IBM Tivoli Netcool

High Level Design for Mobilink

Innovise ESM
Keypoint
High Street
Slough
SL1 1DY
Tel: +44 (0) 1753 513 800
Author: Fakhra Fiaz
Title: High Level Design for
Mobilink
Version: 11

Contents

List of Figures

Mobilink OSS Expansion High Level Design

List of Tables

Mobilink OSS Expansion High Level Design

1. Document Control

Document Prepared By:
The following Innovise Limited personnel have prepared this document:

Name Title
Fakhra Fiaz Consultant

Document Reviewed By:
The following Innovise personnel have reviewed this document:

Name Title

Name	Title
Mark Jewiss	Pre-Sales Technical Consultant

Document Revision History:
The following versions have been distributed:

Version Revised and Issued By:
 11   Fakhra Fiaz

Number of Copies Submitted to Customer: 1

Number of Copies for Innovise Limited: 1

Agreed and approved on behalf of Customer

Name: _____

Title: _____ **Date:** _____

Mobilink OSS Expansion High Level Design

2. Introduction

This document has been produced to define the Design of the Tivoli Netcool product family to perform fault, performance and security management. The aim of the document is to cover the overall aspects necessary to build this Tivoli Netcool based Enterprise management infrastructure for the Mobilink OSS expansion project.

3. The Context of Solution

3.1 The Goals and Scope of Netcool NMS Solution

The Netcool NMS Solution aims to replace the current OSS system that is in place. After reviewing Mobilink's requirements, it is clear that Mobilink is looking to provide the business with the automated support required to support key business processes. The convergence of technology and operational organization is dictating that OSS architectures must be made up of solution components capable of offering generic business wide functional support, as well as specialist domain-specific functionality. In providing such broad and specialized Fault Management support, Service Providers can significantly reduce the number of bespoke

3.2 The Intended Audience

The intended audience for this document include the Mobilink Netcool OSS expansion team and the Innovise Implementation team.

4. Solution Overview Description

4.1 Introduction

A phased approach to the implementation will be used. The initial Phase will deploy the core IBM Tivoli applications, together with the probes to integrate the first set of devices, together with creating an initial set of correlations and root cause analysis and views to display the events. The second phase will add a further set of probes, and the correlations, root cause analysis and views associated with them.

4.2   Functional Architecture View
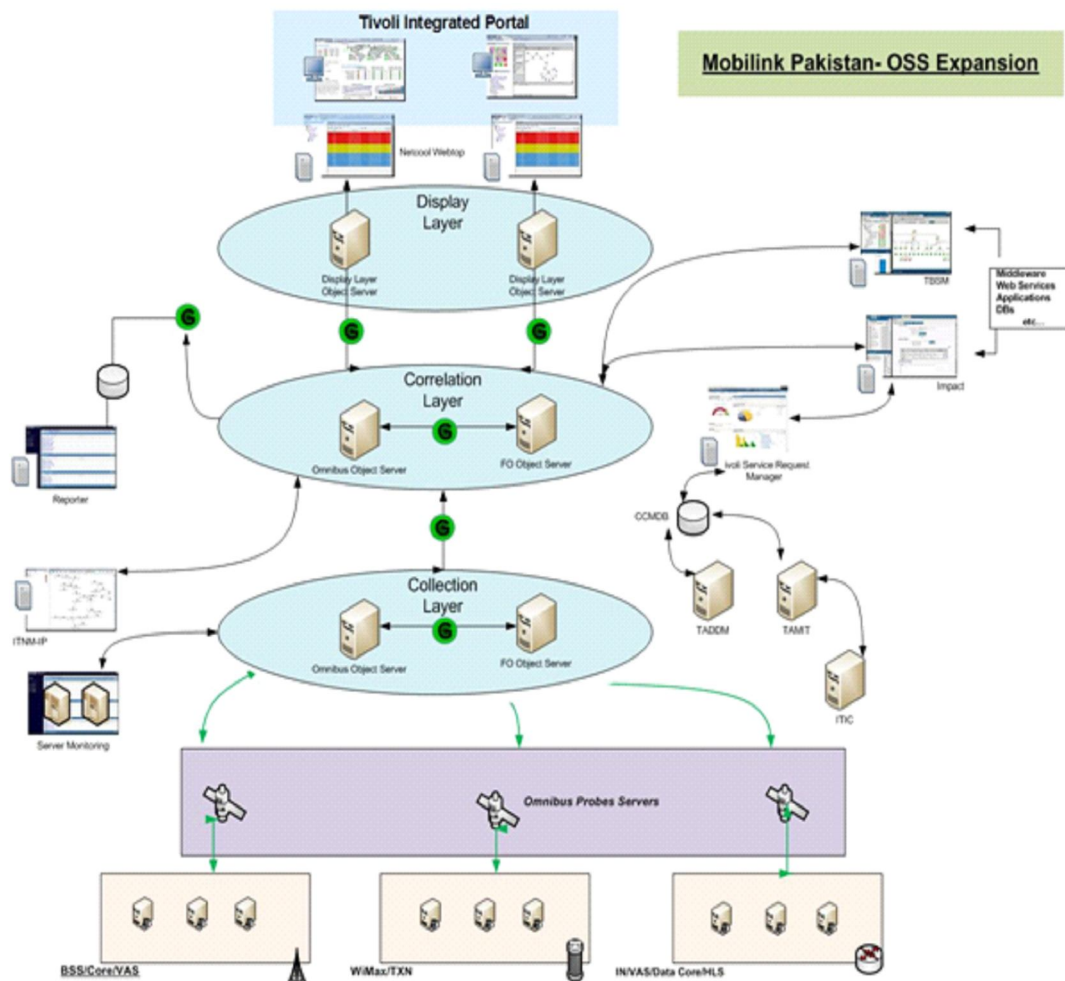
Figure 1: Functional Architecture View

4.3 System Hardware

Server Name	Hardware Platform	Processor	Memory	Hard Disk	Qty
Server 1 (Omnibus AND Impact Server)	AIX	AIX 6 for POWER V6.1	16 GB	4 x 146 GB 15K RPM SAS Disk Drive	1
Server 2 and 4 (WebTop / Portal AND Omnibus Server)	AIX	AIX 6 for POWER V6.1	16 GB	4 x 146 GB 15K RPM SAS Disk Drive	2
Server 3 (Impact AND Omnibus Server)	AIX	AIX 6 for POWER V6.1	16 GB	4 x 146 GB 15K RPM SAS Disk Drive	1
Server 5 and 6 (ITNM/IP AND CCMDB Server)	AIX	AIX 6 for POWER V6.1	24 GB	4 x 146 GB 15K RPM SAS Disk Drive	2
Server 7 and 8 (Omnibus Probe AND Reporter Server)	AIX	AIX 6 for POWER V6.1	8 GB	4 x 146 GB 15K RPM SAS Disk Drive	2
Server 9 (TADDM AND TAMIT/ITIC Server)	AIX	AIX 6 for POWER V6.1	8 GB	4 x 146 GB 15K RPM SAS Disk Drive	2
Server 10 (Tivoli Request Manager AND TADDM Server)	AIX	AIX 6 for POWER V6.1	8 GB	4 x 146 GB 15K RPM SAS Disk Drive	1
Server 11 (Tivoli Request Manager AND TAMIT/ITIC Server)	AIX	AIX 6 for POWER V6.1	8 GB	4 x 146 GB 15K RPM SAS Disk Drive	1
Server 12 (Application Manager Server)	AIX	AIX 6 for POWER V6.1	4 GB	2 x 146 GB 15K RPM SAS Disk Drive	1

Table 1: System Hardware

The diagram below shows the hardware architecture for the components to be deployed as part of the OSS Expansion project
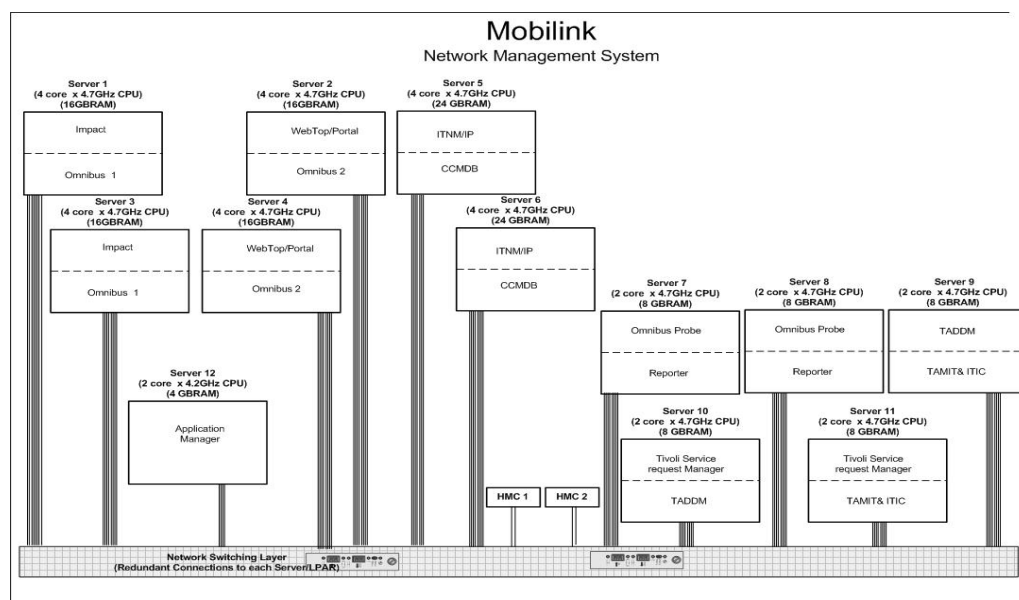
Figure 2: Hardware Architecture

Mobilink OSS Expansion High Level Design

4.4 Assumptions

This document will form the basis for a comprehensive set of functional tests, to be carried out during the duration of the project.

4.5 Solution Components

4.5.1 Alarm Surveillance

Tivoli Netcool OMNIbus

Tivoli Netcool/OMNIbus delivers real-time, centralized monitoring of complex networks and IT domains. This information can then be assigned to operators and passed to helpdesk systems as well as logged in a database.

Tivoli Netcool/OMNIbus tracks alert information in a high-performance, in-memory database, and presents information of interest to specific users through filters and views that can be configured individually. Tivoli Netcool/OMNIbus has automation functions that can perform intelligent processing on managed alerts.

The Tivoli Netcool/OMNIbus components work together to collect and manage network event information. The components of Tivoli Netcool/OMNIbus are:

- The Objectserver

  The Objectserver is an in-memory database. Alert information is forwarded to the Objectserver from external programs such as probes, monitors, and gateways, stored and managed in database tables, and displayed in the event list.

- Probes

  Netcool Probes collect alarm information from the EMS and process this information before forwarding the event data to the Objectserver. They use the rules file logic to manipulate the event elements before converting them into a readable format into fields of an alert in the Objectserver.

- Gateways

  Netcool/OMNIbus gateways enable the exchange of alerts between Objectservers Gateways can replicate alerts and maintain a backup Objectserver.

- Process Control

  Process agents are responsible for starting and stopping Netcool components and it also restarts these components in case they die abnormally. Process agents are also responsible for executing automation requests coming in from remote systems.

  The following figure shows an overview of the Tivoli Netcool/OMNIbus component architecture.
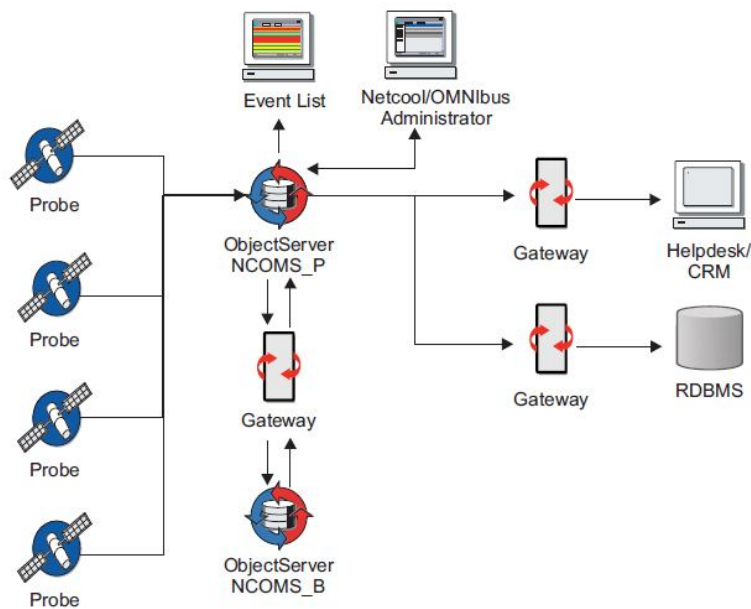
Figure 3: Netcool OMNIbus Component Architecture

Netcool Impact

Netcool/Impact provides event management and integration functionality for the Netcool suite of products. It is a platform that can be used to build new functionality into the installation.

