TSG-RAN Working Group 3 meeting #6
23rd – 27th August 1999, Sophia Antipolis

TSGR3#6(99)822

Agenda Item: x

Source: Editor

Title: I3.05 –Node B O&M Functional Description v 0.2.1

Document for: Approval

This document summarises the changes agreed at RAN-WG3 meeting #5 in Helsinki. The changes agreed as per tdoc 99601 have been incorporated, and the working assumptions taken as a result of tdocs 99704 and 99775 included as change bars. Other minor editorial changes are also shown as change bars, as detailed in the document history.

TR I3.05 V<0.2.1> (<1999-07>)

Technical Specification

3rd Generation Partnership Project (3GPP);
Technical Specification Group (TSG) RAN;

Node B O&M Functional Description

3GPP

Reference

<Workitem> (<Shortfilename>.PDF)

Keywords

<keyword[, keyword]>

3GPP

Postal address

Office address

Internet

secretariat@3gpp.org
Individual copies of this deliverable
can be downloaded from
http://www.3gpp.org

Copyright Notification

Contents

Intellectual Property Rights

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project, Technical Specification Group RAN.

The contents of this TR may be subject to continuing work within the 3GPP and may change following formal TSG approval. Should the TSG modify the contents of this TR, it will be re-released with an identifying change of release date and an increase in version number as follows:

Version m.t.e

where:

m indicates [major version number]

x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated into the specification.

Introduction

This technical report defines an O&M functional model for the Node B Radio Site. The purpose of this functional model is to ensure that the scope of O&M functions supported over the Iub interface is sufficient to allow a multi-vendor environment to be realised. To define this scope a proper understanding of the O&M functions performed at Node B is required. This will ensure that, in order to minimise the impact of O&M operations at Node B on the quality of service available, all O&M functions requiring functional interaction with the RNC are identified and the Iub interface specified accordingly.

Scope

The principle objective of the document is to provide supporting information for the Iub O&M work item. The actual specification work relating to the Iub interface O&M can be found in [1]. For this reason the document may contain information or working assumptions which are not a direct part of the aforementioned work item, but are essential to the progress and informed decision making. Where information or working assumptions are outside the scope of TSG-RAN-WG3, this shall be indicated.

References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] 25.433, NBAP Specification
[2] 25.401, UTRAN Overall Description
[3] 25.442, UTRAN Implementation Specific O&M Transport
[4] 25.432, UTRAN Iub interface signaling transport
[5] 25.426, UTRAN Iur and Iub interface data transport and transport signaling for DCH data streams
[6] 25.434, UTRAN Iub interface data transport and transport signaling for CCH data streams
[7] 25.832, Manifestations of Handover and SRNS Relocation
[8] X.721 (2/92) Information Technology – Open Systems Interconnection – Structure of Management Information: Definition of Management Information
[9] Q.821 (3/93) Stage 2 and Stage 3 Description for the Q3 Interface – Alarm Surveillance

Definitions, symbols and abbreviations

Definitions

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

Logical O&M shall be as defined in section 10.1.2 of [2]

~~1.2~~Symbols

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

⟶	NBAP Procedures
⟹	Implementation Specific O&M procedure
- - - -▶	Optional Procedures
=:=:=:=:=:	Conditional Procedures

~~1.3~~Abbreviations

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

UTRAN O&M

UTRAN O&M Overview

[Editors Note: The following text is included as a working assumtion as agreed at RAN-WG3#5]

Figure 5.1.1 below shows a typical configuration of the O&M systems for UTRAN part. The figure also identifies all the interfaces between various management systems and NE's.

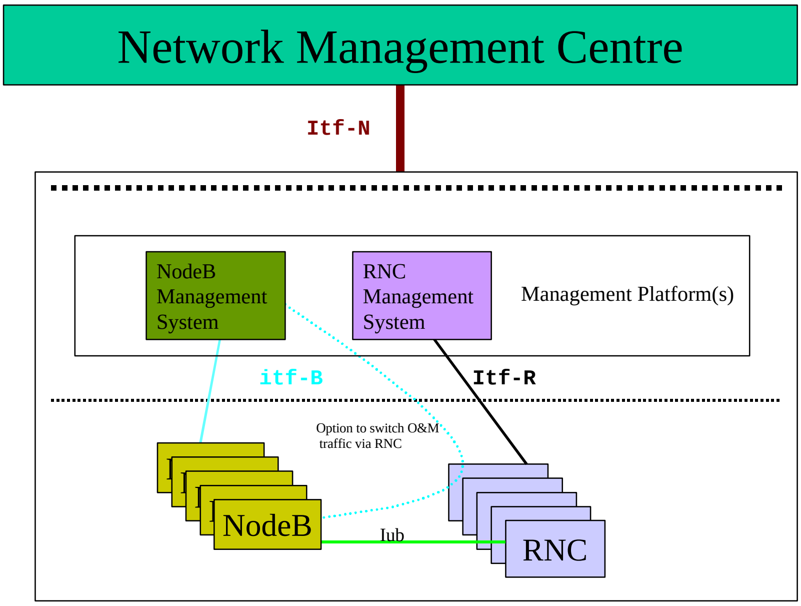


Figure 5.1.1: O&M Management Interfaces

The Management Interfaces are:

1. **Itf-B** - between NodeB & its Manager (physically, this may be a direct connection or via the RNC)
2. **Itf-R** - between RNC & its Manager
3. **Itf-N** – between Management Platforms & Network Management Centre

UTRAN O&M Procedures

This following list of UTRAN procedures should be used to derive requirements for the O&M functions of UTRAN elements, and to identify all information that has to be exchanged via Iub (i.e. NBAP messages) to provide the required functionality.

~~1.1.1~~Network Expansion Procedure

Network Expansion in general includes expansion of existing elements and integration of new elements. The most frequent expansion processes are:

Node B Expansion The Node B Expansion means a modification of several Node B parameters that are possibly provided by a previous planning process (see section 10.1.6).

Node B Installation Installation of a new Node B including setting of all required parameters. Additionally the Node B is attached to the appropriate RNC and all links are dimensioned accordingly. Possibly causes Expansion/Modification of adjacent Node B's. An automatic configuration with the download of all required, not vendor specific data can reduce the required effort significantly. One possible example of such a configuration process is ~~as follows:~~described in section 10.1.9.

- ~~After the physical installation of NodeB including all wired and wireless connections to RNC and/or Management System the signalling bearers for NBAP according to [4] and ALCAP according to [5] and [6] have to be established.~~

  ~~[Note: It is ffs whether the signalling bearers have to be established manually or whether an automatic establishment is possible.]~~

- ~~Following to the successful establishment of the NBAP signalling bearer the NodeB initiates it's configuration by sending a configuration request to the RNC.~~
- ~~Since the RNC knows the address of the new NodeB, the RNC establishes the signalling bearer intended for implementation specific O&M link from Node B to it's Management System (only in case of routing the implementation specific O&M signalling via the RNC).~~
- ~~The successful establishment of the implementation specific O&M signalling bearer is communicated to the new NodeB including all required addresses and interface descriptions.~~
- ~~The NodeB requests it's implementation specific and therefore manufacturer dependent initialisation from the Management System.~~

  ~~[Note: It is ffs. Whether the RNC can trigger the NodeB initialisation.]~~

- ~~After receiving the configuration request from the NodeB the vendor specific part of the Management System sends all required initialisation parameters to the NodeB.~~
- ~~The NodeB performs a self-test after the implementation specific configuration and sends a result report to the Management System and a Node B Healthy notification to the RNC indicating that the NodeB is ready to operate.~~
- ~~After receiving the Node B Healthy notification (following to the initial configuration request) the RNC send all required radio and cell parameters to the NodeB (including common channel setup data). These parameters must have been previously provided to the RNC from the management system.~~
- ~~The NodeB performs a self-test after the radio/cell configuration and sends a final result report to the Management System and a resource notification to the RNC indicating the successful radio/cell configuration.~~

~~When the RNC receives the notification that the NodeB is configured accordingly the RNC issues a BCH transmission begin notification.~~

Node B Swap In case of integration of a new RNC one or more Node B's are detached from neighbouring RNC's and attached to the new RNC. After configuration of the Node B and the new RNC and all according links the Node B is detached from the old RNC and operates connected to the new RNC. Possibly Node B expansion procedures are triggered in all affected Node B’s (in the neighbouring cells) (see section 10.1.7).

Cellular Network Configuration Procedure

Cellular network configuration processes deal with all modifications to network elements that have impact on the radio access network. For example parameters required for power management or synchronisation may be modified. A notification message to the according element indicating the planned configuration changes will be sent. However, both discreet message and file transfer methods should be supported for cellular network configuration, enabling the selected mechanism to be chosen dependent on the number of parameters to be configured. *(Editors note: The concept of configuration using file transfer is proposed for Implementation Specific O&M configuration only, the concept of file transfer for Logical O&M configuration is for further study).* If the modification requires a larger amount of data to be transferred than the notification message may contain only name and location of a required data file to be downloaded. Afterwards the affected network element(s) can integrate the supplied modifications and report the results of the performed parameter update. The element itself can choose the best time (in case of Node B in co-operation with the RNC) for the update according to it's current load, etc. (see section 10.1.3)

Remote Update Procedure

Remote Update Procedure includes the remote software update of all network elements. Within this update process also self-checks and consistency checks are included. A status request message asking for a response from the affected network elements with the current release number can avoid release conflicts during the update procedure. The update procedure itself can be implemented with pull or with push technologies. A notification message to elements indicating a new software release and the location of the required file could be used the trigger an automatic download of the new release (pull technology). Or, the responses of the status request messages can be used to compose a multicast message carrying the new software release to all affected elements (push technology). (see section 10.1.5)

Network Optimisation Procedure

In order to identify possible modifications that allow an improvement of the overall network performance this process type consists of the collection of measurement data and of the decision process to trigger network expansion and/or configuration procedures to optimise the network. Since expansion and configuration processes are handled separately the network optimisation process deals in this context only with the collection of measurement data. (see section 10.1.4)

Network Monitoring and Fault Management Procedures

In addition to performance measurements collected in the network optimisation procedure this process observes the status of network elements and handles alarm and event notifications. Additionally customer complaints are considered. (see section 10.1.8)

Node B O&M Management Architecture

The working assumption for the Node B O&M management architecture is described in section 10.1 of [2]. This architecture defines two categories of O&M functions at Node B – Logical O&M and Implementation Specific O&M. Logical O&M functions are supported over the Iub interface – see section 10.1.2 of [2]. It should be possible to route the Implementation Specific O&M via the same physical bearer as the Iub interface – see section 10.1.1 of [2], where the transport layer for this scenario is specified in [3].~~0~~

O&M Functional Overview

~~The diagram~~Figure 6.1 below presents a high level functional model of the O&M operations for the Node B radio site. This model should be viewed as logical in nature, it attempts only to identify those categories of functions essential to the operation and maintenance of a generic Node B. The diagram below should not be interpreted as a physical implementation or an exhaustive functional list.

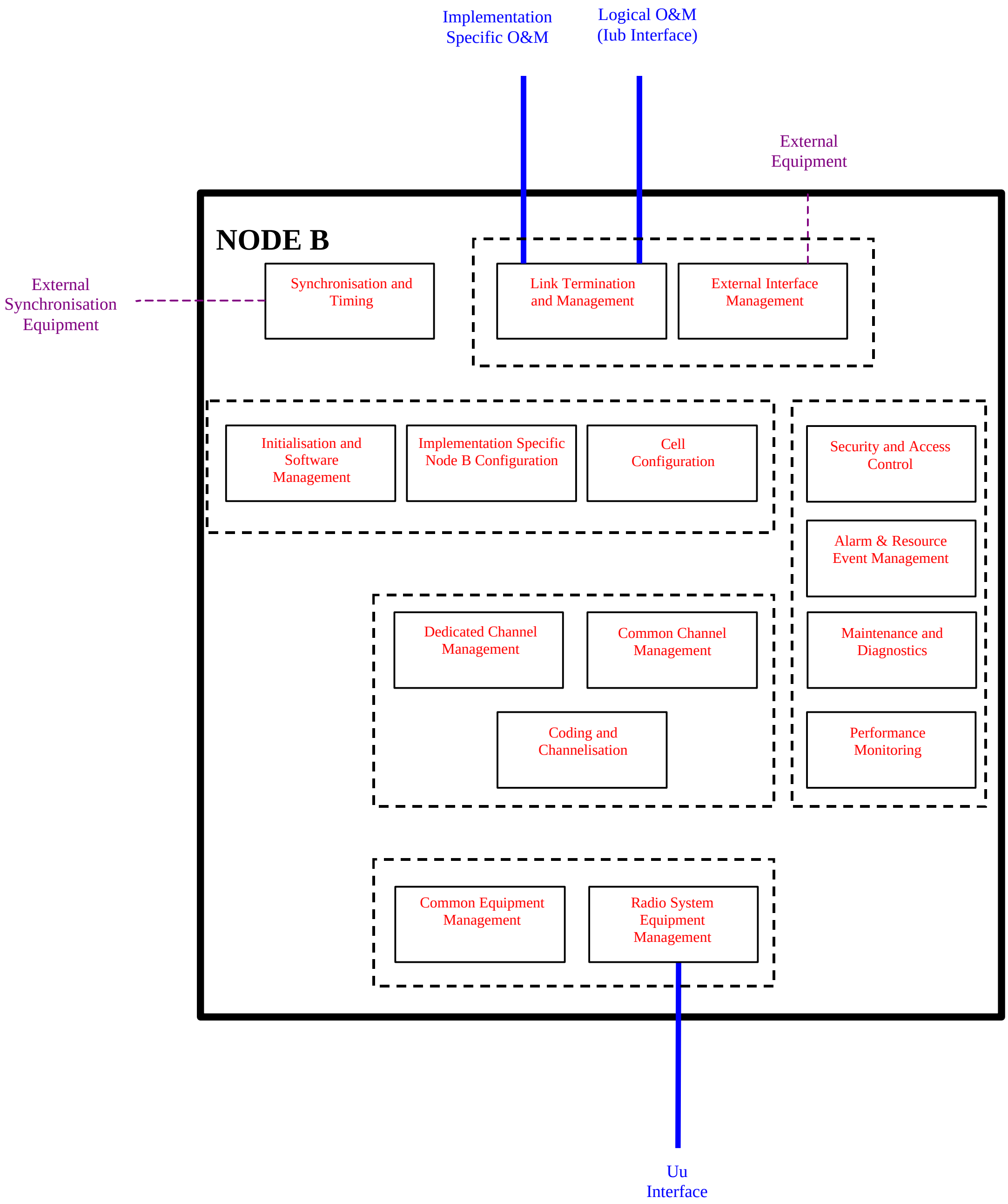

Implementation Specific O&M
Logical O&M (Iub Interface)
External Equipment
NODE B
External Synchronisation Equipment
Synchronisation and Timing
Link Termination and Management
External Interface Management
Initialisation and Software Management
Implementation Specific Node B Configuration
Cell Configuration
Security and Access Control
Alarm & Resource Event Management
Maintenance and Diagnostics
Performance Monitoring
Dedicated Channel Management
Common Channel Management
Coding and Channelisation
Common Equipment Management
Radio System Equipment Management
Uu Interface

Figure 6.1: Node B O&M Functional Model

[Note] The Logical O&M (Iub interface) and Implementation Specific O&M interface are represented above as logically independent interfaces. It should be possible to route both the Iub interface and Implementation Specific O&M interface either independently or via the same physical bearer.

Functional Descriptions

This chapter presents the functional descriptions for the elements of Node B O&M proposed in section ~~5~~ 6 above. The descriptions below shall be interpreted as informative only, their purpose being to assist in a proper understanding of each function. The functional descriptions presented should not be considered exhaustive.

~~1.1~~Initialisation and Software Management

This function will initiate and control all aspects of software management for the Radio site, from initial downloading to intra node software distribution. The function shall support a range of defined processes, from site initialisation and new software loading to software distribution and correction management/fault isolation. The process of software downloading can either be performed in a non-service affecting way (background operation), or it may require the Node B to release some or all of it's traffic. For the latter case, any interruption to traffic must be performed in a controlled fashion,.

Also the actual process of initialising new software (following the download) is very likely to cause an interruption to traffic, and this must also be performed in a controlled fashion. The process of functional interaction of initialisation and software management is termed 'Software Initialisation'. The process of initiating and performing software management

~~1.2~~Link Termination and Management

NOTE: Inclusion of the following text is dependent on the RAN-WG3 decision relating to the suitability of IMA to perform this function.

This function shall deal with the management of the Iub interface and Implementation Specific O&M interface. This will address not only initial link establishment, but also the ongoing monitoring of link health, link recovery following a fault, and load sharing and distribution. The function shall also monitor layer 1/2/3 link performance and status, these being reported back to the RNC/management system as necessary via the appropriate interface, possibly first being processed by the performance monitoring function (see section 7~~6~~.5).

The link termination and management function should control any ATM switching (i.e. to cascaded equipment), and packetisation/de-packetisation of the incoming data from the Iub or Implementation Specific O&M logical interfaces. It should further manage the distribution of data internal to the Node B. This should also cover the communications from the external interface management function (section 7~~6~~.15), to report on the status of any external link management equipment that may be used.

It is important for the termination and management of the Iub to be supported in such a way as to allow the traffic handling to be optimised according to the link performance.

