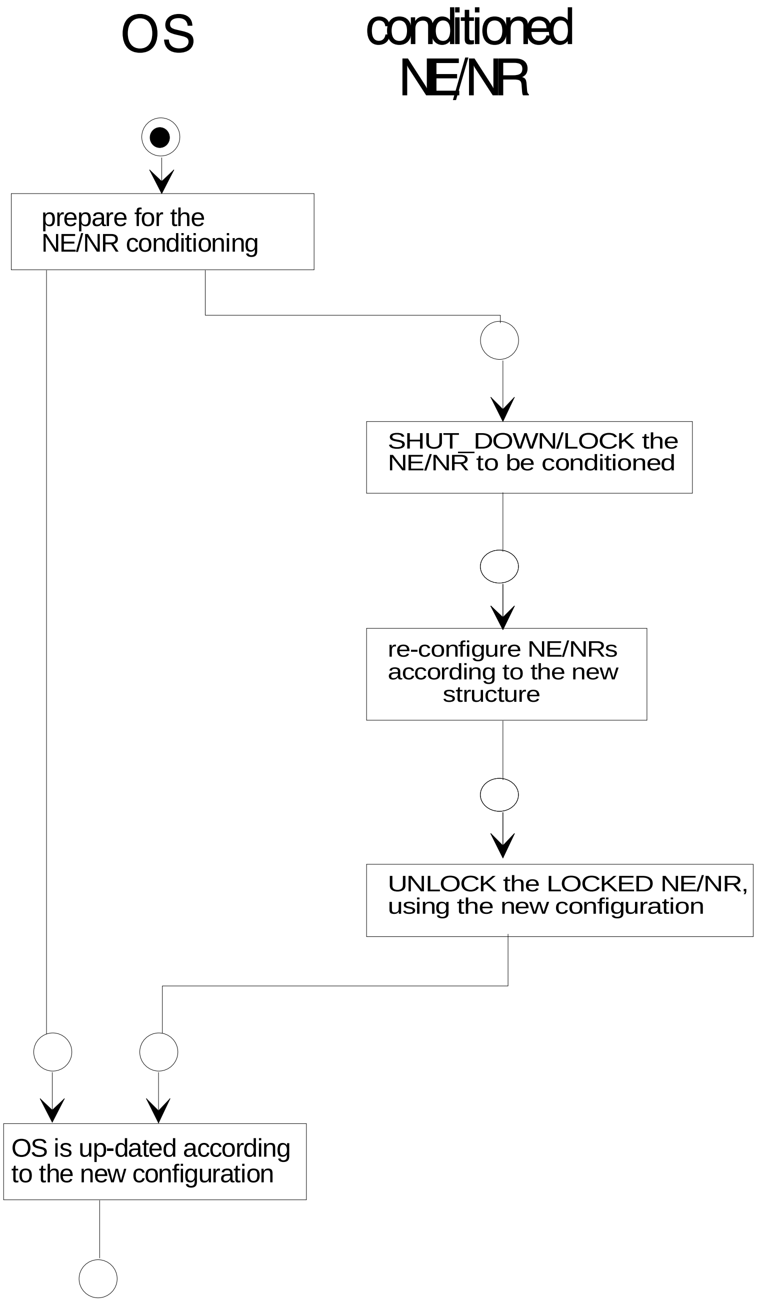
OS
conditioned NE/NR
prepare for the NE/NR conditioning
SHUT_DOWN/LOCK the NE/NR to be conditioned
re-configure NE/NRs according to the new structure
UNLOCK the LOCKED NE/NR, using the new configuration
OS is up-dated according to the new configuration

Figure A.8: NE/NR Conditioning Scenario with traffic impact on one NE/NR

A.2.4 Network element/network resource conditioning scenario with traffic impact on multiple network elements/network resources

Re-configuration which affects more than one NE will require the conditioned NE to be SHUT_DOWN before re-configuration can occur. The other affected NEs shall also be re-configured before the conditioned NE is UNLOCK'ed.