The development tasks that are performed using Netcool/Impact are:

- Modelling data
- Configuring services
- Writing policies

Impact can be used to perform such operations as monitoring an Objectserver for events, or triggering the execution of a policy at timed intervals.

Operations that need automation can be defined by writing policies using the Netcool/Impact policy scripting language and then configuring Netcool/Impact to run them when certain conditions occur within the environment.

From a real-time operations perspective, Netcool/Impact can be understood as an automation engine that runs invisibly in the background and does not require end user interaction. Once Netcool/Impact is set up it does not require any additional management unless an implementation change is required.

Mobilink OSS Expansion High Level Design

4.5.2 Network State Management

A severity level is associated with each generated alert to help prioritize and manage alerts in the event list for network state management. There are six default severity levels, the table below shows the event severity levels.
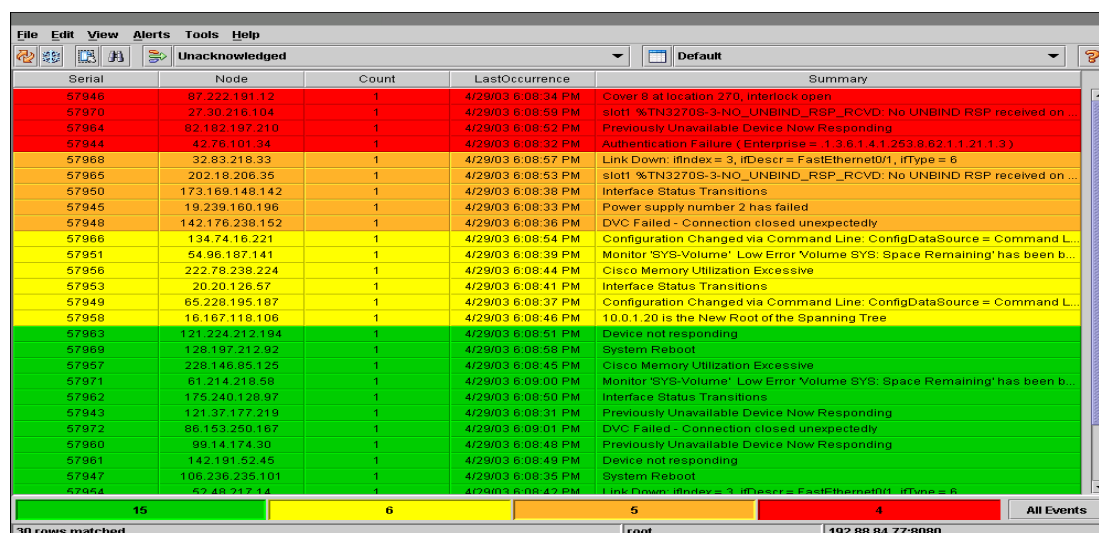
Level	Meaning	Colour
0	Clear	Green
1	Indeterminate	Purple
2	Warning	Blue
3	Minor	Yellow
4	Major	Orange
5	Critical	Red

Table 2: Event Severity Levels

Users can view alarms and their states within the Active Event List, Lightweight Event List or a Table View. The function of these alarms lists are as follows

Active Event Lists

The Active event list (AEL) allows users to execute actions such as acknowledging alerts, viewing alert journals, taking ownership of alerts and running tools

Figure 4: Active Event List

Lightweight Event Lists

The lightweight event list (LEL) provides users with the data filtering, data sorting, and information drill-down capabilities of the AEL

Mobilink OSS Expansion High Level Design

Figure 5: Lightweight Event List

Table View

The table view provides users with a static event list in the form of a table showing a defined set of alerts. The non-interactive table view provides an immediate snapshot of alert status within a monitored system.

Figure 6: Table View

Event Filters and Views

Event filters can be used to control which alerts can be displayed in an event list and Views control the columns that are displayed for the filter. This makes it easier to group events for display for network state management

13
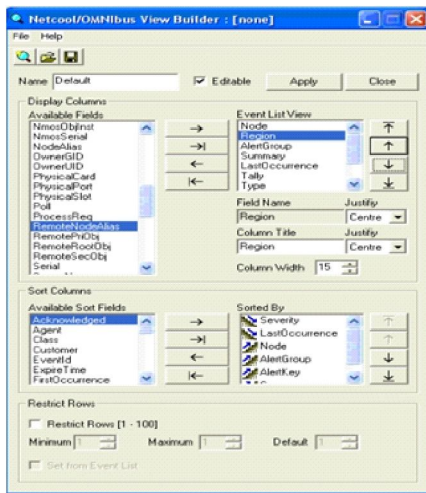
Figure 8: Netcool OMNIbus View Builder
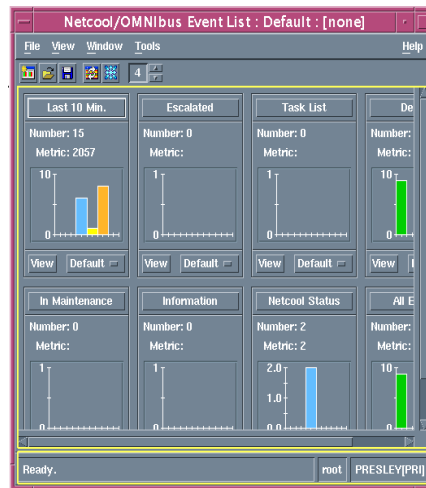
Figure 7: Netcool OMNIbus Event Filter

IBM Tivoli Netcool/ Webtop

IBM Tivoli Netcool/Webtop is a Web-based application that processes network events from Objectservers and presents the event data to users in various graphical formats.

The Netcool/Webtop Version 2.2 user interface is hosted in the Tivoli Integrated Portal framework. Tivoli Integrated Portal provides single sign-on, consolidated user management, and a single point of access for different Tivoli applications. Tivoli Integrated Portal also provides the ability to create customized pages and administer access to content by user, role, or group.

IBM Tivoli Business Service Manager

TBSM delivers the real-time information that is needed in order to respond to alerts effectively in line with business requirements. The TBSM tools are used to build a service model that is integrated with IBM Tivoli Netcool/OMNIbus alerts or with data from an SQL data source.

The diagram shown below illustrates the event flow events to TBSM. TBSM can be integrated with the Objectserver as well as external databases to bring back alarm information for service views.

Mobilink OSS Expansion High Level Design
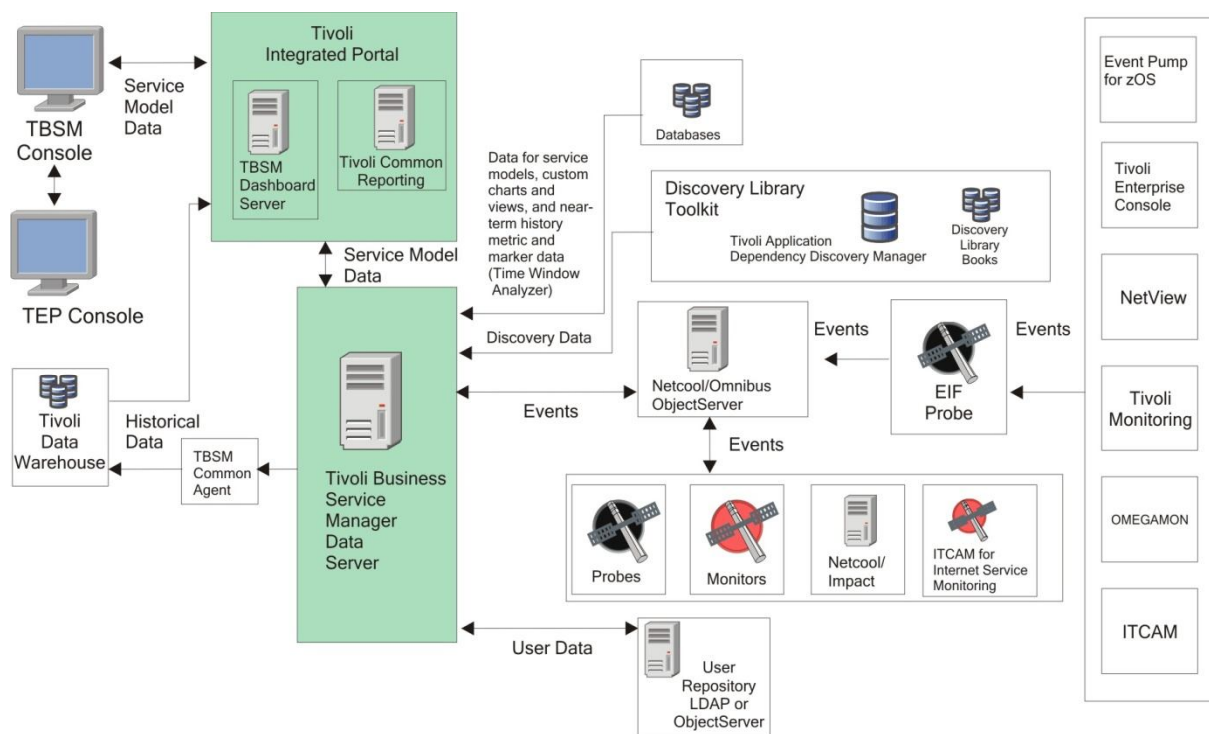
Figure 9: TBSM Event Flow Diagram

The image below shows a sample Service View in Tivoli Business Service Manager.
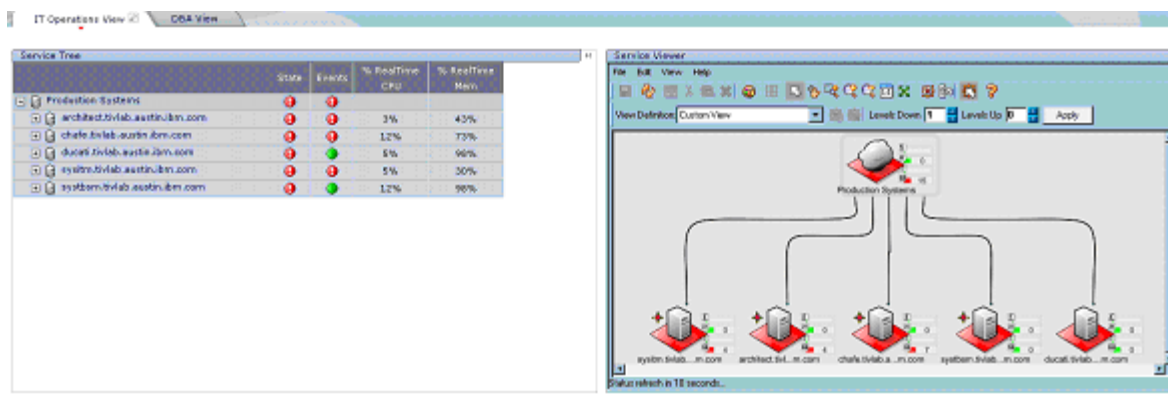
Figure 10: TBSM Sample Service View

IBM Tivoli Network Manager IP Edition

IBM Network Manager provides the features necessary to manage complex networks. These features include network discovery, device polling, including storage of polled SNMP data for reporting and analysis, and topology visualization. In addition Network Manager is able to display network events, perform root-cause

Mobilink OSS Expansion High Level Design

analysis of network events, and enrich network events with topology and other network data.

Tivoli Asset Management for IT

Tivoli Asset Management for IT enables effective management of the IT asset lifecycle to, align IT with business goals. Tivoli Asset Management for IT provides the ability to capture, integrate, and maintain technical and financial information about IT assets from planning to procurement, deployment, and maintenance to end of life and disposal. Tivoli Asset Management for IT can also be used with other products that are based on the Maximo base services, such as IBM Maximo Asset Management, IBM Tivoli Service Request Manager and IBM Tivoli Change and Configuration Management Database.

Tivoli Application Dependency Discovery Manager

TADDM is a configuration management tool that helps IT operations personnel ensure and improve application availability in application environments. TADDM provides operational staff with a top-down view of applications so that they can quickly understand the structure, status, configuration, and change history of their business-critical applications. When performance and availability problems occur, this view helps the staff to immediately isolate issues and to more effectively plan for application change without disruption. An agent-free creation and maintenance of a Configuration Management Database (TADDM database) is delivered without requiring custom infrastructure modelling. TADDM also provides complete cross-tier dependency maps, topological views, change tracking, event propagation, and detailed reports and analytics.