~~1.3~~Implementation Specific Node B Configuration

Whilst this function is passive with regard to service provision it is important from an operational perspective to have an accurate record of the physical configuration of the Node B radio site, combined with the ability to easily configure new hardware. This function should perform the detection and configuration (which should be automatic), of the Node B hardware. The function should further manage a database capable of storing the software and hardware configuration information to serial number/version resolution (i.e. replaceable unit level). It should be possible to interrogate this from the management system.

~~1.4~~Cell Configuration

This function should manage all the relevant (logical) cell configuration information and act as a co-ordinating function for the other controlling blocks, which will implement these parameters physically. All the associated RF parameters, system information parameters, and channel configuration data shall be held and distributed by the cell configuration function. In addition, this function should interface with the Implementation Specific Node B Configuration function (section 7~~6~~.3) in order to ensure high level Node B capabilities (such as basic duplexing and antenna configuration information) are available to the management system. It is envisaged that a number of Implementation Specific cell configuration parameters may exist in addition to those defined within the generic cell model.

~~1.5~~Performance Monitoring

This function shall be responsible for all performance related data collection and processing. All relevant aspects of the radio sites performance, which are not reported back to the RNC implicitly during normal traffic handling, should be incorporated here. It is envisaged that features such as interference measurements, local site events and periodic physical channel test results should be managed here. This function should also interface with other functions within the radio site to collate performance-related data (for example statistics relating to Iub link quality from the link termination and management function - section 7~~6~~.2). Once processed, the resulting reports should be transmitted back to the RNC/management system as applicable via the appropriate logical interface. The impact of performance statistics can be divided into two categories.

Firstly there are a number of performance statistics/measurements that can enable real time optimisation of the traffic environment; these are termed ‘real time’ (e.g. Node B DL transmission power, uplink interference). In addition there are a number of performance statistics which are not immediately required for traffic optimisation, for instance those requiring pre-processing or trend analysis to be useful. These are termed ‘non-real time’. The configuration of the real time and non real time performance measurements and statistics may be different.

~~1.6~~Alarm & Resource Event Management

Each of the individual functions shall be responsible for the generation of alarms and event notifications associated with its specific functional area. A centralised function should then be responsible for the collation and processing of these alarms and events, and their issue to the RNC/management system as applicable via the appropriate logical interface. It should also be possible for the Node B radio site to perform correlation and filtering, and the alarm and resource event management function would be responsible for these processes. All alarms and events raised against logical resource capabilities are termed ‘Resource Events’. When alarms or events relate to implementation specific aspects of the Node B they shall be termed ‘Fault Management Alarms’. In the case where a fault management alarm also impacts on the logical resources, Node B should be capable of assessing this impact and ensuring the appropriate resource event is also issued to the RNC/management system.

~~1.7~~Maintenance and Diagnostics

This function will supervise and repair faults in the Node B hardware. As such it will manage the execution of diagnostics on the Node B hardware, interacting with the Implementation Specific Node B Configuration function (section 7~~6~~.3) as necessary. The maintenance and diagnostics function will also be responsible for the ongoing health monitoring of the Node B (and via the external interface management function its ancillary devices - section 7~~6~~.15) by means such as periodic polling, diagnostics, and automatic calibration of radio hardware. It is envisaged the results of such diagnostics will not normally need to be reported back to RNC/management system, unless problems are discovered which result in resource events or fault management alarms being generated. Any form of remote test equipment installed in the node B site shall be controlled by this function.

Where problems are identified by the maintenance and diagnostics functions it should co-ordinate with the Alarm and Resource Management function (section 7~~6~~.6) to ensure the appropriate logical resource impact is notified accordingly. This should also include the circumstances where service capability is not totally lost but suffers reduced performance.

~~1.8~~Radio System Equipment Management

This function shall control the physical radio system hardware, performing operations such as transmitter tuning and power ramping. The cell configuration function (section 7~~6~~.4) shall perform the mapping of the physical channel information from the logical channels. Other radio related operations should also be performed by the radio system equipment management function. It will be the responsibility of this function to monitor the radio related performance aspects of the hardware, and report the results to the performance monitoring function (section 7~~6~~.5). Additionally, it is envisaged this function will be responsible for the redundancy of radio equipment - providing automatic reconfiguration as required.

The management of the radio system equipment will be dependent on the particular hardware implementation contained in a Node B. However the performance of the radio system is critical to traffic handling. The Radio System Equipment management function should therefore be capable of co-ordinating with the Alarm and Resource Management and Performance Management functions (sections 7~~6~~.6 and 7~~6~~.5 respectively) to ensure the conditions where logical resources may be impacted are notified accordingly.

~~1.9~~Common Equipment Management

The Common Equipment Management function shall control the management of the non-radio hardware within the Node B. This shall include equipment such as power supply units and O&M/support modules. The Node B should be capable of assessing the impact on the logical resources of the loss/degradation of any such common equipment, and generating indication of such loss as necessary.

~~1.10~~Dedicated Channel Management

This function shall perform the activation and management of dedicated channel resources - including both dedicated traffic and control channels. It will also be responsible for other related functionality such as the monitoring of channel performance and generation of resource events and fault management alarms as necessary. Dedicated channel management is an integral part of the core traffic handling function.

~~1.11~~Common Channel Management

This function shall perform the activation and management of common channel resources such as broadcast and paging channels. It will also be responsible for other related functionality such as re-paging, (though this may be transparent to the RNC/management system), as well as the monitoring of channel performance and generation of resource events and fault management alarms as necessary. Common channel management is an integral part of the core traffic handling function.

~~1.12~~Synchronisation and Timing

The Node B controller must be able to obtain accurate timing and synchronisation information for use within the radio site and over the Uu interface. The synchronisation and timing function should manage the extraction of timing information from any desired source (i.e. including external timing equipment). Recovery of timing and temporary generation of clock information must all be supported upon failure (and subsequent re-establishment) of the synchronisation source. This function should also manage the generation of timing related resource events/fault management alarms and performance parameters for communication back to the RNC/management platform as applicable. The synchronisation of the Node B site is critical to the successful handling of traffic, and it is therefore important that the synchronisation and timing function interacts with the Alarm and Resource Event Management function (section 7~~6~~.6) to indicate any impact on the logical resources.

~~1.13~~Coding and Channelisation

The coding and channelisation function shall be responsible for the physical coding and channelisation of the Uu interface. This function shall receive all the appropriate logical data from the dedicated channel and common channel management functions and manage all the required encoding and packaging for transmission by the radio hardware. The coding and channelisation function should contain sufficient intelligence to enable identification of any conflicts between the realisable physical channels and logical channel data. Any errors detected should be reported back to the RNC/management system as applicable via the appropriate interface. Coding and channelisation is an integral part of the core traffic handling function.

~~1.14~~Security and Access Control

The Node B Radio site must be capable of controlling local access both physically (i.e. tamper alarms) and through communication interfaces. Password protection and security levels should be implemented for local interfaces. It should further be possible to report the status of these operations back to the management system - possibly as fault management alarms. These shall provide indication of sessions established, door alarms triggered, operations performed locally, etc.

~~1.15~~External Interface Management

The Node B site should be provided with the ability to interface with external ancillary devices such as standalone power systems, repeaters, link equipment and adaptive antenna's. Whilst it is not within the remit of this document to attempt to define these local interfaces, it should be recognised that support of such ancillary devices may impact on either the Iub or Implementation Specific O&M logical interfaces, or both. Notably, where such equipment is critical to the provision or quality of service, any logical impact where a loss or degradation in the equipment is experienced should be indicated as necessary.

Logical O&M Functions

[Note: The following list of functions must be aligned with those agreed in 25.433 (NBAP Specification) at WG3#4 in Warwick]

The following functions have been identified which consist of elements that can be classified as Logical O&M. The logical O&M elements of these functions should be supported on the Iub interface, as an integral part of the NBAP specification (see reference [1]). The scope of messages required for each function is FFS – some of the functions listed below may consist of both Logical O&M and Implementation Specific O&M elements.

1. Cell Configuration

Since a cell is a logical traffic handling entity, the parameters determining its configuration must all be defined by the RNC. In addition, ongoing changes to the cell configuration must be co-ordinated with the traffic handling entity(s). For this reason cell configuration should be considered as an integral part of the core traffic handling function. The parameters associated with a cell must therefore be derived from the RNC, and the function of Cell Configuration must consequently be supported over the Iub interface. This should included the ability to update or change cell parameters on a real time basis in response to the traffic conditions.

2. Common Channel Management

The management of common channels should be considered an integral part of the traffic handling procedure, and it should therefore be supported over the Iub interface.

3. Dedicated Channel Management

The management of dedicated channels should be considered an integral part of the traffic handling procedure, and it should therefore be supported over the Iub interface.

4. Coding and Channelisation

Coding and channelisation should be considered an integral part of the traffic handling procedure, and it should therefore be supported over the Iub interface.

5. Resource Events

For all resource faults and conditions, Node B must be capable of generating resource event notifications indicating the impact on the logical resources. These resource events must be available to the RNC and must therefore be supported over the Iub interface. This will enable the RNC to compensate for such faults in its core traffic handling procedures, thus maximising the available quality of service.

6. Software Initialisation

Where the process of downloading software (and its initialisation) impact on the traffic carrying abilities of Node B, it is essential that the RNC is informed of such initialisation and can respond to the Node B indicating that a restart is allowed. This will ensure that the traffic can be controlled according to the abilities of Node B**,** thus maximising the available quality of service. In addition, to optimise the Software download process the RNC may be used as a code repository, however download initiation and control should lie with the management system. This may reduce the number of simultaneous downloads that the management system must support, by using the RNC as a distribution function. As such the process of software downloading shall be transparent to the RNC at application level and should not be supported over the Iub. However, the associated process interaction should be supported over the Iub to ensure the impact on traffic can be carefully managed.

7. Link Termination and Management

NOTE: Inclusion of the following text is dependent on the RAN-WG3 decision relating to the suitability of IMA to perform this function.

Knowledge of the status and performance of the Iub interface at the RNC is essential to the optimisation of the service environment. The Iub interface should therefore support the management of the link condition and performance.

8. Performance Monitoring – Real Time

These key statistics should enable the RNC to make traffic handling decisions which best suit the system conditions at that time, and these statistics should therefore be common to all Node B's and available to the RNC on a real time basis. These key measurements are FFS, but the Iub interface should be capable of supporting their transfer to allow the quality of service to be maximised.

Implementation Specific O&M Functions

The following functions should be supported by the Implementation Specific O&M interface. Standardisation of the Implementation Specific O&M shall be limited to the physical transport bearer (reference [3]) – further standardisation is out of scope for RAN-WG3.

1. Radio System Equipment Management

The management of the radio system equipment will be dependent on the implementation of the Node B in question. It should therefore be supported via the Implementation Specific O&M. The performance of the radio system, and any impact of failures on the logical resources of Node B (including performance degradation), should be reported to the RNC via the Resource event alarm management in the logical O&M.

2. Common Equipment Management

The common equipment within a Node B will be dependent on the implementation of the Node B in question. Common Equipment Management should therefore be supported via Implementation Specific O&M. However, where failures impact on the logical resources of Node B this should be reported to the RNC via the Resource event alarm management in the logical O&M.

3. Maintenance and Diagnostics

The maintenance and diagnostic procedures carried out at the Node B radio site will be dependent on the particular implementation. Therefore these functions should be supported via the Implementation Specific O&M. Where the results of such operations impact on the logical resources in Node B, this should be reported to the RNC via the Resource event alarm management in the logical O&M.

4. Security and Access Control

The security and access control functions performed at Node B will be dependent on the implementation in question. Security and Access control should therefore be supported via the Implementation Specific O&M.

5. Implementation Specific Node B Configuration

It is important from a system management perspective to have an accurate record of the hardware and software configuration of the Node B radio site. This should be remotely available, and will be dependent on the implementation of the Node B in question. Implementation Specific Node B Configuration should therefore be supported via the Implementation Specific O&M.

6. Fault Management Alarms

For accurate remote fault diagnosis, all Node B alarms should be available to the management system. All alarms should therefore be supported via the Implementation Specific O&M. However Node B should be capable of assessing the impact of certain faults on the logical resources, and reporting this to the RNC via the Resource event alarm management in the logical O&M.

7. Performance Monitoring - Non Real Time

Measurements or performance statistics should be available from Node B, to assist in the optimisation of the UTRAN. These should therefore be supported via the Implementation Specific O&M.

8. External Interface Management

A number of ancillary devices may be connected to a Node B, and the status of these devices should be accessible to the overall network management system. The Implementation Specific O&M should therefore support the ability to interface between these ancillary devices and the management system.

9. Synchronisation and Timing

The configuration of the synchronisation and timing function of the Node B will be dependent on the implementation of Node B. As such, this function should be supported over the Implementation Specific O&M. Where the timing and synchronisation status of the Node B radio site impacts on the logical resources, this impact should be indicated to the RNC via the Resource event alarm management in the logical O&M.

10. Software Management

Control of Software Download and initialisation should rest with the management system, and is therefore implemented via the Implementation Specific O&M Interface, The RNC should be informed and allowed to ok any Node B initialisation or restart (see section 7 above) via the logical resource management interface.

11. Implementation Specific Cell Configuration

To allow for vendor differentiation of cell functionality, it is envisaged a number of cell related parameters may exist in addition to those defined as part of the generic cell model. The configuration of these parameters shall be supported via the Implementation Specific O&M.

Signalling Procedures

[Editors Note: The following text is included as a working assumtion as agreed at RAN-WG3#5]

~~1.1~~Signalling Procedures

~~[Editor's note: This section should define (where possible) the signalling procedures for the functions identified in section 5. It is not envisaged it will be possible to define signalling procedures for all Node B O&M functions, since some will be implementation specific. These procedures may be required for certain functions to assist in the categorisation as either Logical O&M or Implementation Specific O&M.]~~

This chapter provides examples of comprehensive descriptions of each O&M NBAP procedure defined. For each “O” type procedure, it shall additionally provide a scenario diagram of their execution to clarify interaction between various NE's and Managers. The scenarios shall include both Logical O&M and Implementation Specific O&M procedures, thus ensuring that a comprehensive description of the procedure provided clearly define the scope of that procedure. This should facilitate better understanding of the scope of each such procedure.

UTRAN O&M Procedure Types

It is proposed to have the following procedure type definition:

Procedure Type	Meaning
O	Operator instigated
A	Autonomously executed by RNC

[Editor's note: A table listing all NBAP procedures and their categorisation as above should be inserted here.]

Initial Node B Configuration

The detailed steps of the procedure is given in the below. It describes the scenario that a new Node B is added to the network and one or several cells of the Node B will be set up and activated.

In sections 8.5.1 and 8.1.1 of [1] NBAP procedures are specified for the Cell Setup and Common Channel(s) Setup. But the aspects not described in these sections are how the following is achieved (text taken directly from [1]):

- *Node B equipment has previously been defined and configured to support the cell on the Implementation Specific O&M interface.*
- *A Node B control port is available for communication between the RNC and the Node B, for the procedure to be executed successfully.*

The object of this example is to build a complete picture of the procedure by bringing the management systems into the scenario. The following is a description of the steps in the figure below.

1. The Node B hardware will be installed at the Node B site, as well as software to be installed locally and setting of parameters.
2. The ATM link between the Node B and C-RNC will be established. This includes the establishment of the ALCAP and NBAP signalling bearer.
3. The transport channel for the Implementation Specific O&M will be established. If the Implementation Specific O&M is to be routed by the C-RNC, one or several AAL5/ATM PVC's or SVC's for the transport of O&M IP packets will be established. Otherwise a direct IP transport channel to the Node B Manager will be established.
4. An Node B initialisation procedure will be performed by means of Implementation Specific O&M functions (this could possibly be initiated from the NMC). It includes downloading of software from the Node B Manager which can be done automatically or manually. Having completed this procedure all necessary conditions to allow the subsequent configuration of logical resources in one or several cells will be met in the Node B.
5. Following the Node B implementation specific initialisation some self tests may be performed. The result of these self tests should be communicated to the Node B manager via implementation specific O&M.
6. The Node B informs the C-RNC about the completion of the Node B Initialisation. The Node B sends also the locally set parameters which are needed for the cell configuration, i.e. Local Cell Id(s) and number of carriers
7. C-RNC informs the C-RNC Manager about the completion of the Node B Initialisation, C-RNC Manager subsequently informs Network Management Centre (Step 7').

Note: The remaining logical cell configuration should be performed as described in chapter 10.1.3 below.