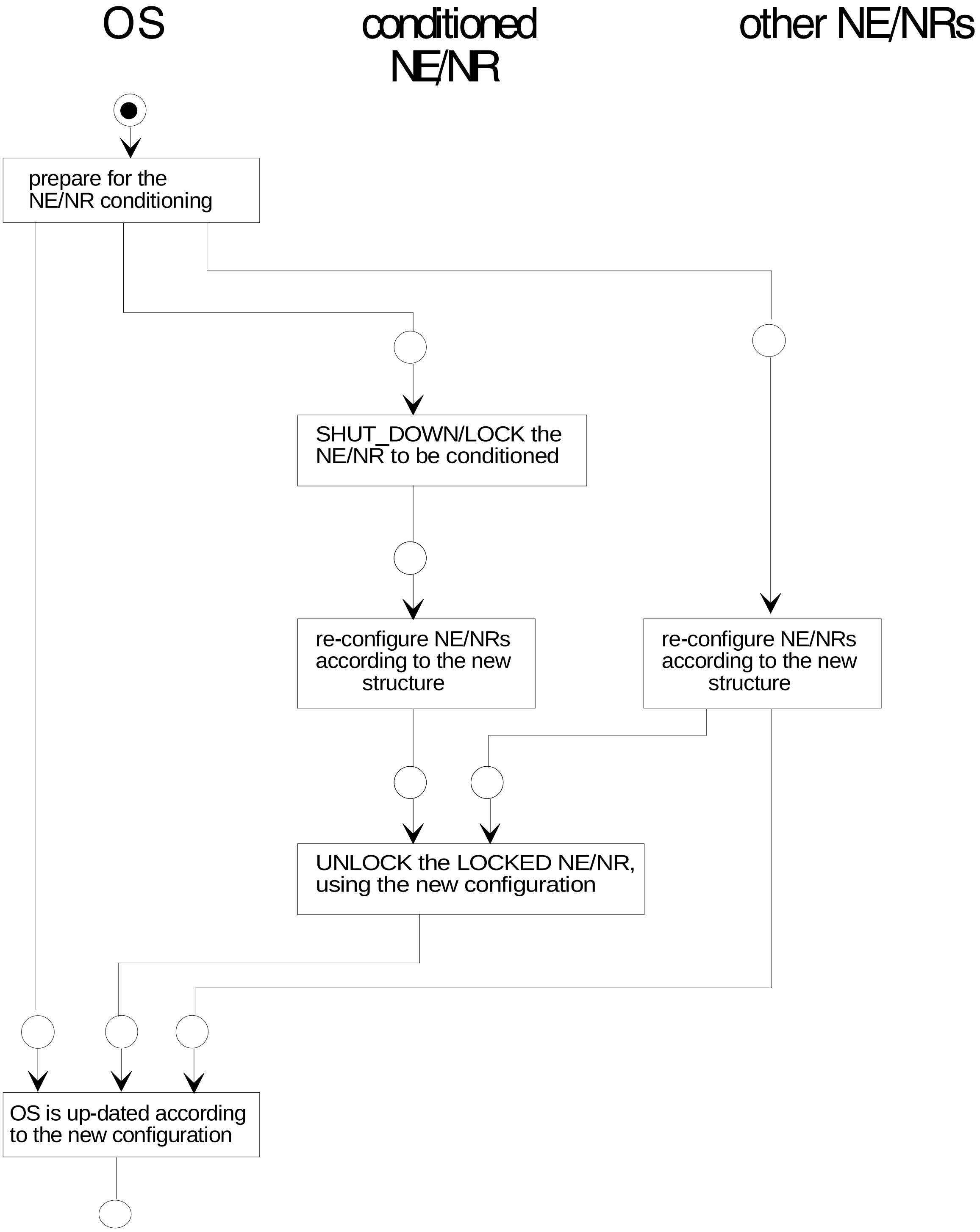
OS
conditioned NE/NR
other NE/NRs
prepare for the NE/NR conditioning
SHUT_DOWN/LOCK the NE/NR to be conditioned
re-configure NE/NRs according to the new structure
re-configure NE/NRs according to the new structure
UNLOCK the LOCKED NE/NR, using the new configuration
OS is up-dated according to the new configuration

Figure A.9: NE/NR Conditioning Scenario with traffic impact on multiple NEs/NRs

Annex B (informative): Bibliography

1) CCITT Recommendation. M.3010: "Principles for a Telecommunications Management Network (TMN)".

2) CCITT Recommendation. M.3020: "TMN Interface Specification Methodology".

3) CCITT Recommendation. M.3100: "Generic Network Information Model".

4) CCITT Recommendation. M.3200: "TMN Management Services".

Annex C (informative): Register

History

Document history		
July 1995	Public Enquiry	PE 87: 1995-07-10 to 1995-11-03
March 1996	Vote	V 100: 1996-03-25 to 1996-05-17