4.5.3   Trouble Ticketing and Resolution

Tivoli Service Request Manager

IBM Tivoli Service Request Manager has the ability to function as a service desk. It is an integrated platform that helps manage any type of critical asset or configuration item.

It is built from the ground up on the Information Technology Infrastructure Library (ITIL) framework ITIL provides a systematic and professional approach to the management of IT service provision. Adopting its guidance offers users the functionality for improved IT services through the use of proven best practice processes and improved customer satisfaction through a more professional approach to service delivery standards and guidance

Service Request Manager provides a comprehensive and modular approach to integrated service desk and service catalogue management.
A bidirectional gateway allows users to create, update, and close tickets in TSRM .The gateway allows users to create and maintain TSRM tickets from Netcool/OMNIbus events.
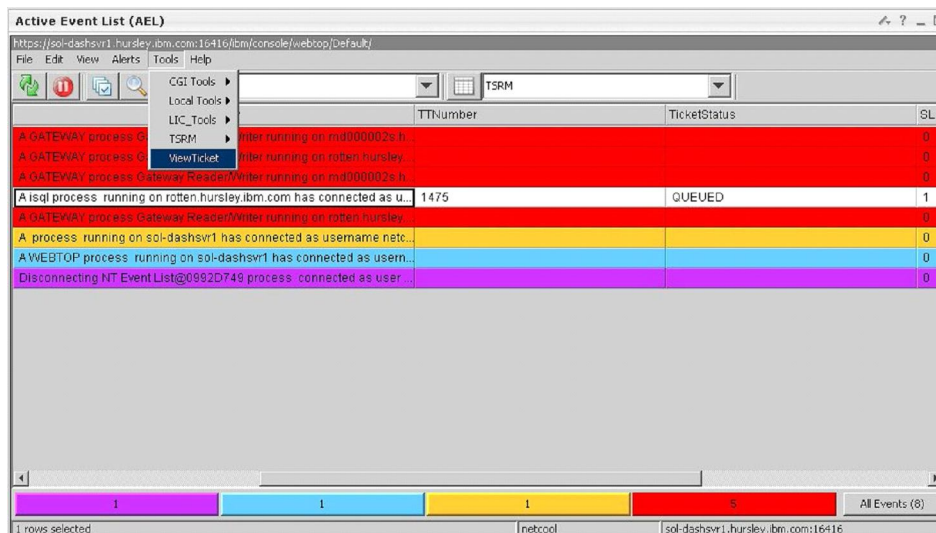
Figure 11: Associate event with TT via right click tool

4.5.4 Configuration and Change Management

Configuration and Change Management Database (CCMDB) is a tool and database that users can use to audit, and coordinate the change and configuration management processes using user interfaces and workflows. Users can create, assign, monitor, notify, and report on change requests and configuration items.

CCMDB enables users to effectively manage end-to-end IT, operations, and business processes.

Figure 12: CCMDB View

Mobilink OSS Expansion High Level Design
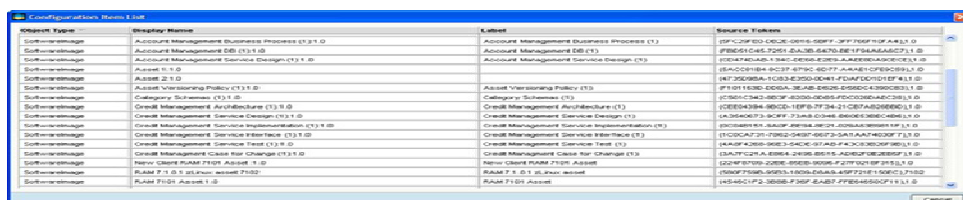
4.5.5 Reporting

Netcool Reporter

Netcool Reporter is a web-based, application that provides historical reporting functionality on a database data repository. Netcool Reporter includes a set of predefined reports for Objectserver data. Netcool Reporter captures stores and displays Netcool event data to help operators understand network behaviour.

It receives event data from the database which is passed from the Objectserver via a gateway and translates the raw data into numerous meaningful reports.
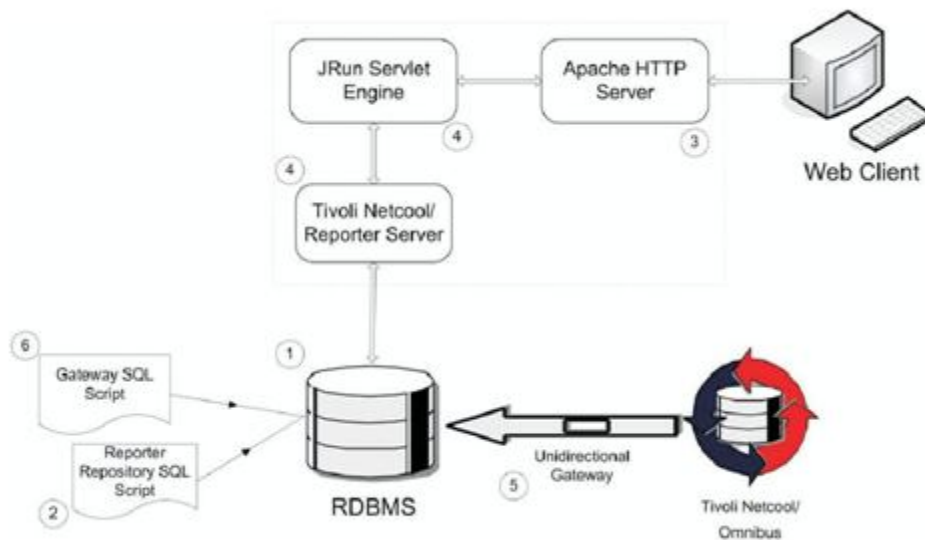
Figure 13: Netcool Reporter Base Architecture View

Tivoli Common Reporting

Tivoli Common Reporting is graphical interface for creating, viewing, and managing reports. Tivoli Common Reporting can be used to produce reports such as device availability, resource utilization, and outage history.

4.5.6 Server Monitoring

IBM Tivoli Server Monitor

IBM Tivoli Monitoring monitors and manages system and network applications on a variety of operating systems by tracking the availability and performance of the system.

The following figure illustrates the base architecture of the IBM Tivoli Monitoring software.
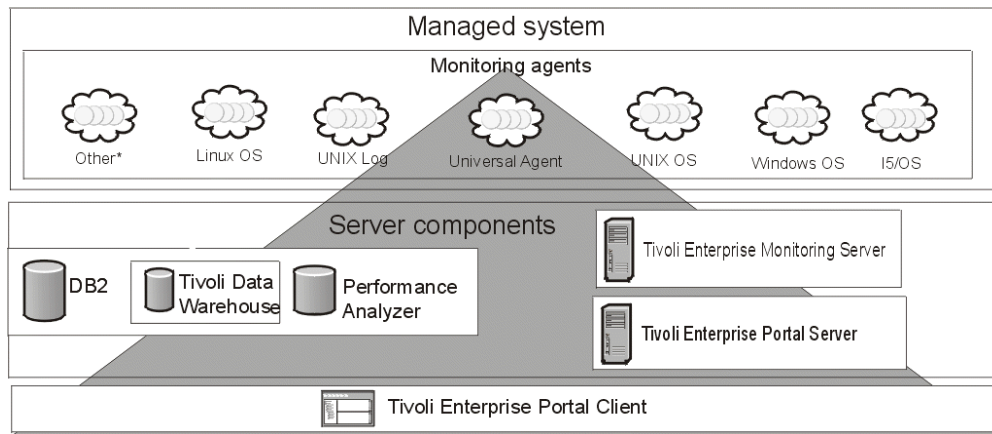
Figure 14: ITM Base Architecture

 Abilisoft Monitor the Monitor

Abilisoft MTM is not an IT infrastructure-monitoring tool, and is not intended to replace any existing system. It focuses on monitoring the tools positioned in the OSS/BSS/BSM stack by assessing the key components and automatically reporting on the true health of each. It is built with the intelligence to understand how the existing OSS toolset is designed to perform, and can therefore provide an accurate picture of availability and health of that system. Abilisoft MTM presents this information in the unique Health Analysis View; a clear and concise user interface built using the latest in rich application technology.

Abilisoft MTM brings a number of benefits to the OSS organization. It can:

- Improve the management of the OSS environment
- Reduce cost of running complex systems
- Increase efficiency of support teams.

Abilisoft MTM provides monitoring and measurement of the existing monitoring system. It is OSS vendor agnostic and can be tailored to a given solution.

The key features are:

- An instant view of availability and performance of monitored components
- The ability to monitor and record latency levels of alert flows
- The ability to correlate Hardware Problems with OSS application Problems
- The ability to record OSS configuration changes and to correlate these with possible changes in OSS performance.

Abilisoft MTM automates many of the daily tasks associated with managing a production environment including:

Mobilink OSS Expansion High Level Design

- Checking the health of monitoring components
- Measuring the performance of monitoring components
- Checking throughput of events against a benchmark
- Measuring the end-user experience.

Abilisoft MTM can give faster time to recovery following a failure by providing real time diagnostic information on the failure. The system can also be configured to provide an external escalation action in response to the event, via either SMTP or SNMP.

Abilisoft MTM can be deployed with minimum development effort. It has out-of-the-box configurations for monitoring OSS applications – removing the need for the development of in-house scripts.

5. Alarm Surveillance

A Netcool OMNIbus 3 tier architecture will implemented as a solution for handling alarms. The Objectservers will run failover mode so that when the primary server goes down the backup server takes over. Below is a description of how the alarms are handled at each tier.

The correlated event information is then passed onto the Display layer which users connect to in order to view events.

The collection layer passes events to the correlation layer, where the Objectserver tools and triggers are run against the events for correlation and Impact policies run against this layer.

Probes receive events from EMS and pass events to collection layer Objectservers

Figure 15: OMNIbus 3 tier architecture view

Netcool Probes

The following probes will be installed and configured as part of phase one:

Network	EMS	Probe
BSS	Huawei BSC6000V900R008C01B051Sp18	nco_p_huawei_m2000_corba
	Motorola GSR 8	nco_p_motorola_3gpp_omcr_gsm9
	ALU B-9	nco_p_alcatel_omcr1353ra_b10
TXN	Huawei T2000	nco_p_huawei_T2000_corba
	NEC PNMS	nco_p_mttrapd
	Tellabs 8100	nco_p_tellabs_8000
Core	Siemens - Switch Commanderv11	nco_p_siemens_sc_scr12
	Huawei	nco_p_huawei_m2000_corba
	STP NetBOSS V4.4	nco_p_eaglestp

Mobilink OSS Expansion High Level Design

	NSN MSS R4	nco_p_nokia_netact_3gpp
IN/VAS	IN @COM 7.9,8.5	nco_p_mttrapd
	SMSC LogicaCMG 5.0 , 5.1	nco_p_mttrapd
ITM	IBM Tivoli Monitor Alarm handling	nco_p_eif_itm

Figure 16: Mobilink Probes

Probe rules files will need to be configured to manage the alarms. The configuration of MTTrapd probe rules file is required to group alarms with a Special ID associated to them and these alarms can be filtered within Netcool OMNIbus and Netcool Webtop.

The configuration of Huawei probe rules file will be carried out to group power alarms.

The event severity can be modified within the probe rules files once defined by Mobilink. For example currently for TXN Optical Fibre alarms, some alarms come in with the severity of Major or Minor but are treated as Critical. The severity of these alarms will be modified within the probe rules file to ensure that the alarm appears in the event list as critical.

The probe rules will be configured to modify the Node field so that the fault source and specifier are concatenated to produce the friendly name.

Discarding Alarms

It was discussed within the requirements capture phase that some alarms need to be discarded. Mobilink will discuss this with the vendors to discard alarms at that level. Alarms that will not be discarded include the following. Mobilink require all alarms that are not listed below to be discarded at probe level.