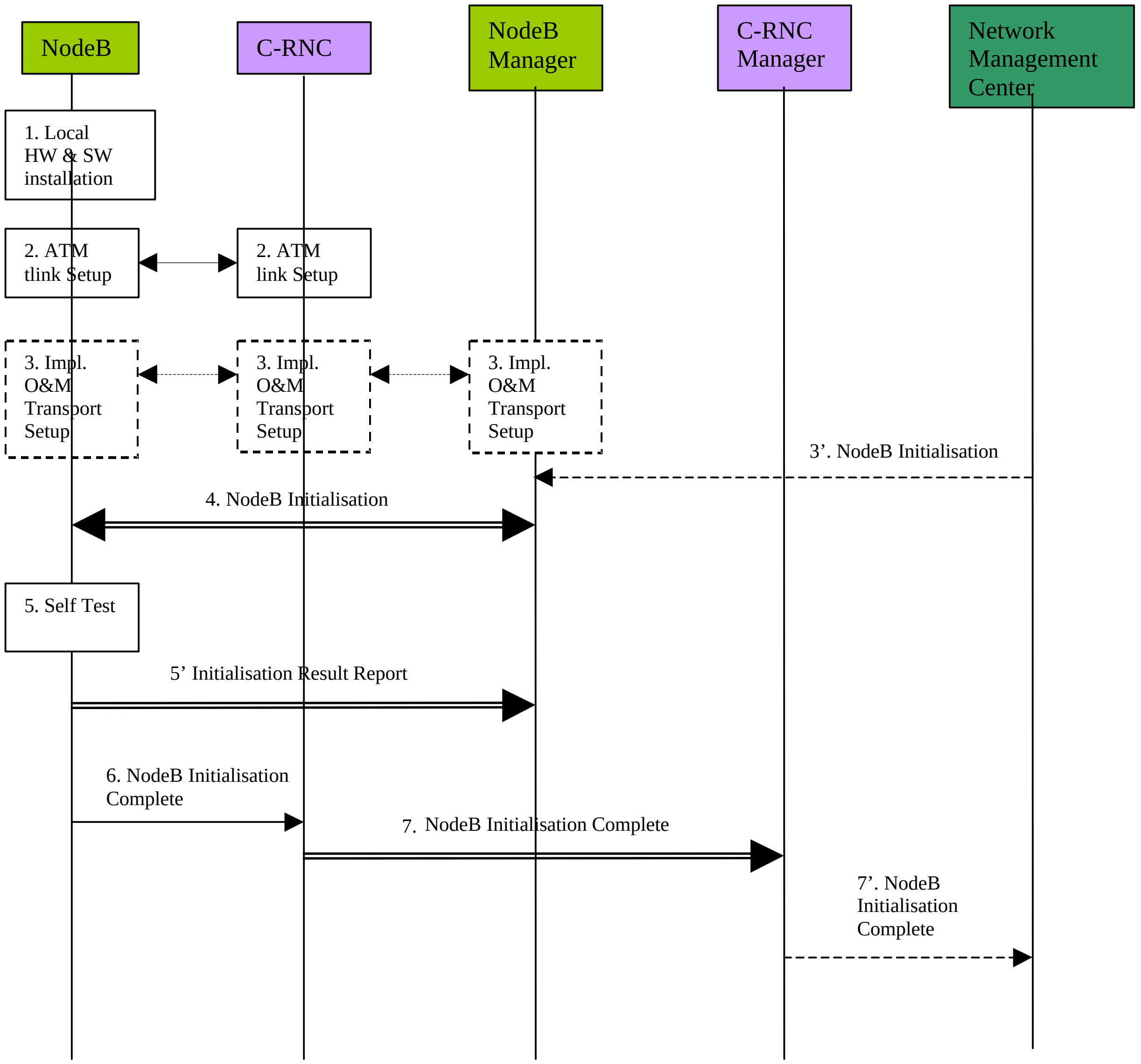

NodeB
C-RNC
NodeB Manager
C-RNC Manager
Network Management Center
1. Local HW & SW installation
2. ATM tlink Setup
2. ATM link Setup
3. Impl. O&M Transport Setup
3. Impl. O&M Transport Setup
3. Impl. O&M Transport Setup
3'. NodeB Initialisation
4. NodeB Initialisation
5. Self Test
5' Initialisation Result Report
6. NodeB Initialisation Complete
7. NodeB Initialisation Complete
7'. NodeB Initialisation Complete

Figure 10.1.2.1: Complete Node B Initial Configuration Procedure

Cellular Network Configuration

As described in section 5.2.2, the cellular network configuration procedure shall enable all required Node B parameter modifications associated with the definition of the Radio Access Network. The configuration of Node B incorporates both configuration of the logical resources supported at Node B, and configuration of the Implementation Specific aspects of Node B to support these resources. In addition, in order to allow the radio access network to be optimised on an ongoing basis depending on the traffic conditions, both initial configuration and ongoing configuration must be supported.

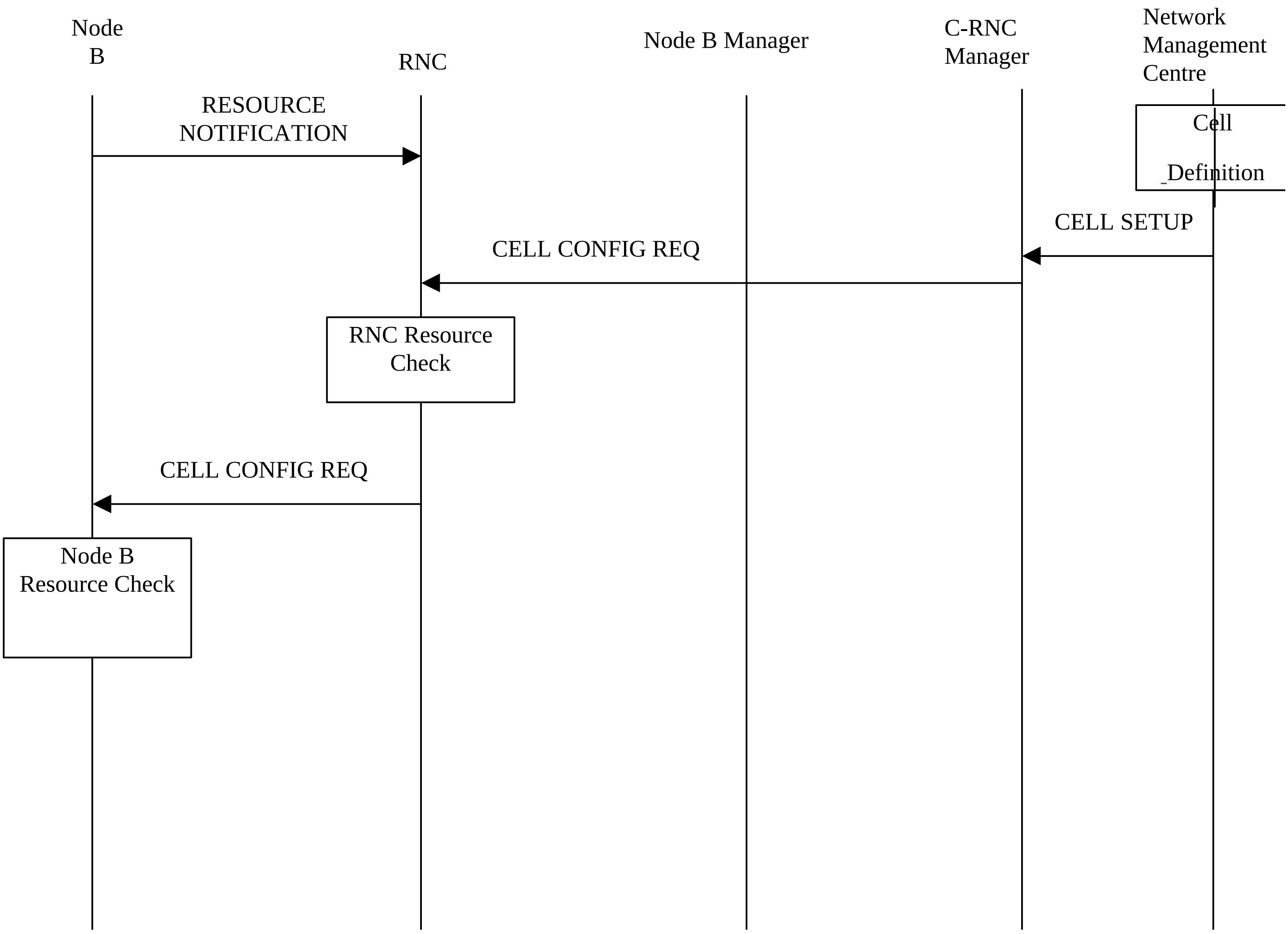
~~1.1.1.1~~Initial Cell Configuration

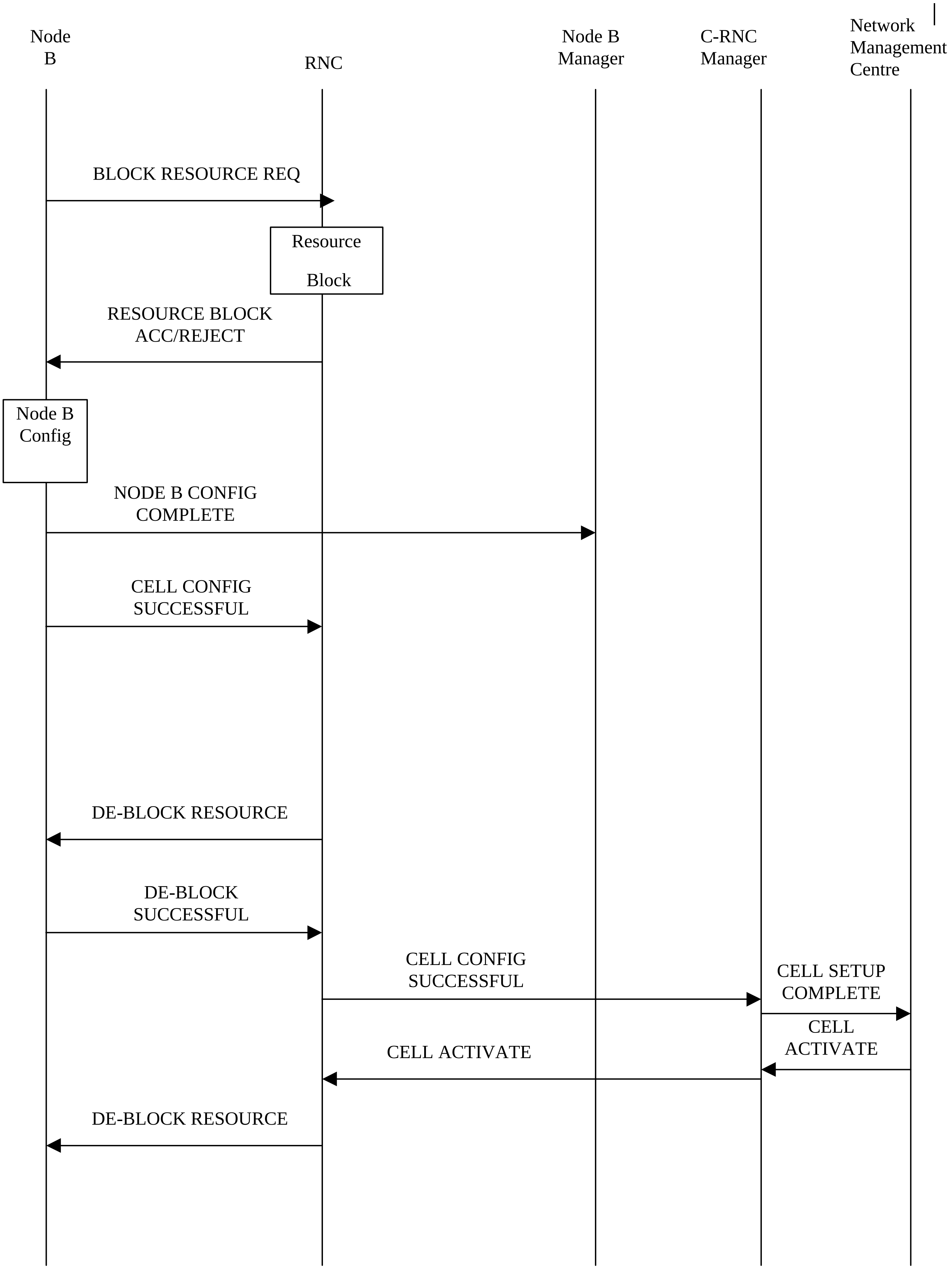
The definition of a cell in the UMTS system will originate from the management system. In order to make this process as simple as possible for the network operator, automation should be used and standardised entities addressed wherever possible. As such, the focus for creation of a cell should be the standardised cell model defined within the UTRAN. The creation of this Logical traffic carrying entity should be the trigger for the overall cell creation process, since this enables the network operator to deal only in standardised entities and not manufacturer specific aspects.

The Logical cell entity itself is assumed to be resident in the RNC, since the cell is a logical traffic carrying entity and the RNC is the traffic controlling entity. The cell shall be as defined in [1]. The creation of the cell communication port in Node B shall be achieved via Implementation Specific O&M.

The following procedure represents one possible method by which a cell can be configured within the UTRAN. This procedure assumes that the associated Node B has already been installed using the procedure described in section 10.1.2, and that both Iub and Implementation Specific O&M communications are established.

[Editors Note: The following figure should be re-drawn in the same format as figure 10.1.2.1]




Node B
RNC
Node B Manager
C-RNC Manager
Network Management Centre
BLOCK RESOURCE REQ
Resource
Block
RESOURCE BLOCK ACC/REJECT
Node B Config
NODE B CONFIG COMPLETE
CELL CONFIG SUCCESSFUL
DE-BLOCK RESOURCE
DE-BLOCK SUCCESSFUL
CELL CONFIG SUCCESSFUL
CELL SETUP COMPLETE
CELL ACTIVATE
CELL ACTIVATE
DE-BLOCK RESOURCE

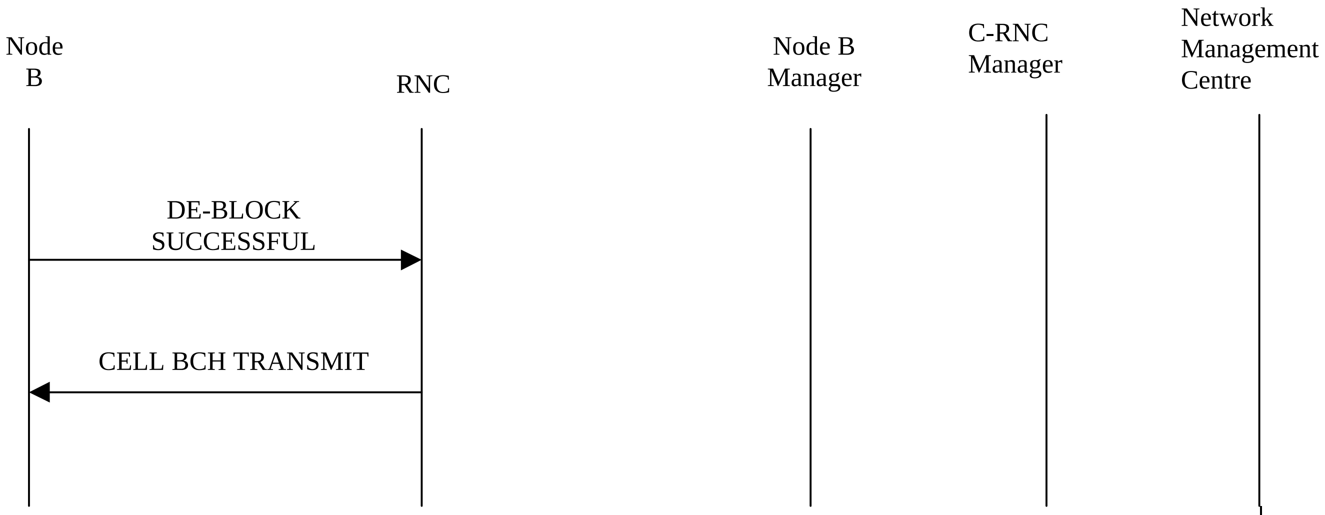


Figure 10.1.3.1.1: Initial Cell Configuration

The procedure above consists of the following steps.

1. Following the Node B initialisation (implementation specific), Node B sends a resource notification to the RNC.
2. The cell is defined and created in the network management system by the operator. This may be by manual means or as an output from network optimisation tool. The definition should include identifiers relating to the related Node B for creation of this cell and the associated C-RNC. These identifiers are FFS.
3. The operator initiates the creation of the cell, and the network management system sends the cell configuration data to the appropriate C-RNC manager. The C-RNC manager passes the cell data to the C-RNC for creation.
4. The C-RNC performs a resource check to ensure it has sufficient resources to support the new cell it has been instructed to define. This resource check applies only to the RNC's capabilities and not the Node B.
5. The C-RNC sends the associated cell configuration data to the target Node B.
6. The Node B then determines whether the configuration process to follow will impact on the logical resources it is currently supporting (if any). If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.
7. The RNC will attempt to block the resources as requested by the Node B.
8. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
9. Once all resources are finally blocked, the Node B performs it's Implementation Specific configuration.
10. The Node B then advises the management system that the Implementation Specific configuration is complete.
11. Node B then performs the configuration of the new cell.
12. Once complete, the Node B advises the C-RNC that the configuration of the new cell has been successful. The state of the resources for the new cell should be blocked at this stage.

13. The RNC then instructs the Node B to de-block any other Node B resources which might have been blocked to perform the configuration of the new cell. Note: this does not include the resources associated with the new cell.

14. Node B advises the RNC of the success of this de-block.

15. The RNC then advises the C-RNC manager that the configuration of the new cell has been successful. This success notification is passed to the network management system.

16. The operator then initiates the activation of the new cell from the network management system, and a message is sent from the management system to the C-RNC manager and then to the C-RNC to trigger the activation of the cell.