IN and @Comms Alarms

Severity	Alarm Text	Type
critical	OEM:in1ce1:+-------+ PCIMB Adapter Streams Driver [May 24 2007 14:06:02] | PCIMB | Copyright 1998-2006 [Ulticom, Inc] +-------+ All Rights Reserved	processingErrorAlarm
critical	OEM:in1ce1:Concat vdisk40: configured	processingErrorAlarm
critical	OEM:in1ce1:Critical on Host in1ce1: S80 #010, Enclosure disconnected	processingErrorAlarm
critical	OEM:in1ce1:Critical on Host in1ce1: S80 #010, S80 #056, Enclosure disconnected	processingErrorAlarm
critical	OEM:in1ce1:DTCP node name : in1ce1	processingErrorAlarm
critical	OEM:in1ce1:EVENT NU (nucleus.c,1575) Database 1 is ONLINE. dtcp_nodename: in1ce1 dtcp_nodeid: 0	processingErrorAlarm
critical	OEM:in1ce1:EVENT NU (nucleus.c,2037) Sync Configuration from node: in1ce1	processingErrorAlarm

Mobilink OSS Expansion High Level Design

critical	OEM:in1ce1:LOG3.012695504311080025 0 6 0 Version 4.1 SIS EVENT NU (nucleus.c,1575) Database 1 is ONLINE. dtcp_nodename: in1ce1 dtcp_nodeid: 0	processingErrorAlarm
critical	OEM:in1ce1:LOG3.012695504311080025 0 6 0 Version 4.1 SIS EVENT NU (nucleus.c,2037) Sync Configuration from node: in1ce1	processingErrorAlarm
critical	OEM:in1ce1:NOTICE DM (dml.c,2756) dml thread bound to port 33570	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,2574) DTCP nodename is in1ce1	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,3351) dtcp_nodeid: 0 dtcp_dbnode: 1 dtcp_dbonline: 1	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,3357) DML NODELIST	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,3361) name: in1ce1	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,3361) name: in1ce2	processingErrorAlarm
critical	OEM:in1ce1:NOTICE NU (nucleus.c,3363) nodeid: 0 version: 4 addr: 2 flags: 0x3 node_status: 1	processingErrorAlarm
critical	OEM:in1ce1:pcimb7 is /pci@8a,4000/pci12d4,200@3	processingErrorAlarm
critical	OEM:in1ce1:RCFS module initialized (ics level 1)	processingErrorAlarm
critical	OEM:in1ce1:server-mount: /global/TspFt on /dev/vd/vdisk800, state=2,pfs=ufs,logging,largefiles,rw,suid	processingErrorAlarm
critical	OEM:in1ce1:WARNING GW (gateway.c,3342) dtcp_gw_sniffer_add_vif: arphandle=0x2215c3c8	processingErrorAlarm
critical	OEM:in1ce2:Concat vdisk40: configured	processingErrorAlarm
critical	OEM:in1ce2:DTCP node name : in1ce2	processingErrorAlarm
critical	OEM:in1ce2:NOTICE: I_PLINK IPv4	processingErrorAlarm
critical	OEM:in1ce2:NOTICE: Ulticom SCTP Driver loaded	processingErrorAlarm
critical	OEM:in1ce2:pcimb7 is /pci@8a,4000/pci12d4,200@3	processingErrorAlarm
critical	OEM:in1ce2:RCFS module initialized (ics level 1)	processingErrorAlarm
critical	OEM:in1ce2:tcpsniff_ioctl:SIOCLIFFAILOVER: movetoindex:0xa,name=fjqe5	processingErrorAlarm
critical	OEM:in1ce2:WARNING GW (gateway.c,3342) dtcp_gw_sniffer_add_vif: arphandle=0x220fa3d8	processingErrorAlarm
critical	OEM:in1ce2:WARNING: lom_upperMessageProcessing() link 5 not allocated, suppressed count 0	processingErrorAlarm
critical	OEM:in3ce1:NOTICE: alloc: /global/TspFt: file system full	environmentalAlarm
critical	OEM:in8ce1:DTCP node name : in8ce1	processingErrorAlarm
critical	OEM:in8ce1:NOTICE DM (dml.c,2756) dml thread bound to port 33542	processingErrorAlarm
critical	OEM:in8ce1:pcimb13 is /pci@9a,4000/pci12d4,200@2	processingErrorAlarm
critical	OEM:in8ce1:server-mount: /global/TspFt on /dev/vd/vdisk800, state=2,pfs=ufs,logging,largefiles,rw,suid	processingErrorAlarm

Mobilink OSS Expansion High Level Design

critical	OEM:in8ce1:server-mount: /global/TspOam on /dev/vd/vdisk810, state=2,pfs=ufs,logging,largefiles,rw,suid	processingErrorAlarm
critical	OEM:in8ce1:WARNING GW (gateway.c,3342) dtcp_gw_sniffer_add_vif: arphandle=0x22138948	processingErrorAlarm
critical	OEM:in8ce1:WARNING: lom_upperMessageProcessing() link 1 not allocated, suppressed count 0	processingErrorAlarm
critical	OEM:in8ce2:(c7sccp @ Q 0x9DDAF168) N1.SCCP, sccp_unbind() ssn=146, class=0x20, name=in8ce2.BU_DP146_513	processingErrorAlarm
critical	OEM:in8ce2:Concat vdisk40: configured	processingErrorAlarm
critical	OEM:in8ce2:DTCP node name : in8ce2	processingErrorAlarm
critical	OEM:in8ce2:Mirror vdisk41 Piece 0 disabled - dkmirror -d	processingErrorAlarm
critical	OEM:in8ce2:NOTICE: Ulticom SCTP Driver attached	processingErrorAlarm
critical	OEM:in8ce2:NOTICE: Ulticom SCTP Driver loaded	processingErrorAlarm
critical	OEM:in8ce2:pcimb7 is /pci@8a,4000/pci12d4,200@3	processingErrorAlarm
critical	OEM:in8ce2:RCFS module initialized (ics level 1)	processingErrorAlarm
critical	OEM:in8ce2:tcpsniff_ioctl:SIOCLIFFAILOVER: movetoindex:0xa,name=fjqe5	processingErrorAlarm
critical	OEM:in8ce2:WARNING GW (gateway.c,3342) dtcp_gw_sniffer_add_vif: arphandle=0x2211e688	processingErrorAlarm
major	OEM:in1ce1:EVENT NU (nucleus.c,2261) Node : in1ce2 has LEFTCLUSTER Now	equipmentAlarm
major	OEM:in1ce1:LOGLOG3.012695532311080025 0 6 0 Version 4.1 SIS EVENT DB (database.c,513) GATEWAY in1ce2 went down. Version SIS EVENT DB (,) GATEWAY went down.	equipmentAlarm
major	OEM:in1ce1:LOGLOG3.012695532311080025 0 6 0 Version 4.1 SIS EVENT NU (nucleus.c,2222) Node : in1ce2 is going DOWN Now. Version SIS EVENT NU (,) Node : is going DOWN Now	equipmentAlarm
major	OEM:in1ce1:Marking CE in1ce2 down due to timeout	equipmentAlarm
major	OEM:in1ce1:Mirror vdisk21: 1 online piece left - this mirror disk is now NOT-MIRRORED	equipmentAlarm
major	OEM:in1ce1:WARNING: Mirror vdisk21: No online pieces left - this mirror disk is now DOWN	equipmentAlarm
major	OEM:in1ce2:Marking CE in1ce1 down due to timeout	equipmentAlarm
major	OEM:in1ce2:Mirror vdisk21: 1 online piece left - this mirror disk is now NOT-MIRRORED	equipmentAlarm
major	OEM:in3ce1:WARNING: /pci@WARNING: /pci@81,2000/fibre-channel@1/sd@1,0 (sd370): Error for Command: Error Level: Retryable,/fibre-channel@/sd@, (sd): Error for Command: Error Level: Retryable	equipmentAlarm
minor	BU_DP146_259:GTT failed: error returned from GTTrans()	communicationsAlarm
minor	DB:in8ce1:operation disallowed: snapshot	processingErrorAlarm

Mobilink OSS Expansion High Level Design

	controlfile enqueue unavailable	
minor	DP146_1_1_1:Aborted 2 dialogs within the last 60 seconds due to expired lifetime.	processingErrorAlarm
minor	DP146_1_1_1:Sending TCAP request failed	communicationsAlarm
minor	DP146_3_1_3:Could not construct communication block [APIErr: "No TRANSLATION FOR SPECIFIC ADDRESS, ADDRESS=P=C7, NI=0, RI=GT, GTI=4, SSN=146, TT=0, NP=1 (isdn), ES=2 (even), NAI=4 (international num), DIG=393205831000"]	processingErrorAlarm
minor	DP146_3_1_3:Sending TCAP request failed	communicationsAlarm
minor	GUISVR:Temporarily disabling the sending of messages to client process in1ce1.RtpAdmSubAgt01	qualityOfServiceAlarm
minor	OEM:in1ce1:10.14.4.30,	processingErrorAlarm
minor	OEM:in1ce1:Cabinet 10, Enclosure SGAMS00052NBM002, Battery 1: Replacement of S80 battery necessary, expiration of the life time cycle !	processingErrorAlarm
minor	OEM:in1ce1:Cabinet 10, Enclosure SGAMS00052NBM002, Battery 2: Replacement of S80 battery necessary, expiration of the life time cycle !	processingErrorAlarm
minor	OEM:in1ce1:gethostbyname: error in solctr_collectTrustedHosts during resolution of trusted hosts in the dtcpnfd.hosts file	processingErrorAlarm
minor	OEM:in1ce1:No new trusted hosts collected. The existing ones are:	processingErrorAlarm
minor	OEM:in1ce1:Remote file guiserver.client.tbl.99 exists and does not have the same time stamp or size as local file	processingErrorAlarm
minor	OEM:in1ce1:Remote file Meas.N5.99.0326 exists and does not have the same time stamp or size as local file	processingErrorAlarm
minor	OEM:in1ce1:Remote file rc.N1.99 exists and does not have the same time stamp or size as local file	processingErrorAlarm
minor	OEM:in1ce1:Setup vip. addr = 0xa0e0409	processingErrorAlarm
minor	OEM:in1ce1:Tore down vip. addr = 0xa0e0509	processingErrorAlarm
minor	OEM:in1ce1:WARNING DB((dbmaintainer.c,1508) Place_Req(0xa0e0515/4887,0xa0e0509/445): cant elect target	equipmentAlarm
minor	OEM:in1ce2:1102 - RMS not running on rms_in1ce1	processingErrorAlarm
minor	OEM:in1ce2:guiserver.client.tbl.99 file header/footer is corrupted	processingErrorAlarm
minor	OEM:in1ce2:No new trusted hosts collected. The existing ones are:	processingErrorAlarm
minor	OEM:in1ce2:Remote file guiserver.client.tbl.99 exists and does not have the same time stamp or size as local file	processingErrorAlarm
minor	OEM:in1ce2:Remote file Meas.N5.99.0326 exists and does not have the same time stamp or size as local file	processingErrorAlarm
minor	OEM:in1ce2:Remote file rc.N1.99 exists and does not have the same time stamp or size as	processingErrorAlarm

Mobilink OSS Expansion High Level Design

	local file	
minor	OEM:in1ce2:Setup vip. addr = 0xa0e0409	processingErrorAlarm
minor	OEM:in1ce2:Tore down vip. addr = 0xa0e0409	processingErrorAlarm
minor	OEM:in2ce1:13 - Run fcatcli(1M) to adjust configuration	processingErrorAlarm
minor	OEM:in2ce1:316 - fp_offline_ticker 20 found in /etc/system, should be 10	processingErrorAlarm
minor	OEM:in2ce1:363 - ssd_max_throttle not found in /etc/system	processingErrorAlarm
minor	OEM:in2ce1:378 - FileSystemusageWarningThreshold not found in /usr/local/elSSM/bin/ssm.conf	processingErrorAlarm
minor	OEM:in2ce1:WARNING DB((dbmaintainer.c,1508) Place_Req(0xa0e0537/1150,0xa0e0529/445): cant elect target	equipmentAlarm
minor	OEM:in3ce1:816 - Spheras agent ssmProxy not running	processingErrorAlarm
minor	OEM:in3ce2:13 - Run fcatcli(1M) to adjust configuration	processingErrorAlarm
minor	OEM:in3ce2:316 - fp_offline_ticker 20 found in /etc/system, should be 10	processingErrorAlarm
minor	OEM:in3ce2:363 - ssd_max_throttle not found in /etc/system	processingErrorAlarm
minor	OEM:in8ce1:378 - FileSystemusageWarningThreshold not found in /usr/local/elSSM/bin/ssm.conf	processingErrorAlarm
minor	OEM:in8ce1:379 - AcceptableFileSystemusageChange not found in /usr/local/elSSM/bin/ssm.conf	processingErrorAlarm
minor	OEM:in8ce2:13 - Run fcatcli(1M) to adjust configuration	processingErrorAlarm
minor	OEM:in8ce2:316 - fp_offline_ticker 20 found in /etc/system, should be 10	processingErrorAlarm
minor	OEM:in8ce2:363 - ssd_max_throttle not found in /etc/system	processingErrorAlarm
minor	OEM:in8ce2:377 - FileSystemusageWarningThreshold not found in /usr/local/elSSM/bin/ssm.conf	processingErrorAlarm
minor	OEM:in8ce2:378 - AcceptableFileSystemusageChange not found in /usr/local/elSSM/bin/ssm.conf	processingErrorAlarm
minor	OEM:ipdp1n2:13 - Run fcatcli(1M) to adjust configuration	processingErrorAlarm
minor	OEM:ipdp1n2:366 - sd_io_time not found in /etc/system	processingErrorAlarm
minor	OEM:ipdp1n2:367 - sd_retry_count not found in /etc/system	processingErrorAlarm
minor	OEM:ipdp1n2:6 - No shared storage disks found, type of shared storage system unknown	processingErrorAlarm
minor	POP:RtpAdmSubAgt02 failed health check [entry=341 PID=21546]	qualityOfServiceAlarm
minor	RtpAccPam01:Data record access failed [read blob ID 0 returns EACCDBNOTFOUND].	processingErrorAlarm
minor	RtpAccPam01:Send API acknowledge failed [RtpAccSendLockNotify] [ECOMTIMEOUT].	processingErrorAlarm
minor	RtpNm01:Process CFRAMEFwd_257 lost 0 normal and 140 high priority messages because of a full queue within the last 60 seconds.	communicationsAlarm