17. The RNC instructs the Node B to de-block the new cell resources.

18. The Node B de-blocks the resources and advises the RNC of the success of this operation.

19. The RNC instructs the Node B to begin transmission of the BCH in the new cell (this shall be achieved using a deblock procedure from the RNC to the Node B for the BCCH).

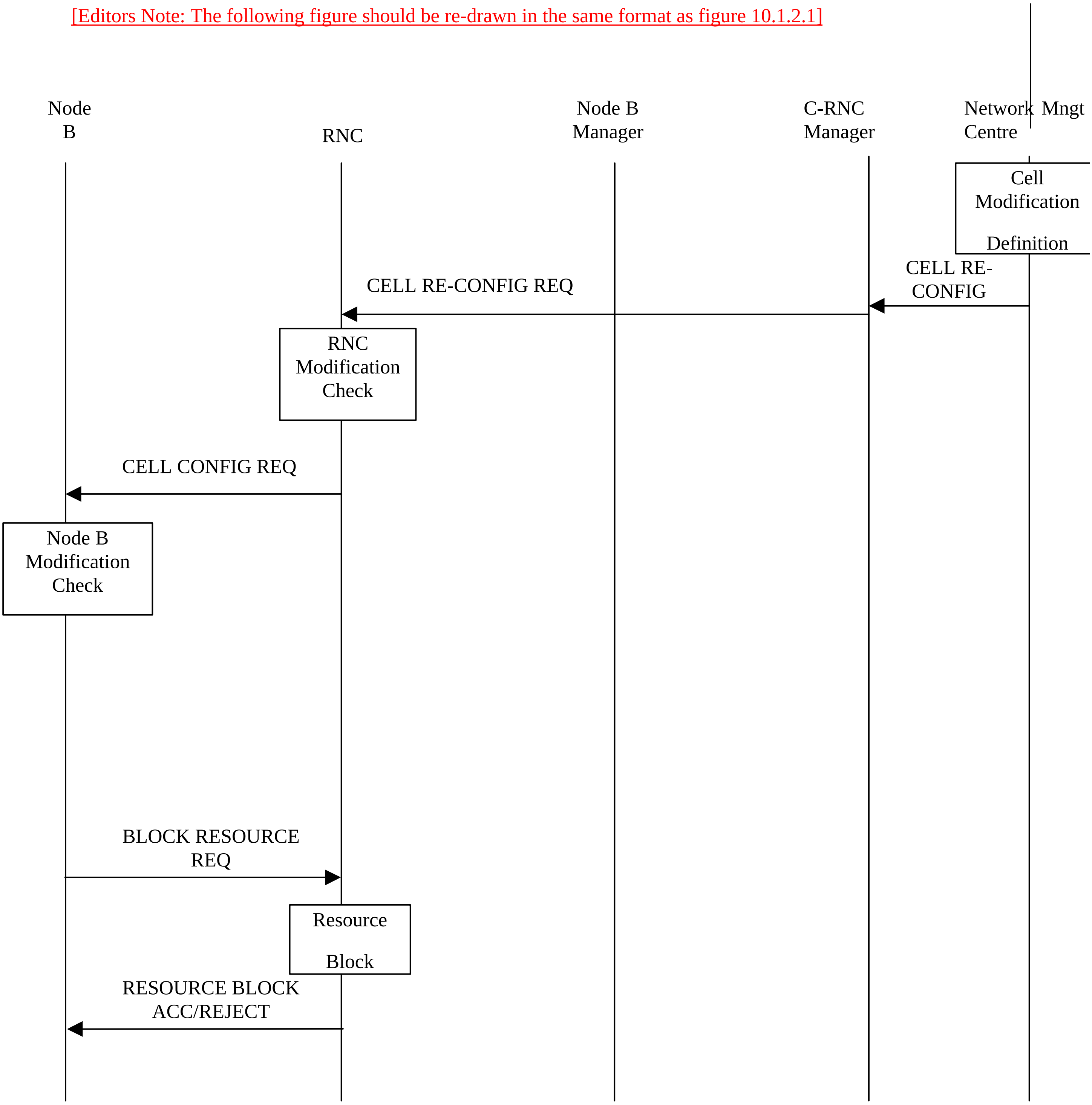
Cell Re-Configuration

In order to enable the traffic environment to be optimised, the ongoing re-configuration of cell parameters must be supported within UMTS. To ensure that both long term and real time optimisation can be applied to the UTRAN, the RNC should control the traffic carrying entity (i.e. the cell) and its associated parameters. In applying this philosophy, the generic cell model is held at the RNC giving the RNC access to all parameters for any required modification. This is essential if the cell parameters are to be altered on a real time basis in order to optimise the traffic environment, since the RNC is the only UTRAN entity with real time knowledge of the traffic conditions. This generic cell model controlled by the RNC does not include any Node B Implementation Specific parameters which may be interpreted as 'cell

Therefore, two categories of cell re-configuration must be supported – that which is initiated from the management system (operator or optimisation tool), and that which is automatically initiated by the radio resource algorithms in the RNC.

The procedure below represents one possible method by which a cell can be re-configured from the management system.

[Editors Note: The following figure should be re-drawn in the same format as figure 10.1.2.1]



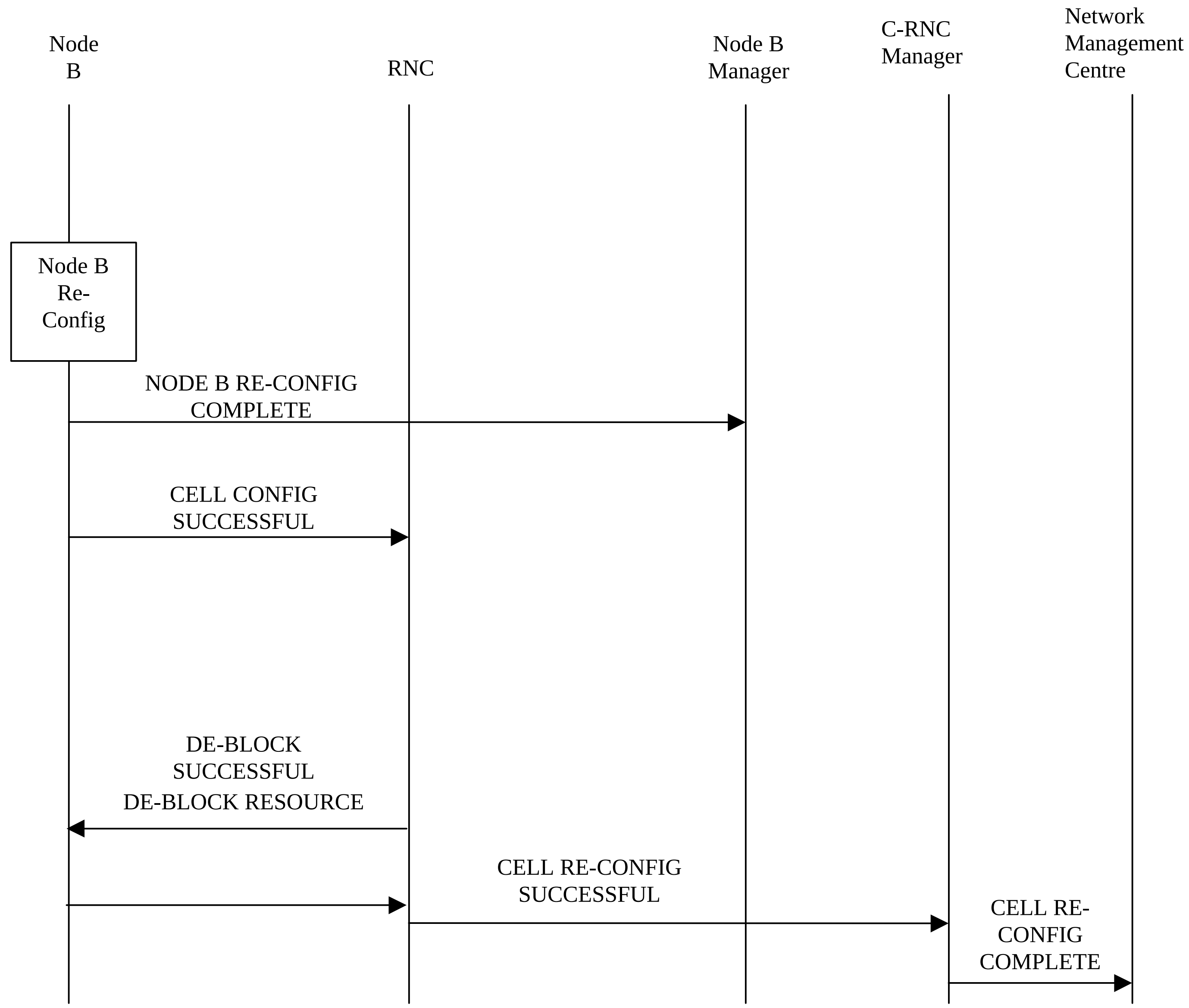


Figure 10.1.3.2.1: Cell Reconfiguration Initiated by the Management System

The procedure above consists of the following steps.

1. The change to the cell configuration is defined and created in the network management system by the operator. This may be by manual means or as an output from network optimisation tool. The definition should include the cell identifier and the associated C-RNC identifier.
2. The operator initiates the re-configuration of the cell, and the network management system sends the cell re-configuration data to the appropriate C-RNC manager. This is then passed to the C-RNC to trigger the process.
3. The C-RNC performs a check on the requested configuration changes to ensure they are compatible with the remaining cell configuration and capabilities.
4. The C-RNC sends the associated cell configuration data to the target Node B.

5. The Node B performs a check on the requested configuration changes to ensure they are compatible with the remaining Node B configuration and capabilities.

6. The Node B then determines whether the re-configuration process to follow will impact on the logical resources it is currently supporting (if any). If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.

7. The RNC will attempt to block the resources as requested by the Node B.

8. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.

9. Once all resources are finally blocked, the Node B performs it’s Implementation Specific re-configuration.

10. The Node B then advises the management system that the Implementation Specific re-configuration is complete.

11. Node B then performs the re-configuration of the cell.

12. Once complete, the Node B advises the C-RNC that the configuration of the cell has been successful.

13. The RNC then instructs the Node B to de-block any Node B resources which might have been blocked to perform the re-configuration of the cell.

14. Node B advises the RNC of the success of this de-block.

15. The RNC then advises the C-RNC manager that the re-configuration of the cell has been successful. This success notification is passed to the network management system.

The procedure below represents one possible method by which a cell can be automatically re-configured from the RNC.

[Editors Note: The following figure should be re-drawn in the same format as figure 10.1.2.1]

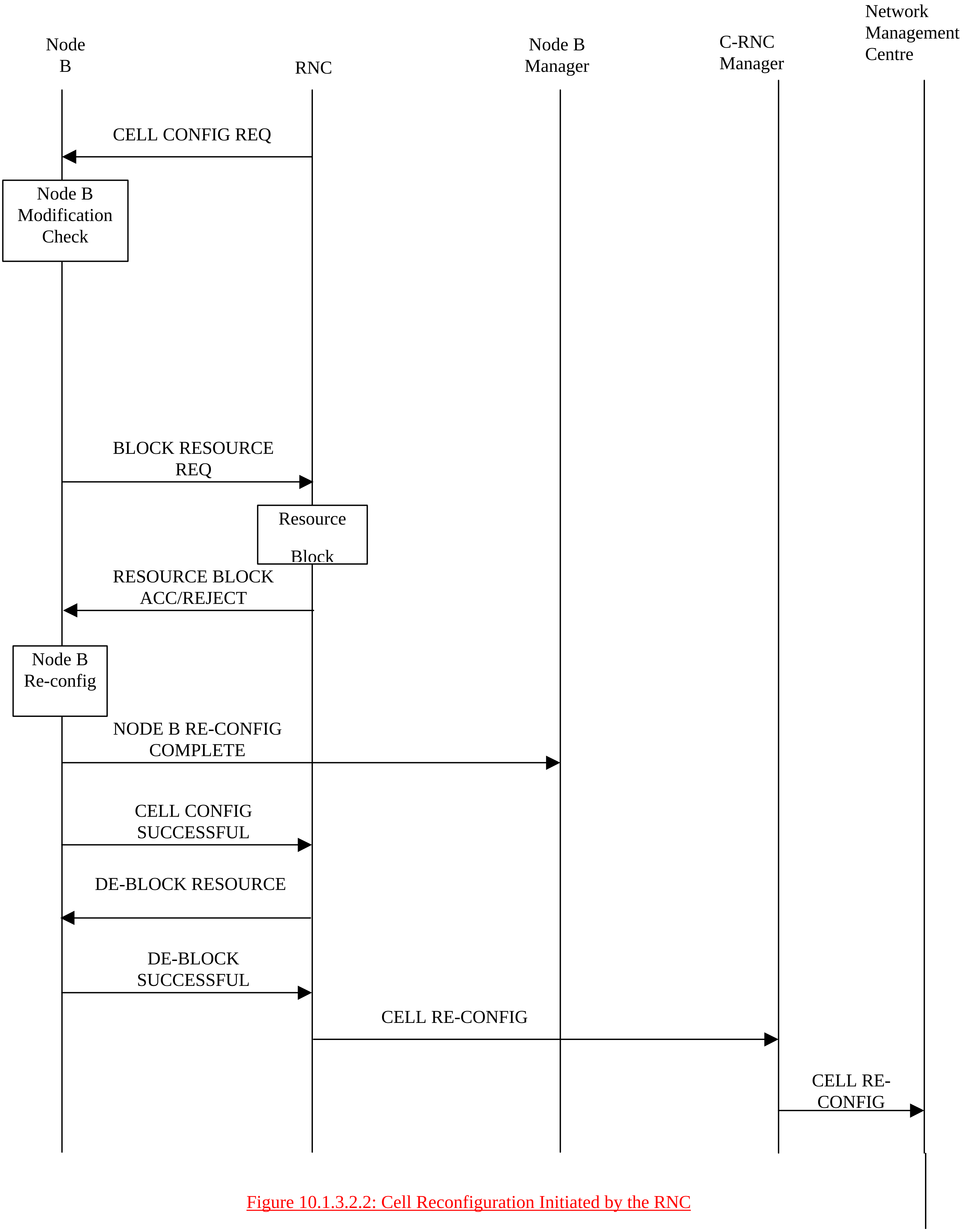


Figure 10.1.3.2.2: Cell Reconfiguration Initiated by the RNC

The procedure above consists of the following steps.

1. Following a decision in the radio resource algorithms due to the traffic conditions, the C-RNC sends new cell configuration data to the target Node B.
2. The Node B performs a check on the requested configuration changes to ensure they are compatible with the remaining Node B configuration and capabilities.
3. The Node B then determines whether the re-configuration process to follow will impact on the logical resources it is currently supporting (if any). If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC.
4. The RNC will attempt to block the resources as requested by the Node B.
5. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
6. Once all resources are finally blocked, the Node B performs it's Implementation Specific re-configuration.
7. The Node B then advises the management system that the Implementation Specific re-configuration is complete.
8. Node B then performs the re-configuration of the cell.
9. Once complete, the Node B advises the C-RNC that the configuration of the cell has been successful.
10. The RNC then instructs the Node B to de-block any Node B resources which might have been blocked to perform the re-configuration of the cell.
11. Node B advises the RNC of the success of this de-block.
12. The RNC then advises the C-RNC manager which in turn advises the network management system of the cell re-configuration that has been executed for updating of the management system cell database.

Network Optimisation Procedure

Reports regarding the cell performance

In order to identify possible modifications that allow an improvement of the overall network performance this process type consists of the collection of measurement data within the cell. Below the reports are discussed.

No. of active channels per cell

In order to compare the planned cell capacity with the real traffic load the no. of active channels within the cell has to be measured. This has to be done at least in a statistical way, e.g. n active channels per measurement time period (e. g. 15 minutes). The operator has to know the data rates / the services of this channels. Just to give an example, the output of this collection could be

12:00 - 12:15

8k circuit switched service:	16
16k circuit switched service:	12
128k circuit switched:	2
358k packet switched:	1

12:15 – 12:30

8k circuit switched service:	12
128k circuit switched:	1
358k packet switched:	2

It's for discussion if there is also some information necessary regarding the spreading factor (SF) and the use of multi code transmission.

Sector call Setup

The number of call setup attempts within a cell has to be measured together with the number of call setup failures and the reasons for these failures. It should be distinguished between UE originated and UE terminated calls.

The sector call setup failures shall distinguish between failures which occur at Node B (i.e. before channel requests have been sent to the RNC) and those which occur in the RNC.

RF Loss

The number of RF losses per cell has to be counted. It shall be possible to combine the result with a failure indicator.

Node B output power

The output power of a Node B depends on the no. of channels and the location of the UE's. That means that the overall output power of a Node B varies. For the network planning, the interference given to the neighbour cells is of interest. So the distribution of the overall output power of a Node B (per sector) has to be reported to the Management Platform. It's for discussion if this information is also needed within the RNC.

~~10.1.4.2~~Node B interference level

For the measurement of the interference level at the Node B (antenna connector) the RNC has to measure the overall receive power.

~~10.1.4.3~~Uplink DCH input power

The distribution of the Uplink DCH input power at the antenna connector should be measured.

~~10.1.4.4~~Downlink DCH output power

The distribution of the downlink DCH output power at antenna connector should be measured.

Performance Thresholds exceeded

It shall be possible to define "performance" thresholds. If this thresholds are reached the events should be counted. Thresholds could be defined for Eb/No, Tx power, Rx power, BER, FER, etc.. It has to be investigated whether the values can be derived at the Node B or at the RNC.

~~10.1.4.5~~Reports regarding the Node B performance

~~10.1.4.6~~Node B hardware report

The Node B hardware report shall include

- an overview of the share of the traffic load on the different hardware components (cards, RAKE receivers, etc.)
- stability report (e. g. out of service time)
- busy time of the different hardware components

~~10.1.4.7~~Node B resource report

This report shall include the usage of the physical L1 resources (e.g. channel no., code no., etc.).

~~10.1.4.8~~Reports regarding the Handover performance

The no. of successful / unsuccessful handover attempts is of interest for the optimisation of UTRAN as well as the core network.

Regarding the handover report the following cases are distinguished (refer to [7]):

softer handover

intra RNC soft handover

inter RNC soft handover

intra cell hard handover

inter cell hard handover

inter Node B hard handover

inter RNC hard handover

handover from UMTS to GSM

handover from GSM

The number of the branches should be part of this statistics.

It' s for further study if their is any time information needed, e.g. how long a UE is in the handover case (i.e. medium time).

~~10.1.4.9~~Routing of the PM reports

The RNC should be able to make traffic handling decisions which best suit the system conditions at that time. Therefore some key statistics should be routed to the RNC. These key statistics should be common to all Node B’s and available to the RNC on a real time basis. The Iub interface should be capable of supporting their transfer to allow the quality of service to be maximised.

The table below lists the PM reports. Besides these reports there will exist implementation specific reports.

Node B parameter / report	Node B to NMP	Node B to RNC	RNC to NMP
No. of active channels per cell			X
Sector call setup	?		X
RF Loss			X
Node B output power	X	real time meas.	
Node B interference level	X	real time meas.	
Uplink DCH power	X	real time meas.	
Downlink DCH power	X	real time meas.	
Performance Thresholds exceeded	X	real time meas.	
Node B hardware report	X		
Node B resource report	X		
Softer handover			X
Intra RNC soft handover			X
Inter RNC soft handover			X
Intra sector hard handover			X
Inter sector hard handover			X
Inter Node B hard handover			X
Handover CDMA to GSM			X
Handover from GSM			X
Inter RNC soft handover			X
Inter RNC hard handover			X
Data rates			X
Multi code usage			X

The real time measurements can be used for admission control. To avoid collision of the PM measurements in the Node B done in parallel by the MNP and the RNC (real time measurements) the MNP starts the measurements in the Node B. The RNC can request these measurements.

Remote Node B Update

As described in section 5.2.3, the remote update procedure shall enable the software used by Node B to be updated remotely from the management system. The actual software used by Node B will be specific to a particular vendor implementation, and it's transfer should therefore be supported via Implementation Specific O&M. However, it is possible that the process of updating Node B software may impact on the logical resources within Node B. It is therefore necessary for the RNC to be involved in this process to enable the traffic handling to be optimised during such procedures.

There are two possible mechanisms to initiate the transfer of new software to the Node B. Firstly, the software may be located in a remote node and the Node B provided with an appropriate address to retrieve the software – this is referred to as a 'pull method'. Also, it is possible for the management system to provide the software directly to the Node B – this is referred to as a 'push method'. Both mechanisms should be supported in the standards, with the choice of which method to implement (or both) being left to vendor implementations and operator requirements.

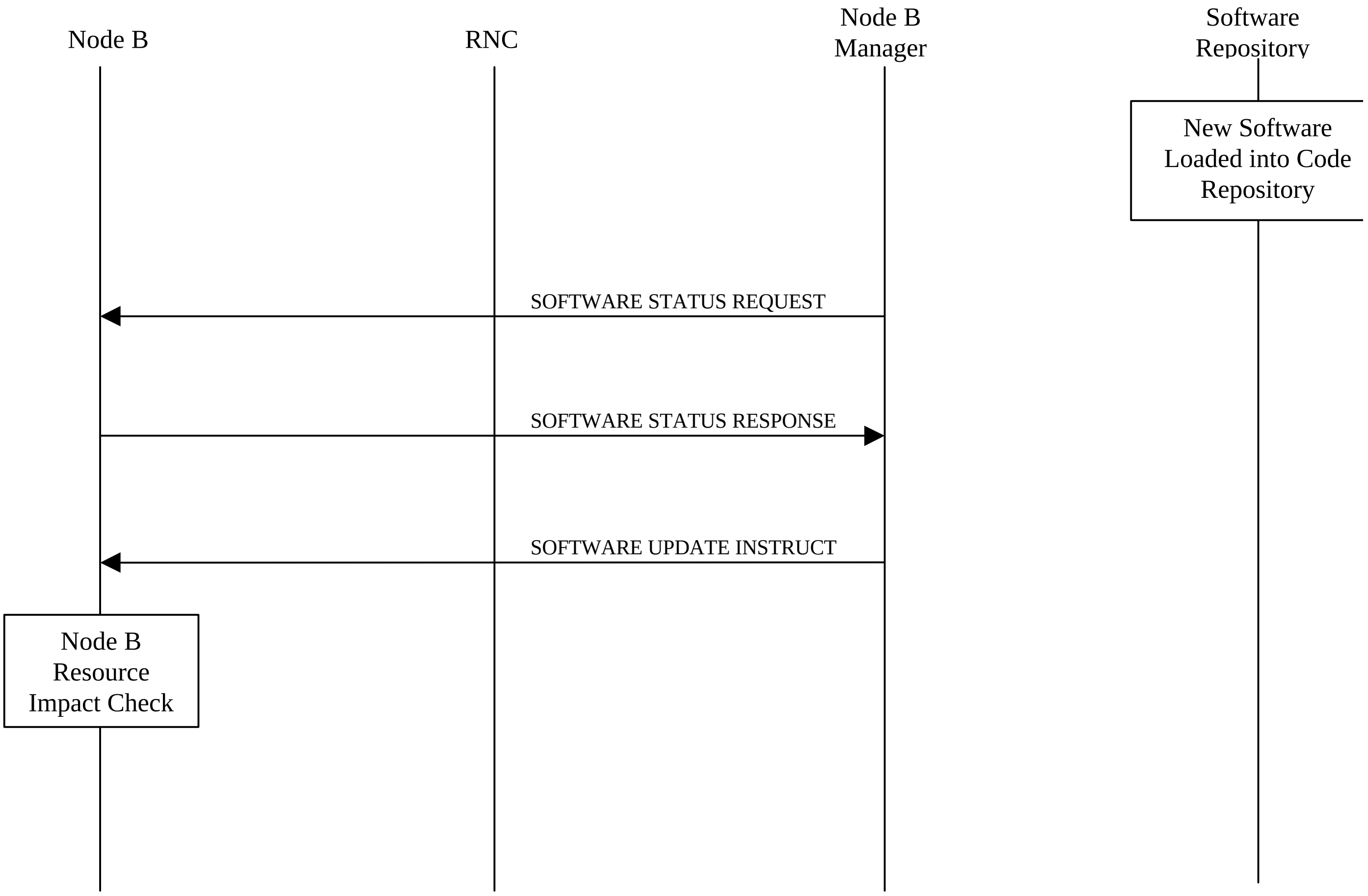
~~1.1.1.1~~Remote Update Procedure ~~-~~Pull Method

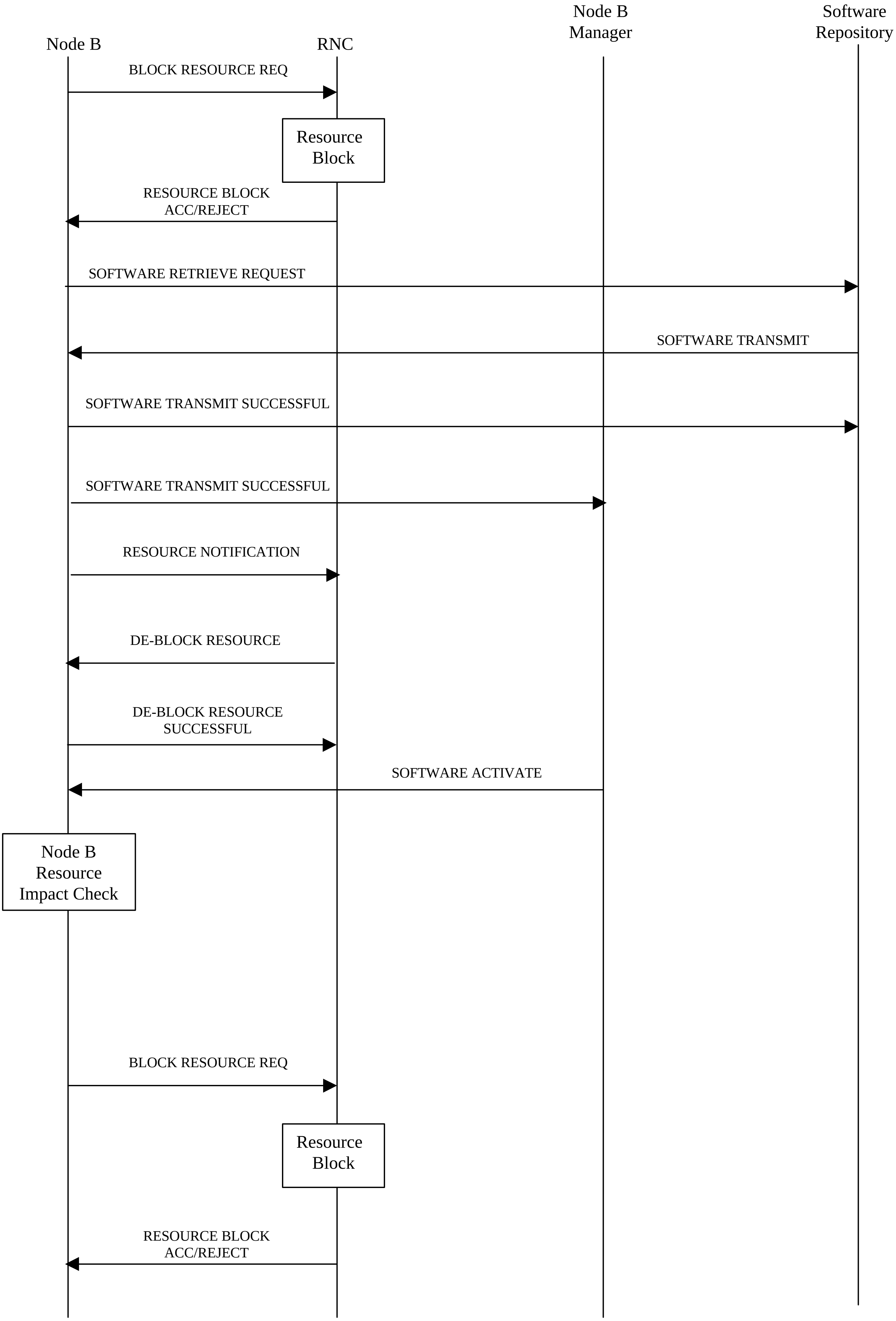
The initiation of the remote upgrade of a Node B will originate from the management system. However, in a mature network a large number of Node B's will be installed and the process of simultaneously upgrading all Node B's places great demands on the bandwidth requirements to the management system and the processing capability within it. To overcome this the management system can manage the update process in the normal way, however the actual software can be stored in remote software repositories which can be accessed by the Node B's. These software repositories are logical entities which can be physically located anywhere in the UMTS system.

In addition, the actual process of downloading software and/or activating it may impact on the logical resources supported in Node B. It is therefore necessary to ensure the RNC is advised of such impact and provided with the opportunity to defer the operation based on the traffic conditions.

The following procedure represents one possible method by which a Node B's software can be remotely upgraded using a pull method. This procedure assumes that the associated Node B has already been installed and configured using separate procedures, and that both Iub and Implementation Specific O&M communications are therefore established.

[Editors Note: The following figure should be re-drawn in the same format as figure 10.1.2.1]




Node B
RNC
Node B Manager
Software Repository
BLOCK RESOURCE REQ
Resource Block
RESOURCE BLOCK ACC/REJECT
SOFTWARE RETRIEVE REQUEST
SOFTWARE TRANSMIT
SOFTWARE TRANSMIT SUCCESSFUL
SOFTWARE TRANSMIT SUCCESSFUL
RESOURCE NOTIFICATION
DE-BLOCK RESOURCE
DE-BLOCK RESOURCE SUCCESSFUL
SOFTWARE ACTIVATE
Node B Resource Impact Check
BLOCK RESOURCE REQ
Resource Block
RESOURCE BLOCK ACC/REJECT

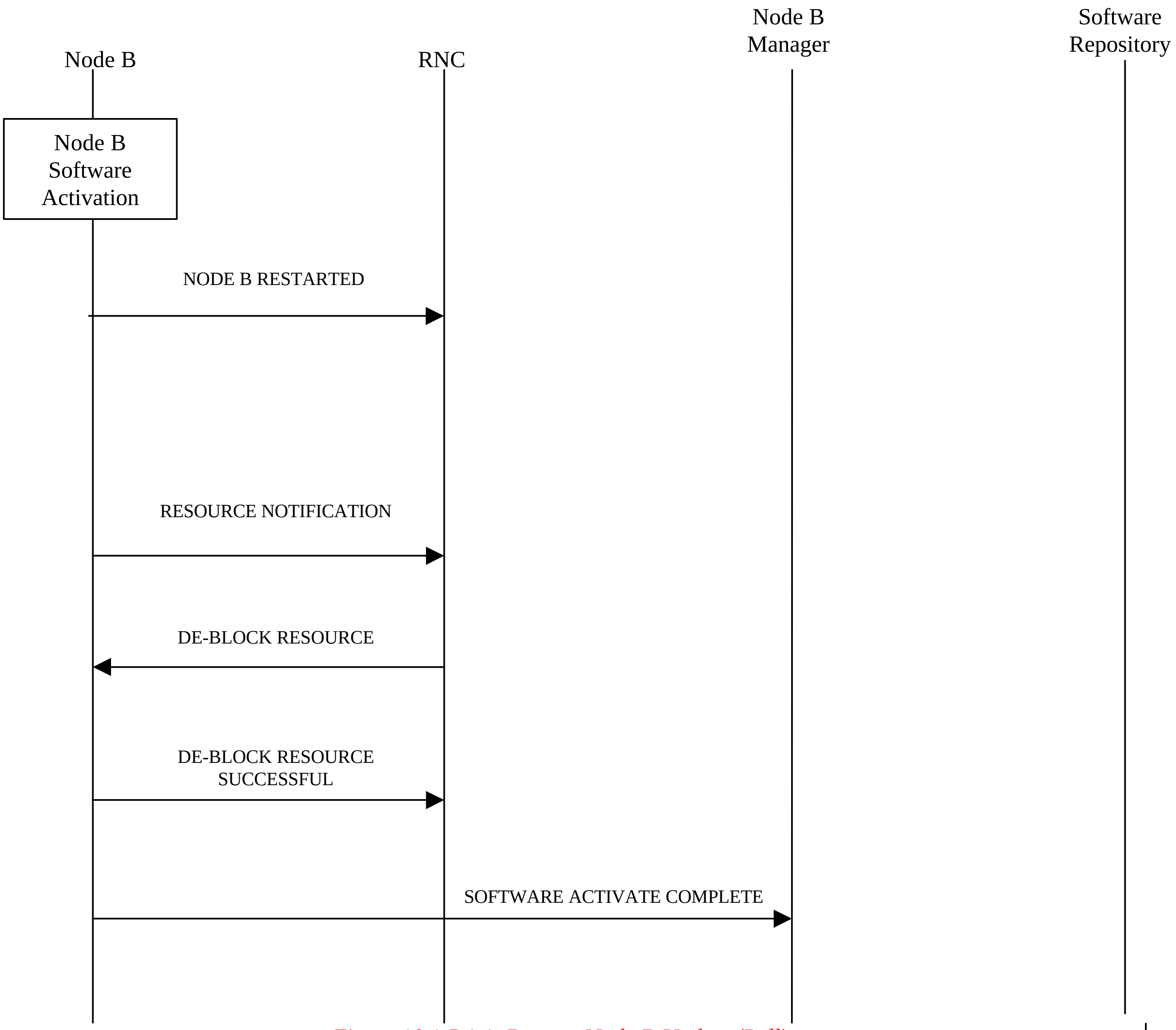


Figure 10.1.5.1.1: Remote Node B Update (Pull)

The procedure above consists of the following steps.

1. The new Node B software is loaded onto the software repository. A unique address is assigned to its location. This loading process may be performed remotely from the management system or manually by the operator.

2. The management system requests the current software status of the target Node B.

3. The Node B responds providing its software status to the management system. The management system is then able to determine whether a software update is required.

4. The management system instructs the Node B to perform a software update. The address of the new software located in the software repository is provided.

5. The Node B then determines whether the software update process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.

6. The RNC will attempt to block the resources as requested by the Node B.

7. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.

8. The Node B then requests transmission of the new software from the software repository, using the address provided from the management system.

9. The software repository responds with the new software.

10. Node B confirms receipt of the software to the repository.

11. Node B then advises the management system that the software transfer from the software repository is complete.

12. The Node B then notifies the RNC of the resources now available, and the RNC then de-blocks any resources blocked during the procedure. This allows for the circumstance where software is transferred but not immediately activated, since the RNC should recover the resources at the earliest opportunity.