Mobilink OSS Expansion High Level Design

Severity	Entity	Alarm Text	Type
minor		RtpSendEvent:O&M Alarm: configuration or environment error: TicketConversion tool not started on this node.	processingErrorAlarm
minor		RtpTicManage01:Performance measuring: RtpTic_system took 15 seconds, threshold is 5 seconds.	processingErrorAlarm

Table 3: IN and @Comms Alarms

VOMS and IPDS Alarms

Severity	Entity	Alarm Text	Type
critical	@Commander	faultMgmt: MAJOR and/or CRITICAL Events were confirmed automatically !	processingErrorAlarm
critical	TopUp(VOMS)	event.ProblemEvent.REC_SAS_PORT_FAILED.description:com.sun.netstorage.fm.storade.agent.catalog.DeviceMessage(2540):event.ProblemEvent.REC_SAS_PORT_FAILED.description:S13:unknown.Port.:	processingErrorAlarm
major	TopUp(VOMS)	ERROR: PAM: AUTHENTICATION FAILED FOR root FROM 10.171.0.91	environmentalAlarm
major	TopUp(VOMS)	BRAlarm: Backup failed, exit code: 1	processingErrorAlarm
major	TopUp(VOMS)	BRAlarm: Backup failed: /opt/nsr/nsr_backup_part_exec.sh VOMS2 exit code: 1	processingErrorAlarm
major	TopUp(VOMS)	************ ACCT ERRORS : see /var/adm/acct/nite/active0325********	equipmentAlarm
major	TopUp(VOMS)	BRAlarm: Backup failed: /opt/nsr/nsr_backup_part_exec.sh VOMS2 exit code: 1	processingErrorAlarm
major	TopUp(VOMS)	BRAlarm: Backup failed, exit code: 1	processingErrorAlarm
major	TopUp(VOMS)	ERROR: PAM: AUTHENTICATION FAILED FOR root FROM 10.13.2.110	environmentalAlarm
major	IPD	reliableEvtTrans: SNMP error for NE 'IPD2-node-1' (sequence number = 12012): 'Timeout Condition Occured.'	communicationsAlarm
major	@Commander	syncing file systems	environmentalAlarm
minor	TopUp(VOMS)	error: ssh_msg_send: write	processingErrorAlarm
minor	IPD	OEM:ipdp2n2:refused connect from 172.27.104.130 (access denied)	equipmentAlarm
minor	@Commander	: [ID 831711 daemon.error] no server suitable for synchronization found	processingErrorAlarm

Table 4: VOMS and IPDS Alarms

The probe rules file will be configured to discard alarms if a burst of alarms are received from the EMS's. Mobilink will identify these alarms to configure the rules to discard the alarms at the probe level.

Mobilink OSS Expansion High Level Design

Event Resynchronization

Event resynchronization is required to allow users to select the event types to send commands to the EMS to get the required current events from the EMS and match them against the events held. This functionality is required to ensure that no alarm is missed, currently alarms are dropped in TeMip this could be due to the vendors sending the alarms or TeMip not picking up the alert. A solution is still being established for event resynchronization as the functionality needs to be developed.

5.1 Alarm Filters

In order to manage the alarms, filters will need to be configured within Netcool Webtop. The following additional fields will be created in the Objectserver to create a view for these filters.

- Domain (BSS/CORE/TXN/IN&VAS)
- Region
- Managing City
- Coverage City
- OMC/EMS Name
- NE Priority
- TSRM Liaison standard Fields (For e.g. Handled by Incident ID, Incident creation Time)
- No of Similar Alarms
- Additional Text
- Outage Flag (Maintenance Window)
- Notified to via SMS/Email

Probe rules will also need to be configured to extract the information and place in the right field.

An Alacatel BSS filter is required which will show the events from five omcr's and will be filtered by region. The same filter is also required for Huawei , Motorola and TXN alarms.

A filter is also required to show only the Critical Events. For IN/VAS alarms a filter is required within Netcool Webtop to filter @com events

Mobilink require a filter which shows probe connectivity and user interaction within Netcool. By default Netcool Omnibus and Webtop have Netcool status filters, these filters show events such as probe connectivity and user interaction.

A Netcool Webtop filter will also be created to display alarms that have not cleared within a period of time so users can delete these alarms and exclude them from reports if a resolution event is not received.

One of the requirements gathered was the ability to save filters created by users, Netcool OMNIbus and Netcool Webtop has the functionality for users to save the filters that they create.

A transient filter will also be created in Netcool Webtop to show alarms for links that are constantly fluctuating. This Filter collects events and queues them during a given timeframe. The filter will operate on the basis of whether a problem is cleared within a given timeframe. If a Clearance event is received within the timeout period, nothing is forwarded. If a Clearance event is not received within the timeout period, the problem is considered to be more serious and an event is forwarded.

An x in y filter will also be created in the Objectserver to discard events that appear 'x' many times. This will also require rules file configuration to group the 'y' type of events.

A separate alarm / event needs to be raised when Alcatel alarms are received which are based on cell level. This event should show that BTS is down. This will be configured using an impact policy when Alcatel alarms are received they will be flagged and a synthetic alarm will be raised within OMNIbus showing that BTS is down.

Alarm De-duplication

Mobilink require a similar alarm handling mechanism. A default Netcool OMNIbus trigger intercepts an attempted reinsert on the alerts.status table and increments the tally to show that a new row of this kind has arrived at the ObjectServer. It also sets the LastOccurrence field.

5.2 Correlation

This section details the event correlations that will take place as part of phase one. For each scenario a description of the requirement and a flowchart of the logic that will be created to handle the scenario are provided. The information required from Mobilink to create the policy is also included for each scenario in this section.

DRI Out of Service alarms

When a DRI Out Of Service alarm is received, the event should be held in the system without generating a trouble ticket (TT) for 10 minutes, to allow the event to clear itself within that period. If the alarm does not clear then a TT should be raised within TSRM, including the DRI density information enriched from the CMDB associated with the alarming DRI. Once the TT is raised an external command

should be executed against the DRI in order to reset it. If the DRI density is double density then 2 DRI's should be reset otherwise one DRI is reset If the reset clears the issue the TT should be closed. However if the alarm still persists after reset the DRI should be locked and unlocked and this should be updated in the TT.

DRI density information will be required from Mobilink to store in CCMDB. The external command that should be executed against the DRI in order to reset it will also be provided by Mobilink.
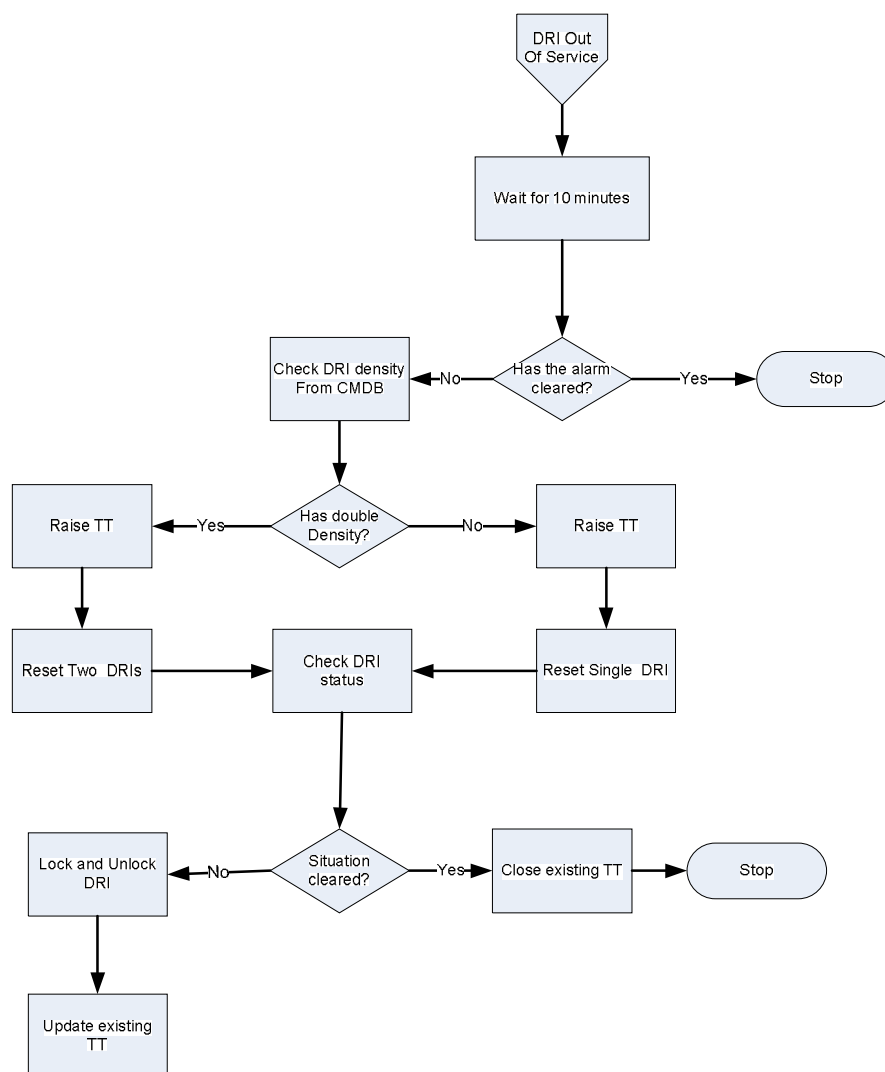
Figure 17: DRI Out-of-Service Alarm Handlin Flow Chart

BSS Environmental Alarm Handling

Multiple environmental alarms associated with the same BSS, for example GenSet alarms and Low Voltage alarms should be handled in as a single incident and not

raise individual TTs. Subsets of environmental alarms are received such as power related alarms and temperature alarms and these should be handled by subsets. The severity of the alarm should be associated with the site type and priority. When all environmental alarms have cleared for the site, the incident is deemed to be closed. The alarm should be enriched with information from the ccmdb which includes; area, address and site information. This information must be stored within the ccmdb to enrich from.
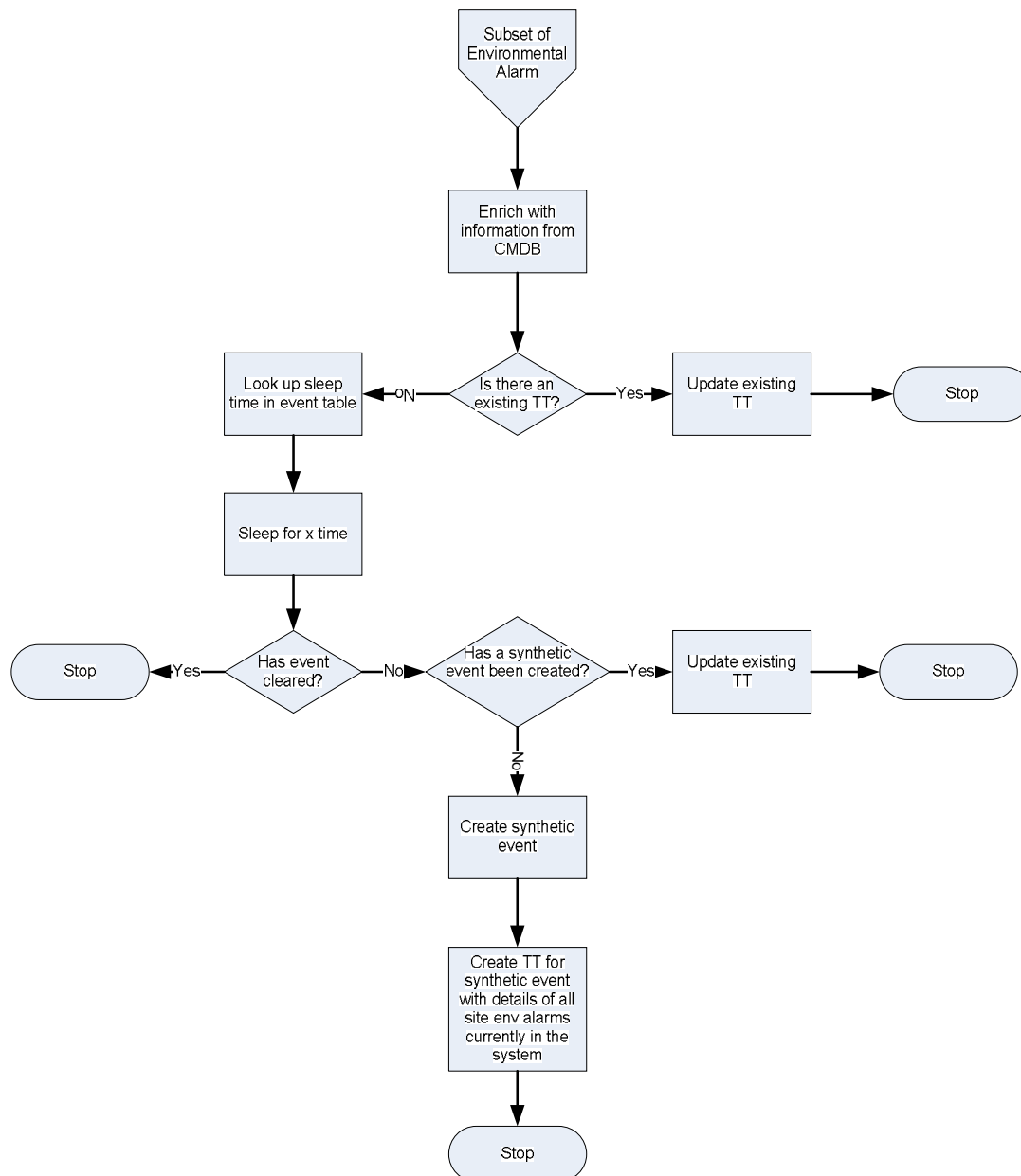
Site Down Alarm handling

When site becomes unavailable a TT should be raised after a specified time and all previously received environmental alarms should be mentioned in the TT. A single

TT is to be created when site becomes unavailable all previously received environmental alarms will be mentioned with this TT and cleared independent of environmental alarms. The following are the site down indicating alarms received from the relevant EMSs:

- Motorola - "Last RSL Link Failure"
- Alcatel - "LOSS_OF_ALL_CHAN" alarm from each of the cells at a site.
- Huawei - "LAPD OML Fault" alarm at site level and "Cell Out of Service" alarm from each of the cells at a site.

The number of cells at site information will be provided by Mobilink to store in the CCMDB.
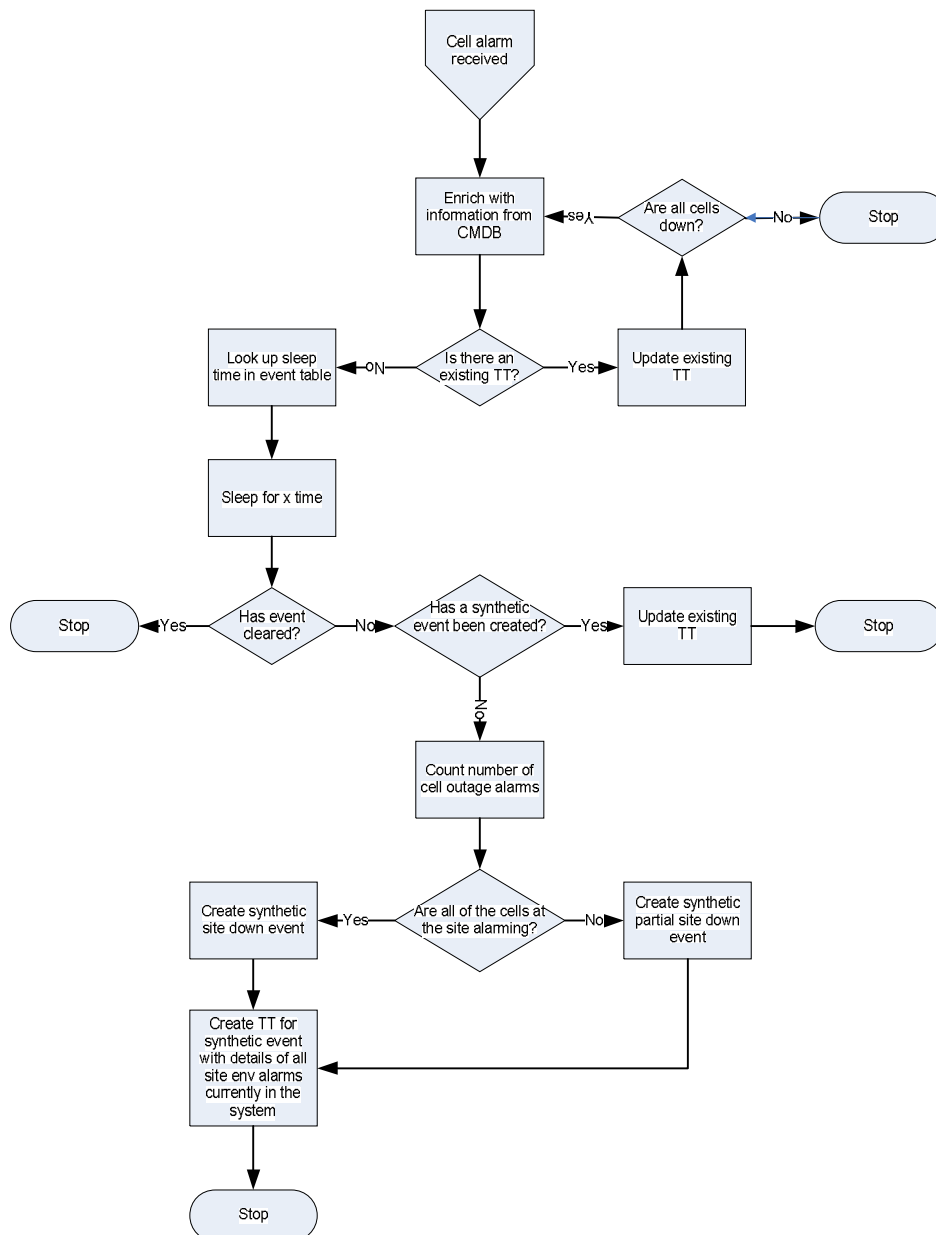
Figure 18: Site Down Alarm Handling Flow Chart

Mobilink OSS Expansion High Level Design
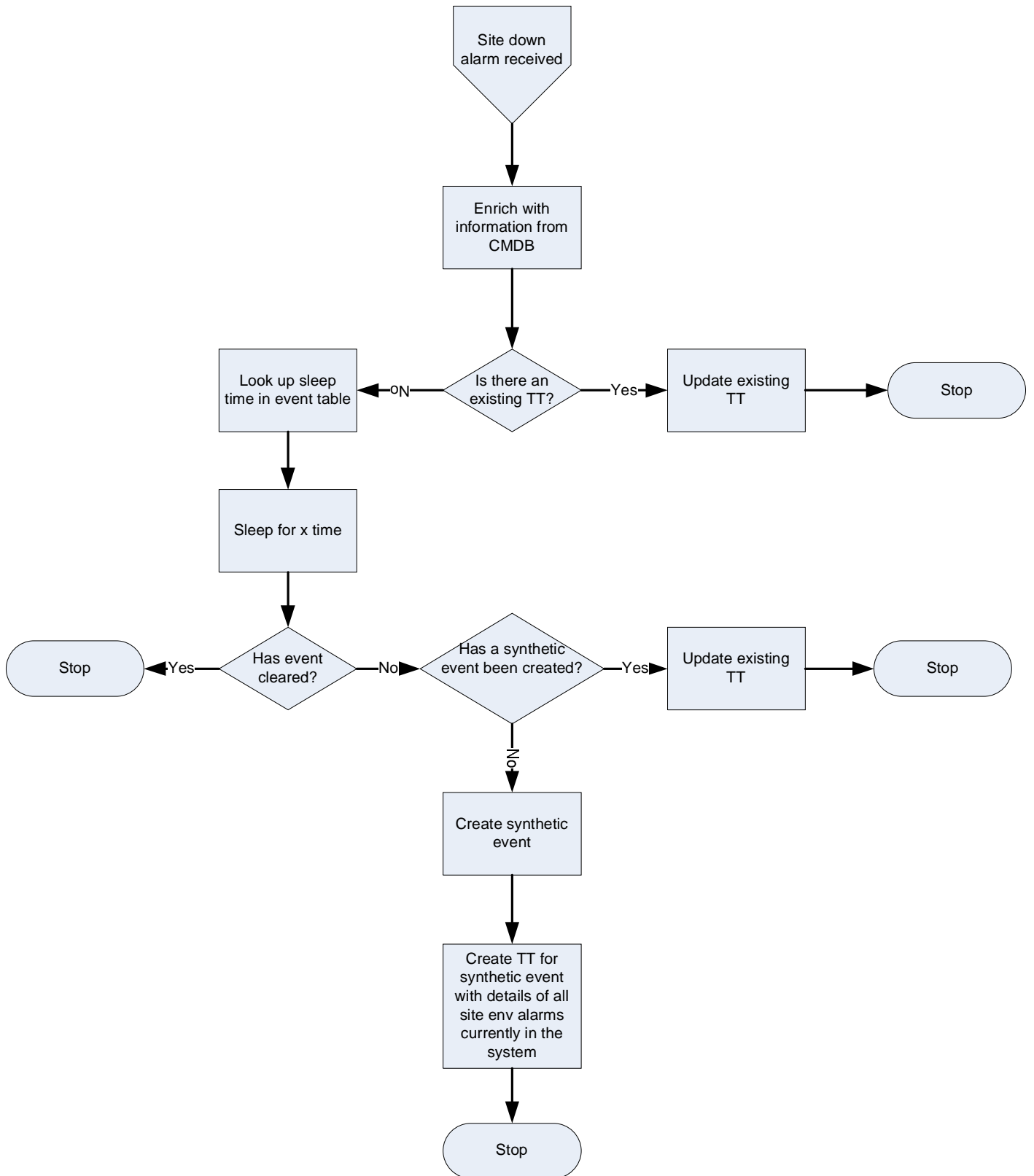
Figure 19: Site Down Alarm Handling Flow Chart

Mobilink OSS Expansion High Level Design

Multiple BTS down alarms

BTS sites are linked via microwave connections. They are configured in both hub and spoke combinations. When multiple BTS downs are detected for root TTs should be generated, after a specified wait time to allow for the events to self clear, indicating the source of the error along the microwave connection. A check needs to be made before raising the TT if the existing TT is for partial site down.

This can be achieved through the use of a parent child relationship for both the hub and spoke configurations, as long as the connectivity information is stored in a suitable place for the Impact policy to gather the connectivity data from.

The parent child event relationships, and the filters that should be used to identify the correct relationships between events and effected devices, needs to be created as this is referenced by the policy to establish the relationships. The parent child events need to be able to gather data to allow them to correlate events against each other from different devices. So if Device A is connected to device B on port X then this connectivity information needs to be looked up, to enrich the data into the event so that the parent child relationships can be established. This data needs to be gathered by Mobilink for this policy.