13. The management system then instructs the Node B to activate the new software.

14. The Node B then determines whether the software activation process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.

15. The RNC will attempt to block the resources as requested by the Node B.

16. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.

17. The Node B then activates the new software. Should this process involve a node restart, the Node B then advises the RNC that a Node B restart has been performed (if required). This will enable the RNC to accept a controlled loss/re-establishment of communication with the Node B.

18. The Node B then indicates to the RNC the resources now available.

19. The RNC is then able to de-block any resources blocked during the procedure.

20. The Node B confirms these resources have been de-blocked and indicates to the management system that the software activation is complete.

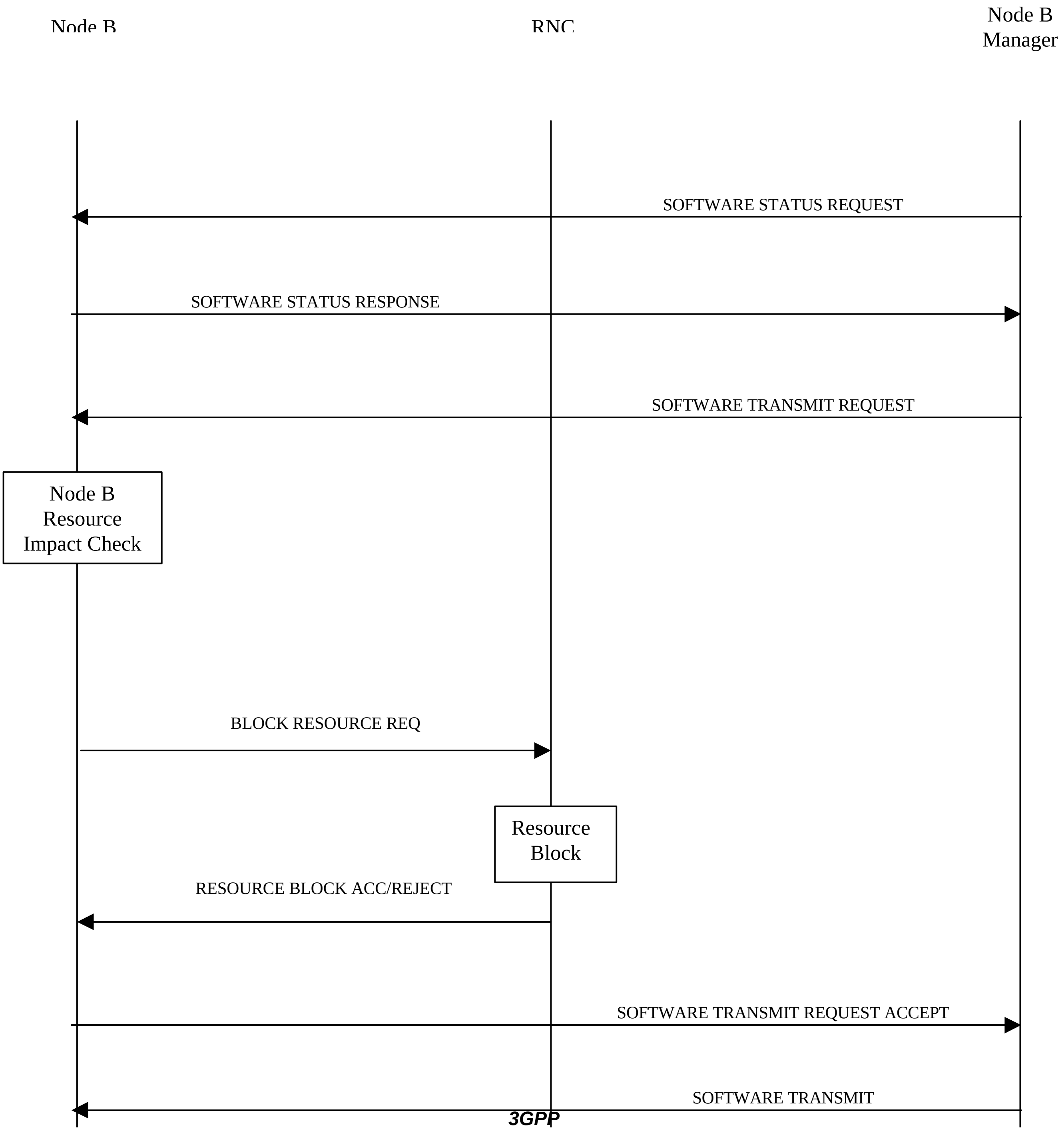
~~1.1.1.2~~Remote Update Procedure ~~-~~Push Method

The initiation of the remote upgrade of a Node B will originate from the management system. Furthermore, the management system may also directly transfer new software to the Node B as part of the procedure. This approach is referred to as a push method.

In addition, the actual process of downloading software and/or activating it may impact on the logical resources supported in Node B. It is therefore necessary to ensure the RNC is advised of such impact and provided with the opportunity to defer the operation based on the traffic conditions.

The following procedure represents one possible method by which a Node B’s software can be remotely upgraded using a push method. This procedure assumes that the associated Node B has already been installed and configured using separate procedures, and that both Iub and Implementation Specific O&M communications are therefore established.

[Editors Note: The following figure should be re-drawn in the same format as figure 10.1.2.1]



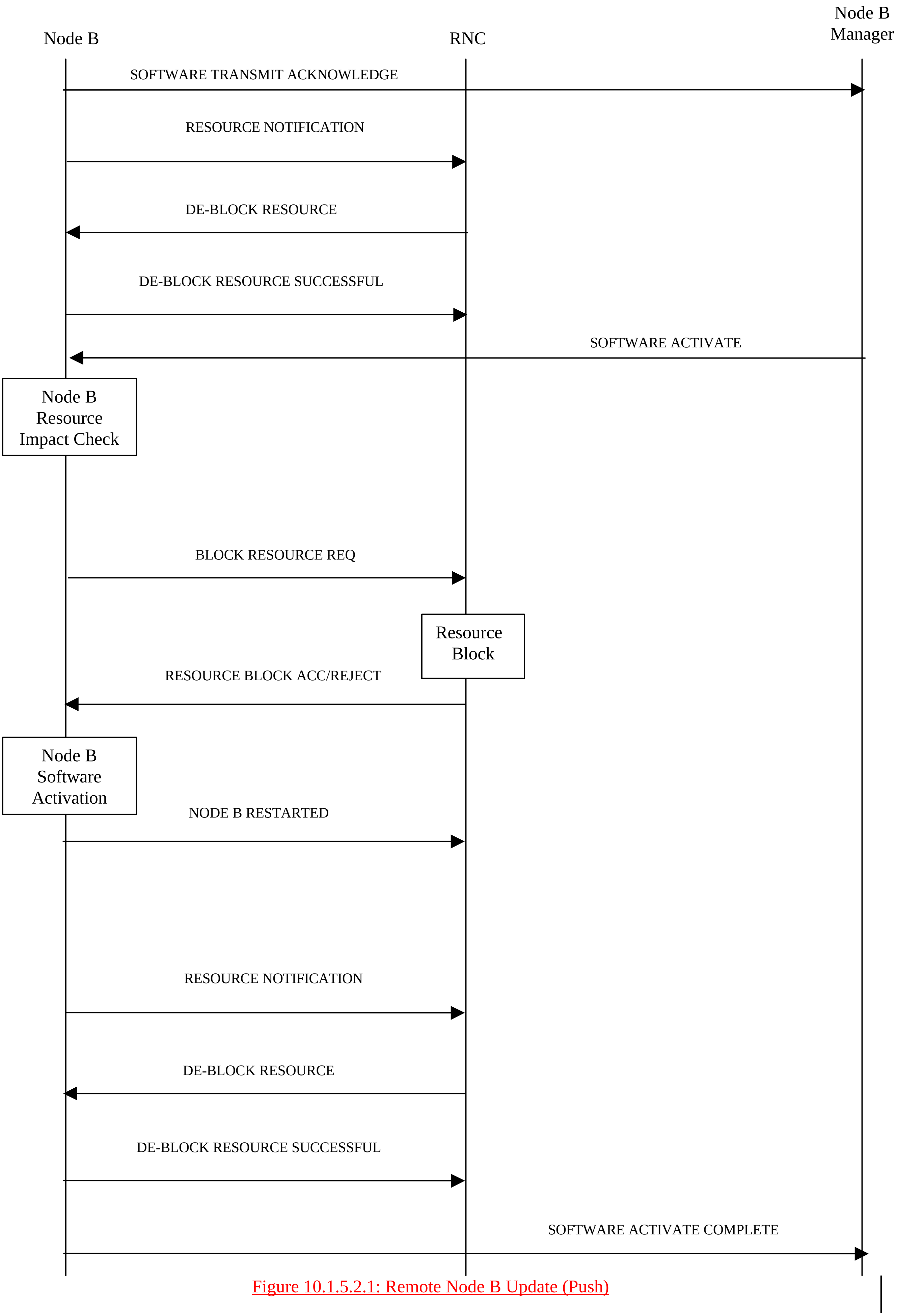

Node B
RNC
Node B Manager
SOFTWARE TRANSMIT ACKNOWLEDGE
RESOURCE NOTIFICATION
DE-BLOCK RESOURCE
DE-BLOCK RESOURCE SUCCESSFUL
SOFTWARE ACTIVATE
Node B Resource Impact Check
BLOCK RESOURCE REQ
Resource Block
RESOURCE BLOCK ACC/REJECT
Node B Software Activation
NODE B RESTARTED
RESOURCE NOTIFICATION
DE-BLOCK RESOURCE
DE-BLOCK RESOURCE SUCCESSFUL
SOFTWARE ACTIVATE COMPLETE

Figure 10.1.5.2.1: Remote Node B Update (Push)

The procedure above consists of the following steps.

1. The management system requests the current software status of the target Node B.
2. The Node B responds providing its software status to the management system. The management system is then able to determine whether a software update is required.
3. The management system instructs the target Node B that a software update must be performed.
4. The Node B then determines whether the software update process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.
5. The RNC will attempt to block the resources as requested by the Node B.
6. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
7. The Node B accepts the software update instruction from the management system and the management system responds by providing the new software.
8. Node B acknowledges to the management system successful transmission of the new software.
9. The Node B then notifies the RNC of the resources now available, and the RNC then de-blocks any resources blocked during the procedure. This allows for the circumstance where software is transferred but not immediately activated, since the RNC should recover the resources at the earliest opportunity.
10. The management system then instructs the Node B to activate the new software.
11. The Node B then determines whether the software activation process to follow will impact on the logical resources it is currently supporting. If logical resources are impacted, the Node B requests permission to block the associated resources from the RNC. This request should carry a priority indicator to indicate to the RNC whether it must block the resources immediately (RNC override) or whether it can delay or prevent the block. This priority should be derived from the initial operator request.
12. The RNC will attempt to block the resources as requested by the Node B.
13. The RNC will respond to the Node B advising of the success or rejection of the block request. In this way the RNC may delay the blocking of the resources based on the traffic conditions, unless it is instructed to block them immediately (see above). This process will be repeated until all necessary resources have been blocked.
14. The Node B then activates the new software. Should this process involve a node restart, the Node B then advises the RNC that a Node B restart has been performed (if required). This will enable the RNC to accept a controlled loss/re-establishment of communication with the Node B.
15. The Node B then indicates to the RNC the resources now available.
16. The RNC is then able to de-block any resources blocked during the procedure.
17. The Node B confirms these resources have been de-blocked and indicates to the management system that the software activation is complete.

Node B Expansion

The Node B Expansion means a integration/modification of equipment in Node B and the modification/configuration of vendor independent parameters that have to be provided by the Management system as result of a previous planning process. The Node B expansion procedure applies whenever new or additional hardware/software modules have to be installed into a previously installed Node B.

In principle, the Node B Expansion procedure can be separated into two steps:

1. Implementation Specific O&M Expansion and

2. Logical O&M Expansion

The above are for configuration of resources in Node B directly by the Management System and for configuration of logical resources owned by the RNC residing in Node B respectively. Assuming that the required configuration data, i.e. the parameters to be modified and their according value, have already been provided by a previous planning process, the procedure involves different entities for both expansion types.

Implementation Specific O&M Expansion

The Node B Expansion includes re-configuration of vendor dependent Node B parameters as well as exchange or installation of hardware modules. The pre-requisite for the Implementation Specific Node B Expansion is a completely installed and configured Node B with existing implementation specific O&M transport channel. The details of this expansion procedure are out of the scope of this document and the following figure only intends to clarify the involvement of the affected entities and the information flow between the RNC and the Node B and their management entities. The RNC is only involved in case that the availability of logical resources owned by the RNC but physically located in the Node B has changed.

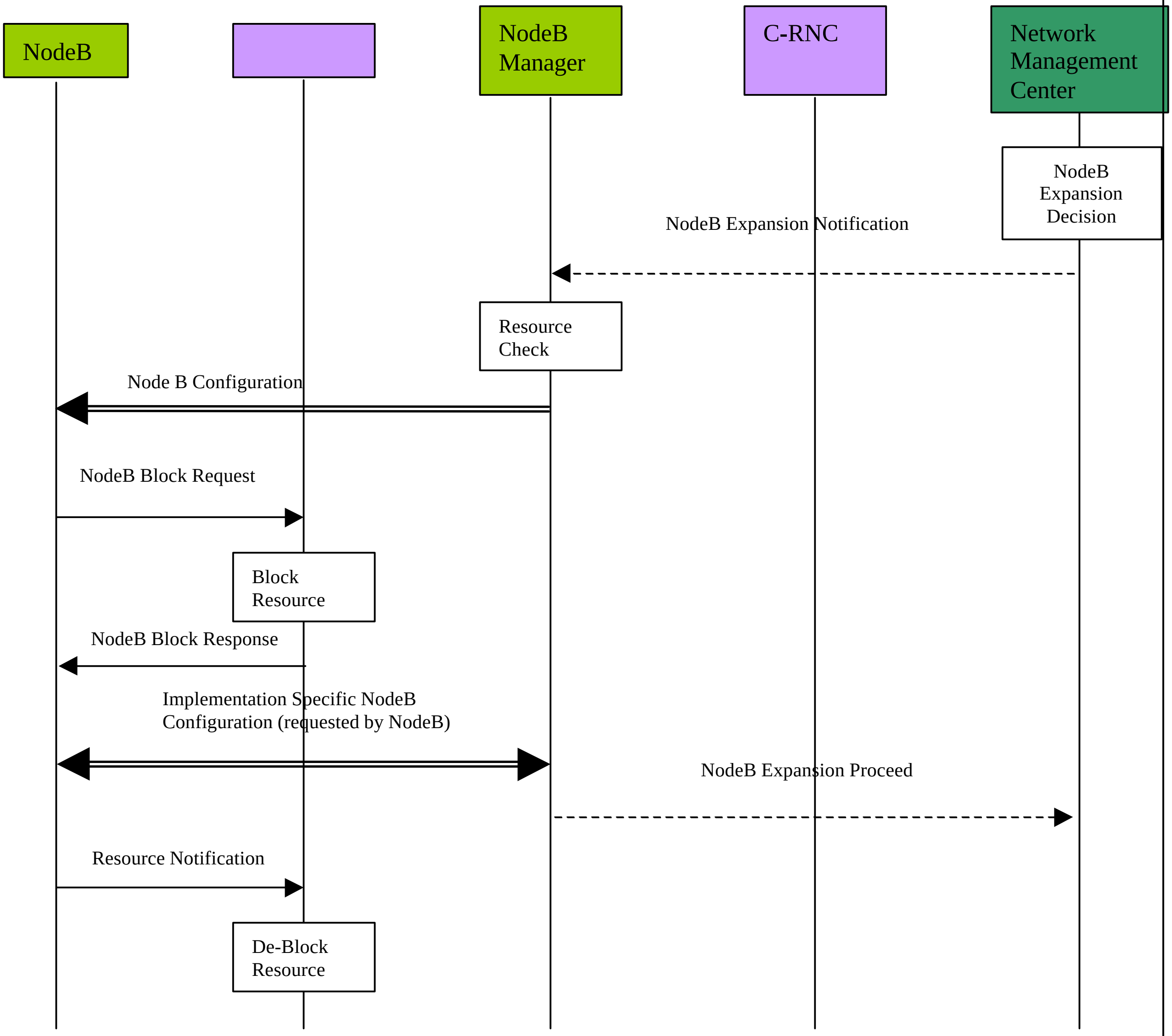


Figure 10.1.6.1.1 : Implementation Specific Node B Expansion

1. The decision for a Node B expansion is decided in the Management System by the operator. Possibly a network optimisation tool can be used for the decision. In case that there are separate sub-systems for the RNC and Node B management and there exists a separate Network Management Centre there might be a *Node B Expansion Notification* message from the Network Management Centre to the Node B Manager.

2. The Node B Manager checks the resources in order to support this expansion (link capacity, etc.) and sends a *Node B Configuration* message via the implementation specific O&M channel. It should be noted that alternatively this procedure can be replaced for example by a technician pressing a button on the hardware module to be exchanged. The following steps remain the same in the case of that manual triggering.

3. The Node B informs the RNC about the unavailability of the affected logical resource by sending a Block Request for the according resource. This request should carry a priority indicator. By interpreting the request priority the RNC can decide whether the resource must be blocked immediately or whether the RNC can delay the blocking causing a later request from Node B. The request priority should be derived from the operator expansion request.