Figure 20: Parent/Child Event Handling Flow chart

New event in ObjectServer

Lookup potential parent events in event relationship table

Count number of potential parent events

Lookup potential child events in event relationship table

Count number of potential child events

Parent/Child Indicator Field Values
0 - Event not involved in any parent/child relationships
1 - Potential child event
2 - Potential parent event
3 - Potential potential parent and child event
4 - Established child event
5 - Established child event
6 - Child event, but no parent found
7 - Parent event, but no children found
8 - Relationships not found in table

Is number of potential child events > 0 — Yes → Set Parent/Child Indicator to 2

Is number of potential parent events > 0 — No

Is number of potential child events > 0 — Yes → Set Parent/Child Indicator to 1

Is number of potential child events > 0 — Yes → Set Parent/Child Indicator to 3

No → Set Parent/Child Indicator to 0

Parent/Child Indicator > 0 & < 4 — No → Does not require processing

Yes

Parent/Child Indicator = 3 — No → Parent/Child Indicator = 2 — No → Parent/Child Indicator = 1

Yes ↓ — Set Parent/Child Indicator of original event to 7

Yes ↓ — Set Parent/Child Indicator of original event to 7

Yes ↓ — Set Parent/Child Indicator of original event to 6

Initiate counter X

Initiate counter X

Initiate counter X

Lookup potential child events in event relationship table — No ← Is counter <= number of potential parent events

Count number of potential child events

Initiate counter X

Is counter <= number of potential child events — No → Increment counter X = X + 1

Lookup potential child event X in ObjectServer

Found relevant child event — No

Parent/Child Indicator of original event = 4 — Yes

Set Parent/Child Indicator of original event to 5

Add Serial of child event to the child event list of the original event

Set Parent/Child Indicator of child event to 4

Return child event updates to ObjectServer

Return original event updates to ObjectServer

Yes ← Is counter <= number of potential parent events

Lookup potential parent event X in ObjectServer

Increment counter X = X + 1

Found relevant parent event — No

Yes

Set Parent/Child Indicator of original event to 4

Add Serial of original event to the child event list of the parent event

Parent/Child Indicator of identified parent event = 4 — Yes

No

Set Parent/Child Indicator of parent event to 5

Return parent event updates to ObjectServer

Increment counter X = X + 1

Is counter <= number of potential child events — No

Yes

Lookup potential child event X in ObjectServer

Found relevant child event — No

Yes

Set Parent/Child Indicator of original event to 5

Add Serial of child event to the child event list of the original event

Set Parent/Child Indicator of child event to 4

Return child event updates to ObjectServer

Return original event updates to ObjectServer

Increment counter X = X + 1

Is counter <= number of potential parent events — No

Yes

Lookup potential parent event X in ObjectServer

Found relevant parent event — No

Yes

Set Parent/Child Indicator of original event to 4

Add Serial of original event to the child event list of the parent event

Parent/Child Indicator of identified parent event = 4 — Yes

No

Set Parent/Child Indicator of parent event to 5

Return parent event updates to ObjectServer

Return original event updates to ObjectServer

Figure 21: Detailed Parent / Child Event Handling Flow Chart

Mobilink OSS Expansion High Level Design

RSL/GSL/MSL alarm handling

RSL, GSL or MSL alarms are sometimes associated with GPROCs. In order to establish the state of links in the same GPROC the correct Motorola EMS associated with it GPROC needs to be queried interactively, via a command line - disp_p 0 command, in order to get the number of links associated with GPROC and the link information associated with GPROC. This command must be provided by Mobilink to complete this policy.

When an alarm RSL, GSL or MSL is received the alarm is to be suppressed for one minute to allow more of these alarms to occur. If all of the links show an error off of the same GPROC after one min then a single TT should be raised in TSRM. However, if not all links off of the GPROC generate alarms, then separate TTs should be raised for each link with an alarm.

Mobilink OSS Expansion High Level Design
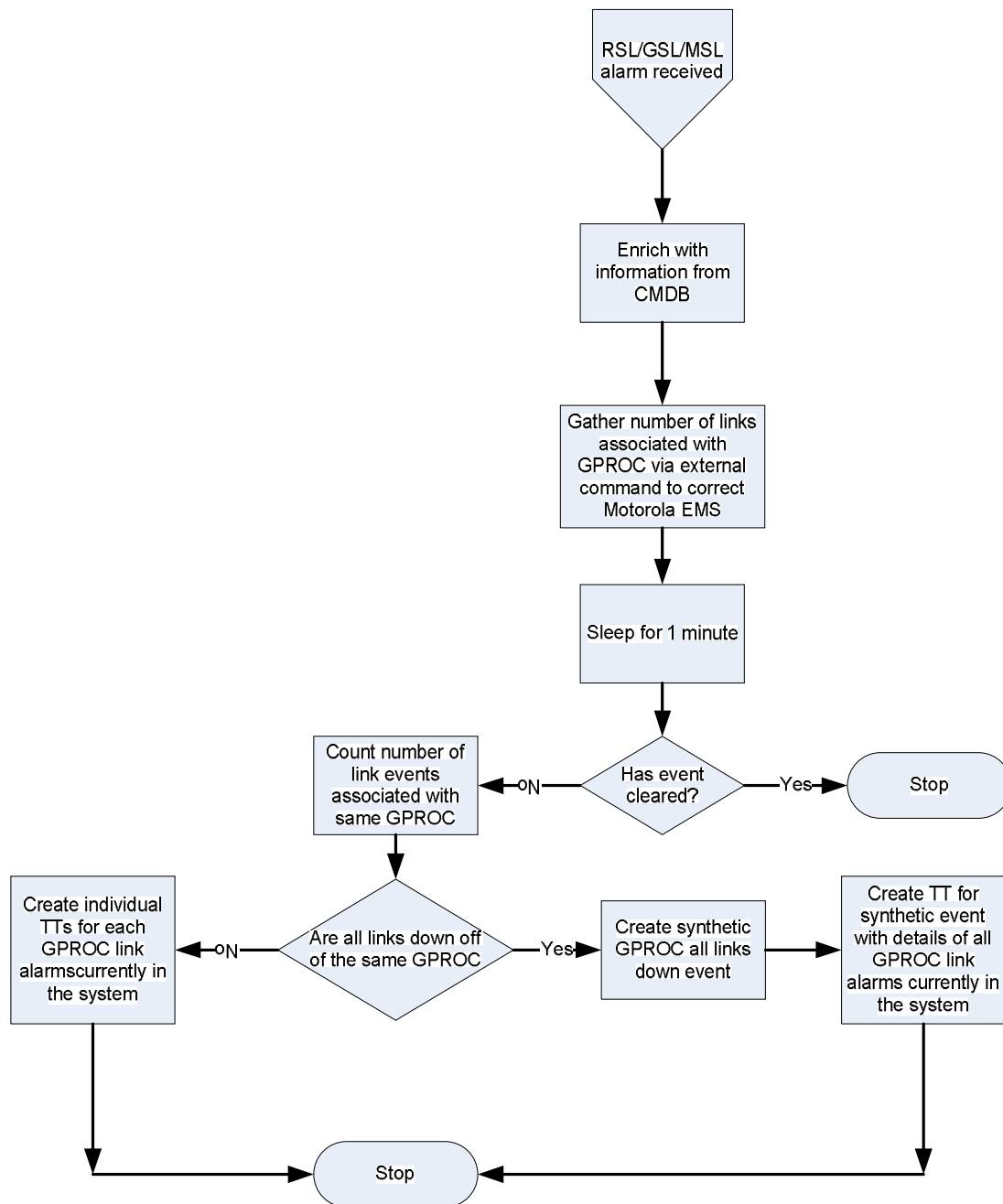
Figure 22: RSL, GLS, MSL Alarm Handling Flow Chart

X25 failures caused by TxN problems

X25 failures are indicated by X.25 Circuit Down from Motorola equipment and BSC unreachable from Alcatel equipment. These events are related together when they are associated with the same BSC. The BSC name also indicates whether the BSC has 2 OML, indicated by an A in the BSC name, or 4 OML, indicated by an E in the BSC name. A TT should be raised when first OML is down, and for all further associated failure alarms for the same BSC, the TT should be update within TSRM.

Mobilink OSS Expansion High Level Design

When all OMLs at the same BSC are down the BSC can be considered unreachable.

The TT generated should be enriched with cross-connect info from a Mobilink external DB. Cross –connect information will be provided by Mobilink as well as the external DB connectivity information.
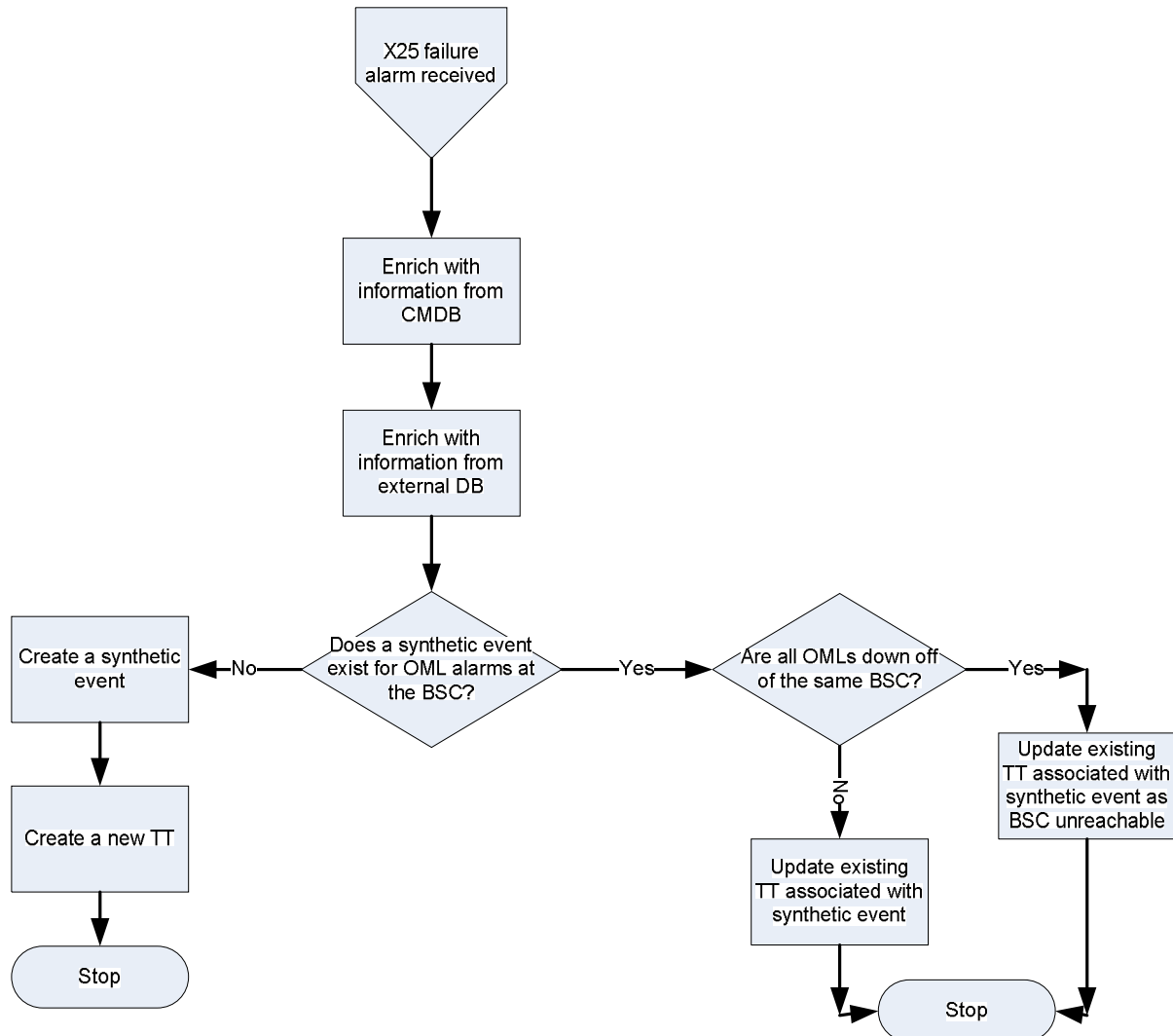
Figure 23: X25 failures caused by TxN problems Flow Chart

Cell performance related alarm handling

The following are events that indicate cell related performance issues. These events should be suppressed from TT generation for a specified period of time, to be held in an external table defining the time to suppress for each site type. If the event clears within this period then no further action is required. However, if the event is still outstanding after the specified time period has elapsed, a TT should be generated for the occurrence. If the alarms are coming in from the same BSC, this should also be mentioned in the TT.