After blocking the resource the RNC sends a *Node B Block Response* message to the Node B indicating that the according resources are blocked.

4. The implementation specific configuration should be initiated/requested by the Node B after it has received the *Node B Block Response* message. The implementation specific configuration (not depicted in detail) includes self-tests of Node B and the report of these self-tests to the Management System. After the successful implementation specific Node B expansion the Node B informs the RNC about the available resource via the *Resource Notification* message. In case of separated Node B Manager and Network Management Centre the Node B Manager informs the Management Centre about the successful implementation specific expansion with a request to proceed with the logical expansion.

5. After receiving the resource indication the RNC de-blocks the previously blocked resources and continues normal operation.

Logical Node B Expansion

The logical Node B expansion includes the re-configuration of logical resources owned by the RNC that might be physically located in the Node B. This procedure shall be used to configure new Node B elements integrated by the Implementation Specific Node B Expansion. This expansion procedure contains no hardware modifications or any other implementation specific change. This procedure is comparable to the Cellular Network Configuration Procedure.

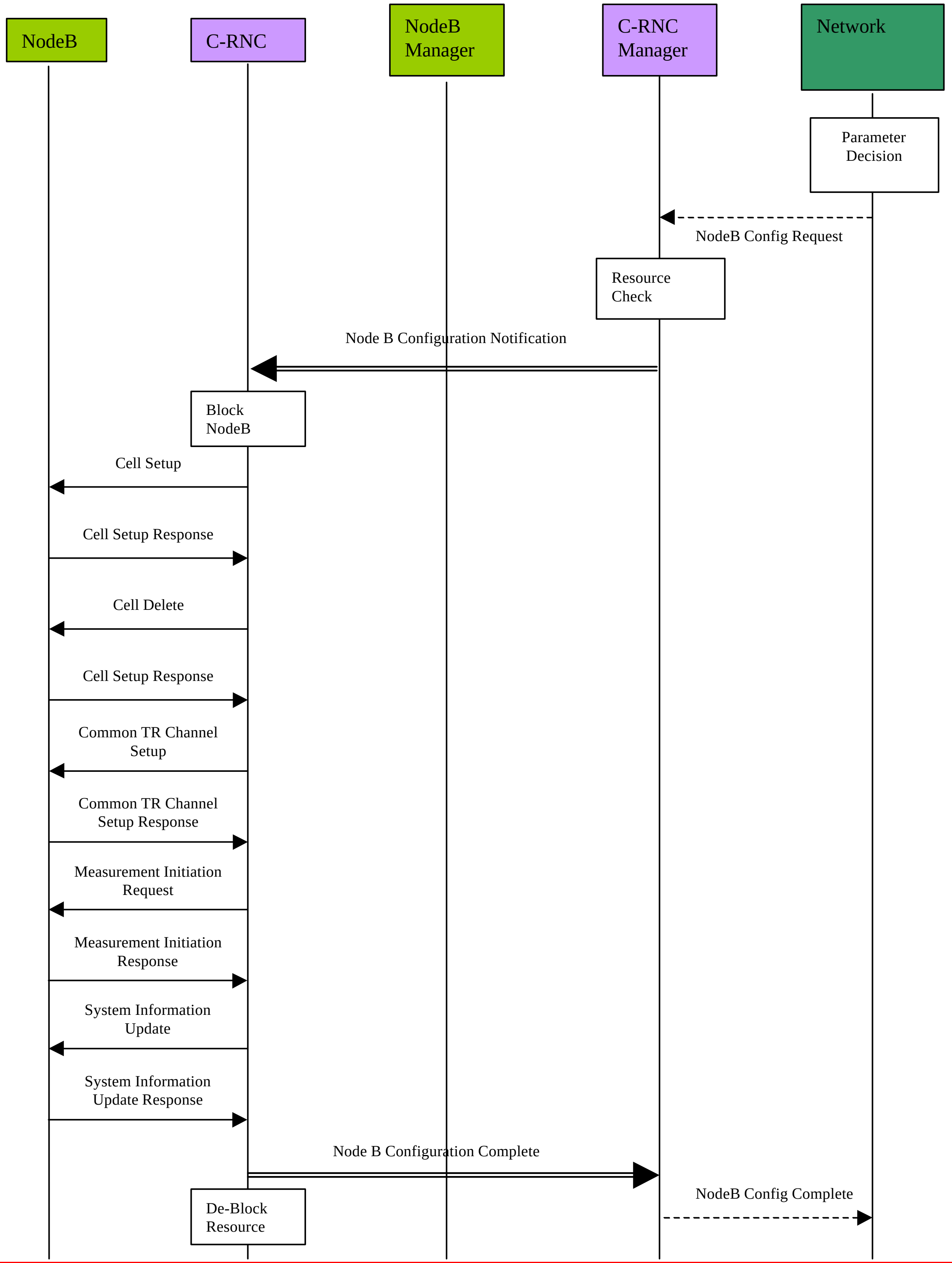


Figure 10.1.6.2.1 : Logical Node B Expansion

1. The new cell parameters or transport channel configuration is defined by the Management System as result of a previous network optimisation process. In the case of separated sub-systems for Node B, RNC and network management there might be a configuration request from the Network Management centre to the RNC Manager with all required information to establish new logical resources in the expanded Node B. It should be noted that in that case the whole procedure is triggered by the Node B Expansion Proceed message that shall be sent as final result of the implementation specific expansion.

2. The RNC Manager initiates the logical Node B expansion by sending the new parameters to the according RNC and requesting the re-configuration of the Node B.

3. Possibly the RNC blocks the affected logical resource in the Node B, e.g. a cell.

4. For cell re-configuration also the Cell Setup message can be used, since it contains all required information for an appropriate cell configuration. The Node B will respond with a successful result report or with a failure notification. The same applies for the deletion of a cell.

5. In case of common transport channel setup the RNC requests the establishment of all required channels including the transport channels on Iub. The successful establishment (or a possible failure) is reported back by a Common Transport Channel Setup Response message.

6. Possibly measurement tasks can be requested or terminated by the RNC and system information messages configured from the RNC.

7. Finally the result of the complete Node B configuration procedure is reported to the RNC Manager. The complete Node B Configuration might be reported afterwards to the Network Management Centre.

Required Actions

From the above description the required actions that have to be fulfilled by the affected network elements can be derived. The following list represents a summary of the previous procedure description with respect to actions to be performed in Node B, RNC and Management System:

- The re-configuration of implementation specific parameters and equipment shall be triggered by a request message from the Node B Manager to the Node B via the implementation specific O&M signalling channel. Alternatively a manual triggering should be possible.

- After receiving the configuration request (including possible parameters indicating which Node B parts are involved) the RNC might request the blocking of affected logical resources in the RNC.

- The Node B performs a self-test after the implementation specific configuration and sends a result report to the Management System via the implementation specific O&M signalling channel.

- Following the implementation specific Node B expansion the RNC has to be notified about the available resources.

- In order to re-configure resources owned and controlled by the RNC and physically located in the Node B (logical Node B expansion) the RNC Manager has to be notified about the implementation specific Node B expansion and has to send all required information, e.g. new cell parameters, to the according RNC as a request for configuration.

- After receiving the configuration request from the Management System the RNC has to perform all required tasks to configure the Node B properly, i.e. cell setup or deletion, establishment or release of common transport channels, or request or termination of measurement tasks in Node B..

The completion of the logical Node B expansion and the result has to be reported back to the RNC Manager by the RNC.

Node B Swap

Within the Node B Swap Procedure one or more Node B’s might be detached from RNC’s and attached to other RNC’s. For example the installation of a new RNC can trigger the Node B Swap procedure. There are potentially five steps to be performed:

1. Physical installation of the new RNC and of all links

2. Configure the new RNC

3. Re-configure the old RNC (including possible re-configuration of adjacent Node B’s attached to this RNC)

4. Detach the Node B

5. Attach the Node B to the new RNC

The Node B Swap is one of the most labour intensive procedures and an appropriate optimisation of this procedure is a valuable improvement of the overall network O&M. For operators it is important to minimise the interruption time of the Node B operation. In particular, this procedure consists of several other potentially optimised procedures. The (re-) configuration of RNC's and Node B's can be included in the Cellular Network Configuration procedure and the Node B Expansion procedure. The attachment of the Node B to the new RNC is comparable to a Node B installation. These procedures will not be described in detail, only possible trigger messages or result messages will be considered.

Assuming that all physical links and the site for the new RNC are prepared the description starts with the installation of a new Node B.

Installation of a new RNC

The installation of the new RNC consists of the following steps:

1. Establishment of the connection to the management system
2. Implementation specific initialisation of the RNC including start of all functional entities residing in the RNC
3. Establishment of all required Iu connections, e.g. signalling bearer for RANAP and ALCAP
4. Establishment of possible Iur connections, e.g. signalling bearer for RNSAP and ALCAP

After the local HW/SW installation and the potentially manual establishment of all ATM links and the connection to the RNC Manager the new RNC is initialised and configured by it's Manager (possibly initiated from the NMC). Comparably to the Node B installation the RNC may request it's initialisation from the RNC Manager. After the initialisation/configuration some self-tests shall be performed. The result of these self-tests is reported back to the Manager. Since the installation of a new RNC does not affect the NBAP messages and most of the performed actions seem to be implementation specific the RNC installation will not be described further.

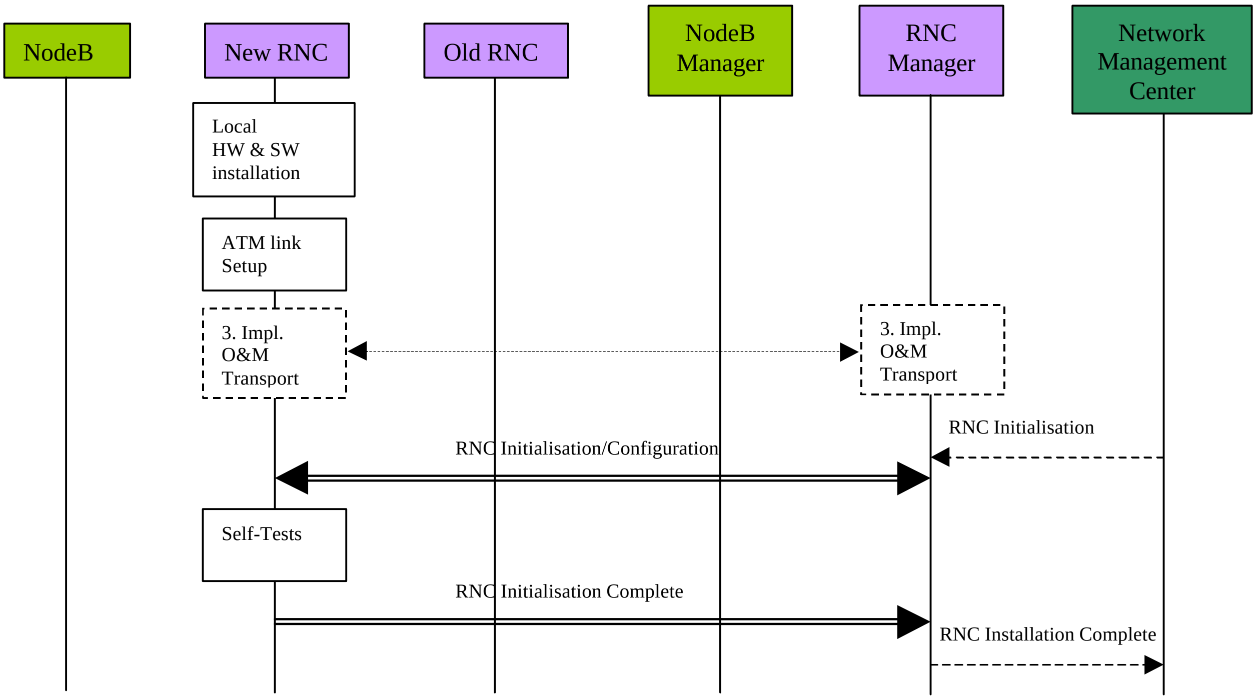

NodeB
New RNC
Old RNC
NodeB Manager
RNC Manager
Network Management Center
Local HW & SW installation
ATM link Setup
3. Impl. O&M Transport
3. Impl. O&M Transport
RNC Initialisation
RNC Initialisation/Configuration
Self-Tests
RNC Initialisation Complete
RNC Installation Complete

Figure 10.1.7.1.1 : RNC Installation

Re-configuration of old RNC

The old RNC has to be re-configured in order to adapt it to the change of resources caused by the detachment . Therefore within the Node B Swap procedure the Network Management Centre sends an RNC re-configuration request to the Manager of the old RNC. In the described example the RNC Manager for the old and the new RNC reside in the same entity. It should be noted that there might be separated Managers, e.g. in case of RNC's from different manufacturers. Since most likely the radio parameters in the cells of the old RNC change by detaching one Node B, the RNC re-configuration should re-configure the data in it's Node B's that is not implementation specific. In particular, the RNC re-configuration consists of the configuration of the RNC and several Cellular Network Configuration procedures. The Network Management Centre may send a RNC Re-configuration Request to the RNC Manager (in case that both management entities exist separately). The RNC Manager performs a modification check taking into account the capabilities of the old RNC and performs the RNC re-configuration. After some self-tests the RNC Re-configuration Complete message is sent to the RNC Manager. Following the RNC re-configuration the RNC Manager that also has control over the logical RNC resources, i.e. cells, performs one or more cell re-configuration procedures (refer to section 10.1.3). The finalisation of the whole re-configuration, i.e. RNC and cell re-configuration, is reported to the Network Management Centre.

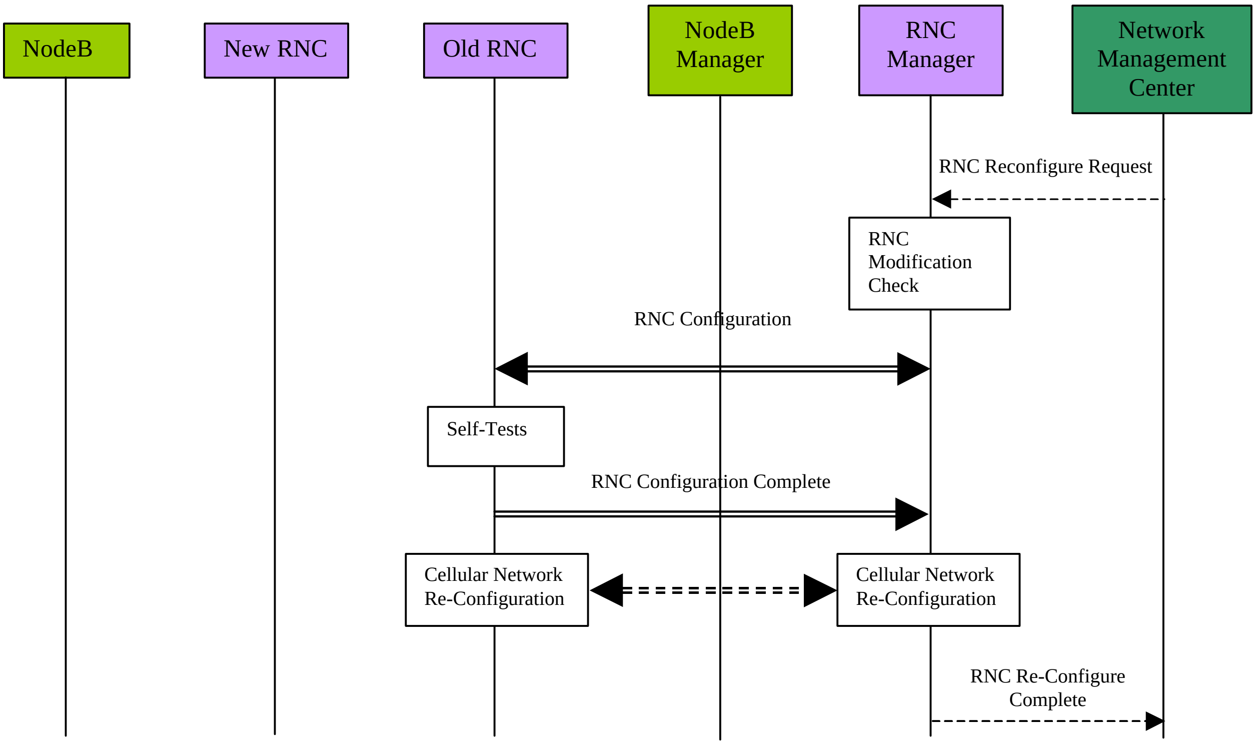

NodeB
New RNC
Old RNC
NodeB Manager
RNC Manager
Network Management Center
RNC Reconfigure Request
RNC Modification Check
RNC Configuration
Self-Tests
RNC Configuration Complete
Cellular Network Re-Configuration
Cellular Network Re-Configuration
RNC Re-Configure Complete

Figure 10.1.7.2.1 : RNC Re-configuration

Node B Detachment

First the Network Management Centre requests the detachment from the according Node B Manager. The Node B Manager informs the Node B (via implementation specific O&M signalling) that the Node B will be detached. After receiving the detach request the Node B asks the RNC to block the Node B's resources. Potentially this step might be performed in the reconfiguration of the old RNC. When the Node B receives the result of the blocking procedure from the RNC, it reports it's blocked-state back to the Node B Manager and initiates it's detachment. The subsequent implementation specific detachment includes the release of established connections (signalling bearer for NBAP, ALCAP and implementation specific O&M). The completion of the detachment should be reported to the Network Management Centre.

New Installation

As soon as the Network Management Centre receives the Node B Detach Complete message, it may trigger the new installation of the detached Node B to the new RNC. For example, the Network Management Centre may inform the installation technician to install the Node B. The remaining installation process is the same as for normal Node B installation. Please refer to the Node B installation procedure for details (see section 10.1.9).

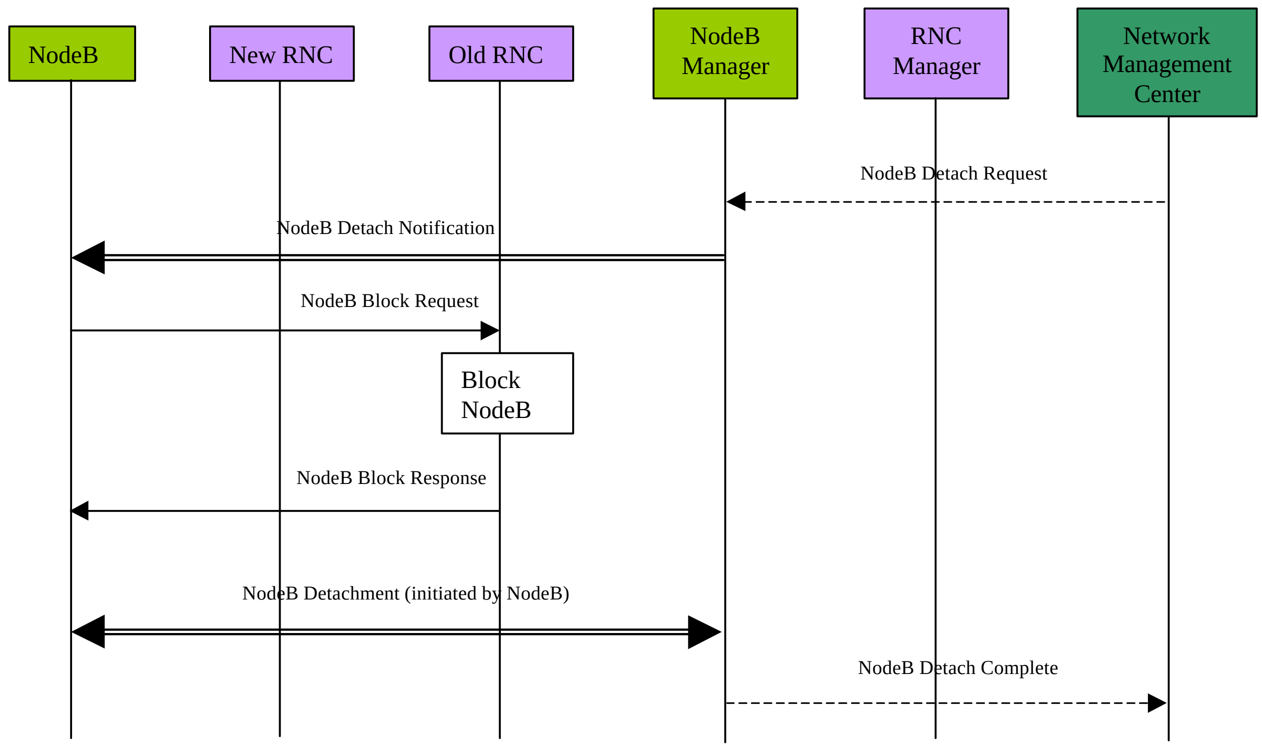


Figure 10.1.7.4.1 : Node B Detach

- Since the Management System receives separate reports for each sub-procedure, i.e. for RNC installation, Node B installation and RNC re-configuration the whole procedure can be seen as successful if all sub-reports indicate successful sub-procedures.

Network Monitoring and Fault Management Procedures

The Network Monitoring and Fault Management Procedures observe the status of network elements and handle alarm and event notifications. In addition to network generated information customer complaints may be considered. Since inherently most faults and alarms are related to vendor specific hardware and software, most functions of the fault management are implementation specific and should be handled in the implementation specific O&M part. In order to exchange failure information between Node B and RNC the logical O&M part also gets involved. In the case that any failures impact on services the RNC might report these service failures to the Management System. The relation between the UTRAN nodes with respect to the entire UTRAN network monitoring and fault management is depicted in figure 10.1.8.1below.

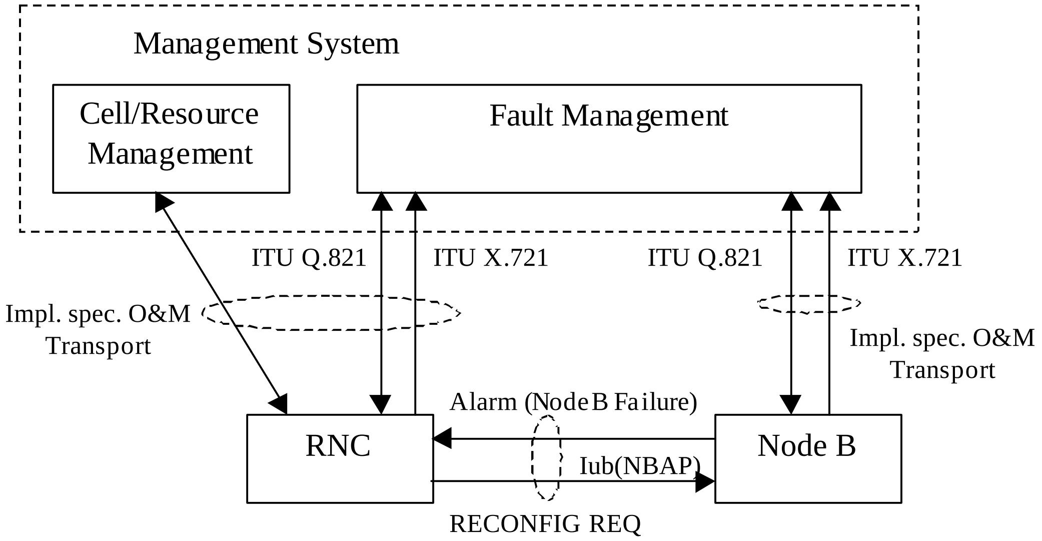


Figure 10.1.8.1 : UTRAN Fault Management

It should be noted that the Management System represents the management of the whole UTRAN and might consist of sub-systems with different functionality. The Management System should not be seen as one physical element but as a logical entity that might possibly be distributed over various physical network nodes. Within the entire procedure some other procedures, namely the block resource sub-procedure and the cell re-configuration procedure will be used. These procedures will not be described in detail.

Implementation Specific Fault Management

In case of any hardware or software failure appropriate alarms should be sent to the Fault Management sub-system of the Management System. One supported alarm message format could be based on [8]. It should be noted that the Q3 interface [9] should not necessarily be used, the alarm signalling should only be backwards compatible to the Q3 interface. These alarm signalling traffic should be carried by the implementation specific O&M transport from Node B and RNC respectively to the Fault Management sub-system. The information contained in the alarm messages shall be used to locate the failure and to repair or replace the faulty modules.

Alarm Filtering and Correlation

The correlation of alarms is crucial to reduce the alarm signalling traffic between the network nodes and the Management System. Therefore both RNC and Node B have to perform alarm correlation and filtering. The correlation of (possibly implementation specific) alarms from different Node Bs in the controlling RNC is questionable. Firstly, the interpretation of implementation specific information from the Node B by a different vendor's RNC will not be possible. Furthermore it is not ensured that the RNC always has exactly the required alarms to correlate. Hence there is a risk that the RNC reports a resulting alarm correlated from the incoming alarms that does not reflect the correct failure behaviour. Therefore no correlation of Node B alarms in the controlling RNC shall be performed.

Apart from correlation and filtering the record of alarms in a database might be beneficial in order to determine the reason for certain operation faults and to respond appropriately to customer complaints. This database may provide information about failure reasons, time and date and the location as well as the affected logical resource. Since collected and correlated alarms shall input to this database it is best located in the Management System.

NBAP alarm messages

With respect to Node B failures it is inevitable to inform the RNC about the unavailability of logical resources due to Node B hardware/software faults. In case of major failures, i.e. failures that significantly limit the operation in one cell or in the entire Node B, the RNC should inform the Management System. There might be two stages in handling major failures. In the first stage the RNC performs some kind of emergency actions for intermediate failure handling. In case of permanent failures of non-redundant elements the Management System gets involved by initiating a re-configuration of cells or even the whole Node B. As soon as the failure in Node B has been removed and the affected resource is ready to operate the Node B notifies the RNC about the available resources. Afterwards the RNC might re-configure the Node B again to restore the old configuration before the failure.

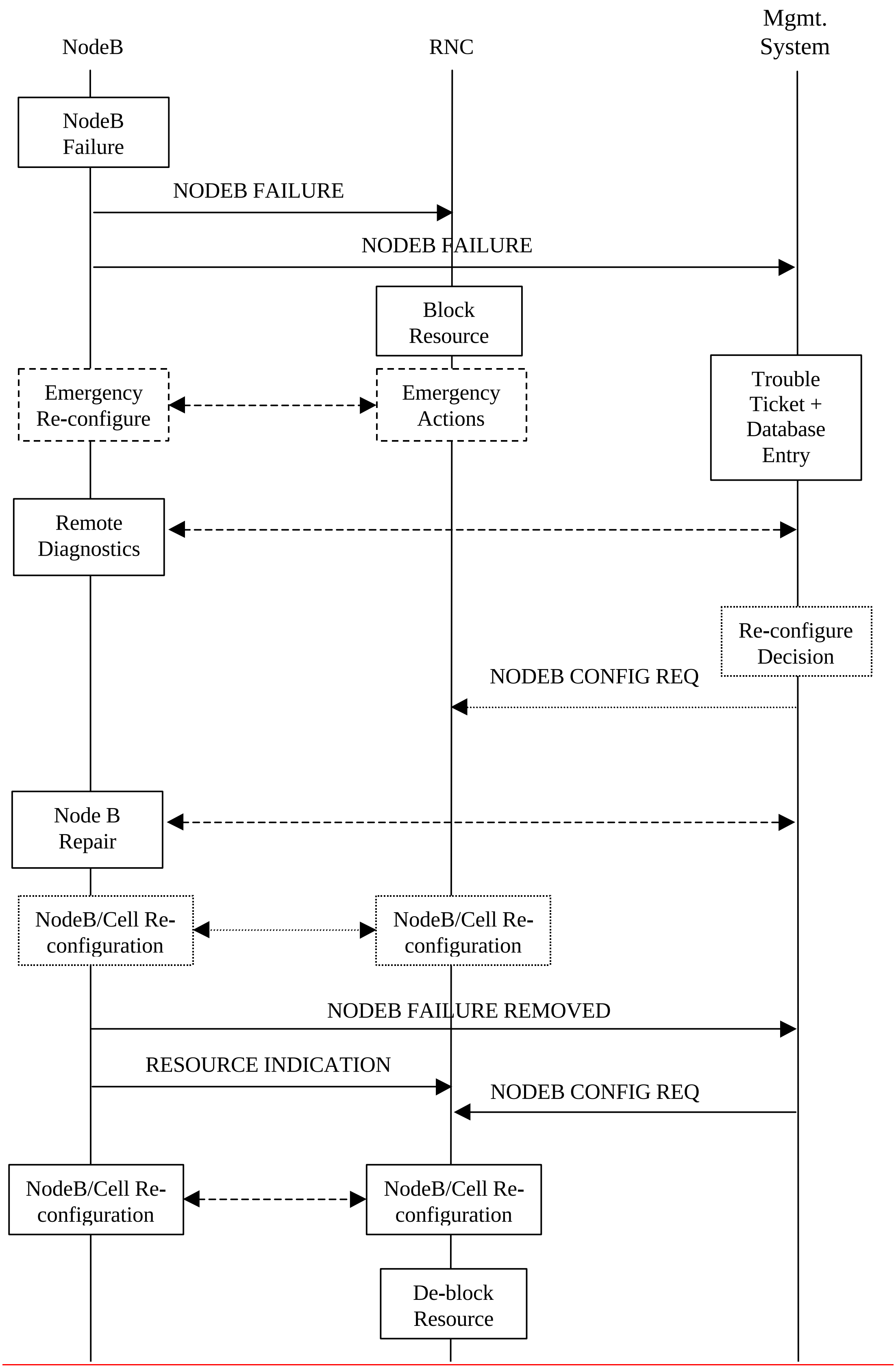


Figure 10.1.8.3.1: Node B Fault Handling Procedure

Required Actions

From the above description the required actions that have to be fulfilled by the affected network elements can be derived. The following list represents a summary of the previous procedure description with respect to the actions to be performed in Node B, RNC and Management System:

1. In the case of a failure in Node B the RNC and the Management System shall be affected by the Node B. The RNC may possibly block the according Node B resource.

2. The RNC performs some actions to reduce the impact of the failure on logical resources and services (emergency actions). This is stage one of the alarm message handling and is marked with the dashed line in figure 10.1.8.3.1 above.

3. The Management System has to start the appropriate procedure to handle the error message. Additionally, a failure database entry can be created.

4. The error message handling in the Management System should trigger a remote diagnostics procedure.

5. In the case of major failures that significantly and permanently limit the operation of the affected resource, (e.g. cell), the Management System can decide to take this resource out of order due to failure and repair. In this case a Node B or one or more cell re-configuration procedures shall be triggered by the Management System. (Note: Only other cells than the blocked cell will be re-configured, for example to extend their coverage in order to cover the blocked cell area) This is stage two of the alarm handling and might be performed in addition to the emergency handling in Node B. Stage two is marked with the dotted line in figure 10.1.8.3.1 above.

6. After the failure in Node B is removed the Node B shall send a notification to the Management System via the implementation specific O&M signalling channel and a resource notification to the RNC informing about the availability of the repaired cell.

In the case of a previous re-configuration of the affected Node B due to it's failure the RNC has to restore the old Node B configuration by performing a Node B re-configuration again.

Node B Installation

After the physical installation of Node B including all wired and wireless connections to RNC and/or Management System the signalling bearers for NBAP according to [4] and ALCAP according to [5] and [6] have to be established.

[Note: It is ffs whether the signalling bearers have to be established manually or whether an automatic establishment is possible.]

- Following to the successful establishment of the NBAP signalling bearer the Node B initiates it's configuration by sending a configuration request to the RNC.

- Since the RNC knows the address of the new Node B, the RNC establishes the signalling bearer intended for implementation specific O&M link from Node B to it’s Management System (only in case of routing the implementation specific O&M signalling via the RNC).

- The successful establishment of the implementation specific O&M signalling bearer is communicated to the new Node B including all required addresses and interface descriptions.

- The Node B requests it's implementation specific and therefore manufacturer dependent initialisation from the Management System.

[Note: It is ffs. Whether the RNC can trigger the Node B initialisation.]

- After receiving the configuration request from the Node B the vendor specific part of the Management System sends all required initialisation parameters to the Node B.

- The Node B performs a self-test after the implementation specific configuration and sends a result report to the Management System and a Node B Healthy notification to the RNC indicating that the Node B is ready to operate.

- After receiving the Node B Healthy notification (following to the initial configuration request) the RNC send all required radio and cell parameters to the Node B (including common channel setup data). These parameters must have been previously provided to the RNC from the management system.

- The Node B performs a self-test after the radio/cell configuration and sends a final result report to the Management System and a resource notification to the RNC indicating the successful radio/cell configuration.

- When the RNC receives the notification that the Node B is configured accordingly the RNC issues a BCH transmission begin notification.

History

<table>
<tr><th colspan="3">Document history</th></tr>
<tr><td>v 0.0.1</td><td>1999-04</td><td>Initial Skeleton</td></tr>
<tr><td>v 0.1.0</td><td>1999-04</td><td>Approved by WG3</td></tr>
<tr><td>v 0.1.1</td><td>1999-06</td><td>Editors proposal based on decisions in TSG-RAN-WG3#4.
• Content added to sections as per tdoc 99568 (O&M Ad Hoc #2 output).
• New section added for UTRAN O&M procedures.</td></tr>
<tr><td>V 0.2.0</td><td>1999-07</td><td>Approval of v 0.1.1 at TSG-RAN-WG3#5 (tdoc 99601).</td></tr>
<tr><td>V 0.2.1</td><td>1999-07</td><td>Editors proposal following TSG-RAN-WG3#5:
• Sub-section added into section 4 as per tdoc 99704 – taken as a working assumption.
• Text added into section 9.1 as per tdoc 99704 – taken as a working assumption.
• New sub-sections added into section 9 as per tdoc 99704 and 99775 – procedures accepted as a working assumption.
• Figure numbering and references adjusted for new text.
• Document sections re-numbered to include Introduction.</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3">Editor for 3GPP TSG RAN I3:05 is:</td></tr>
<tr><td colspan="3">Andrew De La Torre
Vodafone

Tel.: +44 1635 67 3128
Fax : +44 1635 67 3969
Email : andrew.delatorre@vf.vodafone.co.uk</td></tr>
<tr><td colspan="3">This document is written in Microsoft Word version 97.</td></tr>
</table>