Mobilink OSS Expansion High Level Design

- Motorola
    - No calls on cell
    - CSR below threshold
- Alcatel
    - Zero Calls on Cell
    - Zero terminating calls
- Huawei
    - Cell long time no access
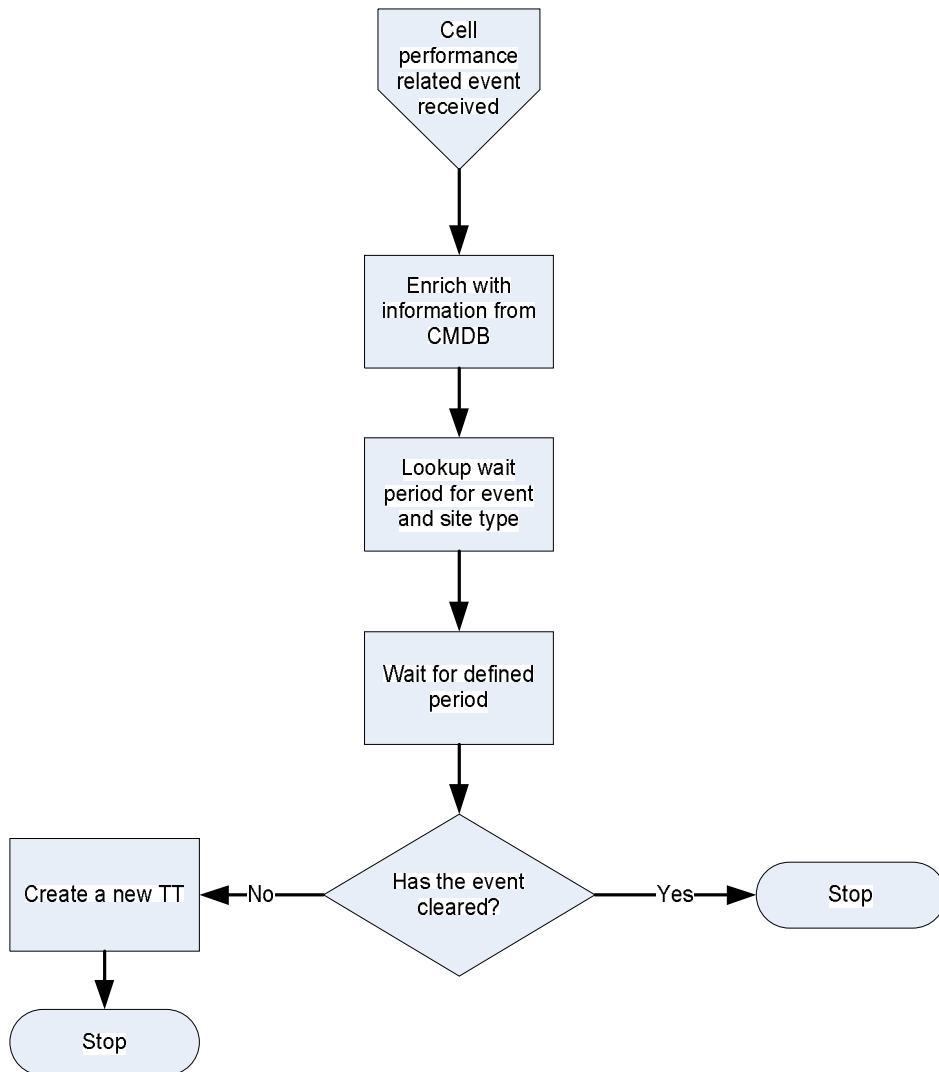
Figure 24:Cell performance related alarm handling Flow Chart

RSL link disconnected alarms

When a RSL Link Disconnect Alarm is received the RSL Alarm failure needs to be checked for the same site and if it exists then the alarm should be suppressed otherwise a TT is to be created in TSRM indicating a partial site down

Mobilink OSS Expansion High Level Design
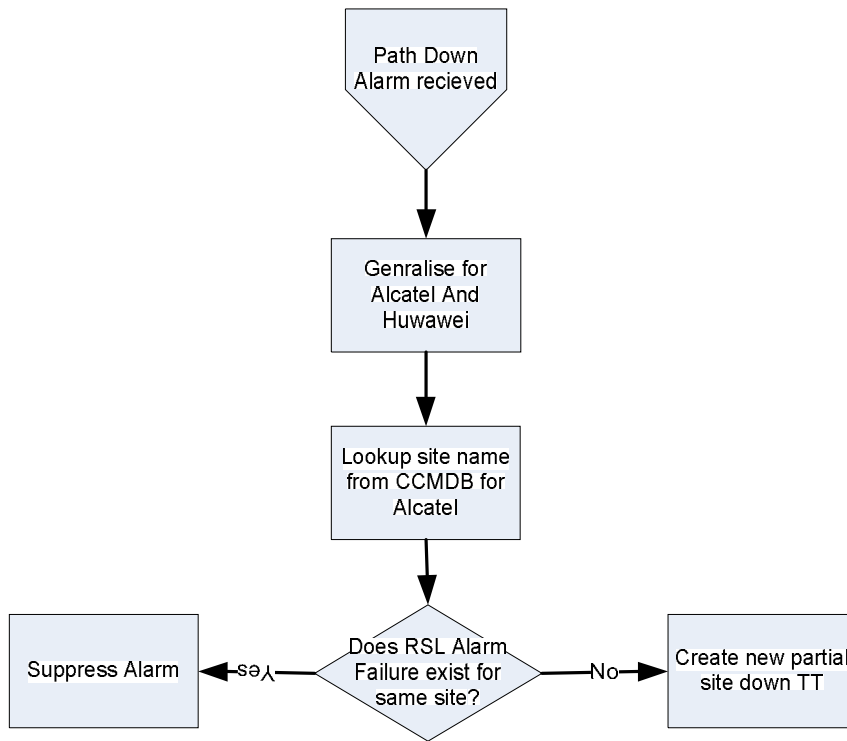
Figure 25: RSL link disconnected alarms Flow Chart

Lack of events detection for each OMC

As OMCs sometimes stop sending events it is necessary to have a mechanism to detect this, and raise TT indicating that an OMC has stopped.

This will be achieved by checking for events from each OMC on a timed basis, and raising synthetic events when no new events from a particular OMC have been received in the system for a specified period of time. The wait time will need to be defined by Mobilink.
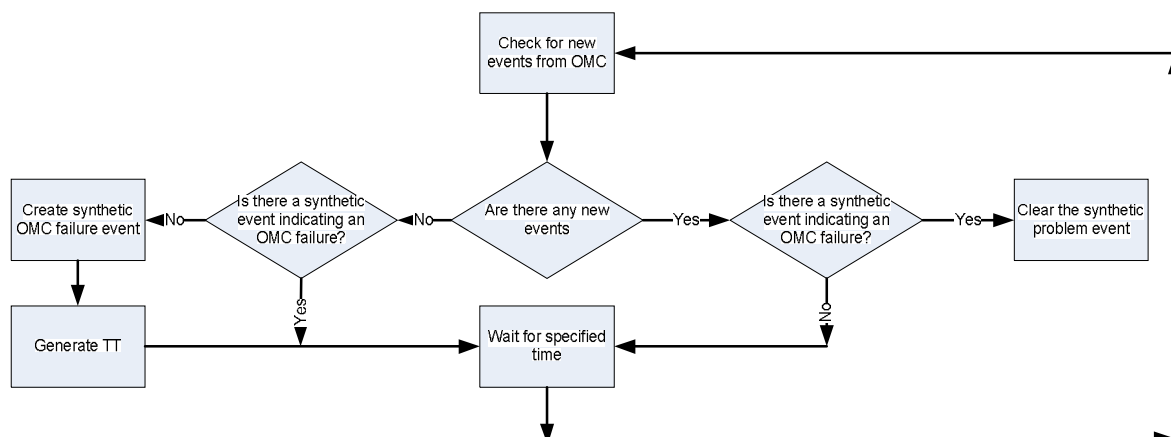
Figure 26: Lack of events detection for each OMC Flow Chart

Mobilink OSS Expansion High Level Design

TxN environmental alarm handling

TxN power related events should correlate against BSC power events at co-located sites. The co-ordinates of the sites should be used to establish which sites are co-located and should be provided by Mobilink. The events should also be enriched with their associated region, in order that external notifications, via TelAlert, can be assigned correctly.
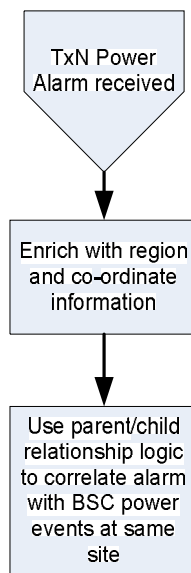
Figure 27: TxN environmental alarm handling Flow Chart

TxN Input power low/high/abnormal

Input power alarms should have TTs raised for them after a specific, 5 minute, wait period, to allow the events to clear automatically. If a power abnormal alarm is received it should be treated as a parent event for the low and high power alarms.

Mobilink OSS Expansion High Level Design
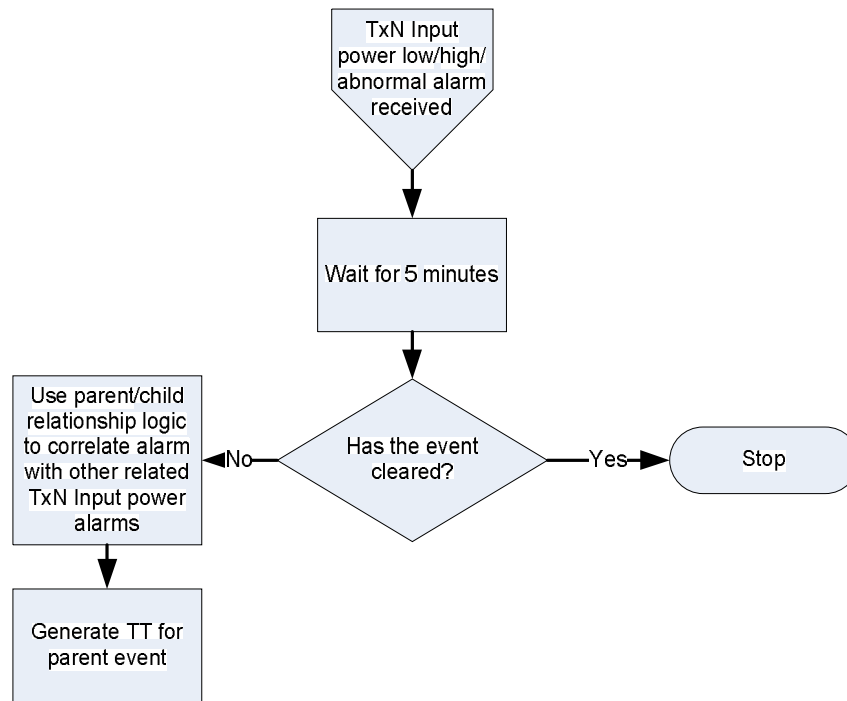
Figure 28: TxN Input power low/high/abnormal Flow Chart

TxN External Customer Alarms

The following events can be associated with external customers, which will be indicated by the setting of a flag value in the event source name.

- T_ALOSS – this is a major alarm

- TU_AIS – this is a major alarm

- UP_E1_AIS – this is a minor alarm

- DOWN_E1_AIS – this is a minor alarm

The associated customer information should be enriched into the event from data held within the CMDB. Details of the customer and alarms associated to the customer should be provided by Mobilink for this correllation.

TTs should be raised immediately for these external customer related alarms.

Also, repeated intermittent occurrences of these external customer alarms should be detected and TT raised indicating that the situation has occurred. These should be detected if an event repeats twice within a 5 minute period.

Mobilink OSS Expansion High Level Design

```
                        ┌──────────────┐
                        │   External   │
                        │ customer alarm│
                        │   received   │
                        └──────┬───────┘
                               │
                               ▼
┌──────────┐         ◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇         ┌──────────────┐
│          │        ◇ Does and existing TT ◇       │ Update existing│
│Generate TT│◄──No──◇ exist for the external ◇─Yes─►│      TT       │
│          │        ◇  customer alarm?    ◇       │              │
└────┬─────┘         ◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇         └──────┬───────┘
     │                                                   │
     │              ┌──────────────┐                     │
     │              │Check in historical│                │
     │              │  event DB for │                     │
     └─────────────►│   previous    │◄────────────────────┘
                    │occurences in past│
                    │   5 minutes   │
                    └──────┬───────┘
                           │
                           ▼
┌──────┐         ◇◇◇◇◇◇◇◇◇◇◇◇◇         ┌──────────────┐       ┌──────┐
│ Stop │◄──No──◇ Is there another ◇─Yes─►│   Generate   │──────►│ Stop │
└──────┘         ◇ occurrence within the◇    │  intermittent │       └──────┘
                 ◇   past 5 mins?   ◇       │external customer│
                  ◇◇◇◇◇◇◇◇◇◇◇◇◇         │   aalrm TT   │
                                            └──────────────┘
```

Figure 29: TxN External Customer Alarms Flow Chart

R-LOS Fibre break alarm handling

When a fibre break occurs an RLOS event will be received from NEs at both ends of the connection. ASP-IND events will also be received, indicating that connections have been switched away from the broken fibre connection. Where an NE become isolated due to losing all of its fibre connections RLOS events will not be received from it, as it cannot communicate back, but rather from the remote NEs that it was connected to.

RLOS events will also be received from the DWDM layer, and these should be associated with the TxN layer events. In order for this to be possible a table holding details of the NEs and DWDM elements positions on the fibre rings will be required in order to relate the position of the break correctly.

Mobilink OSS Expansion High Level Design
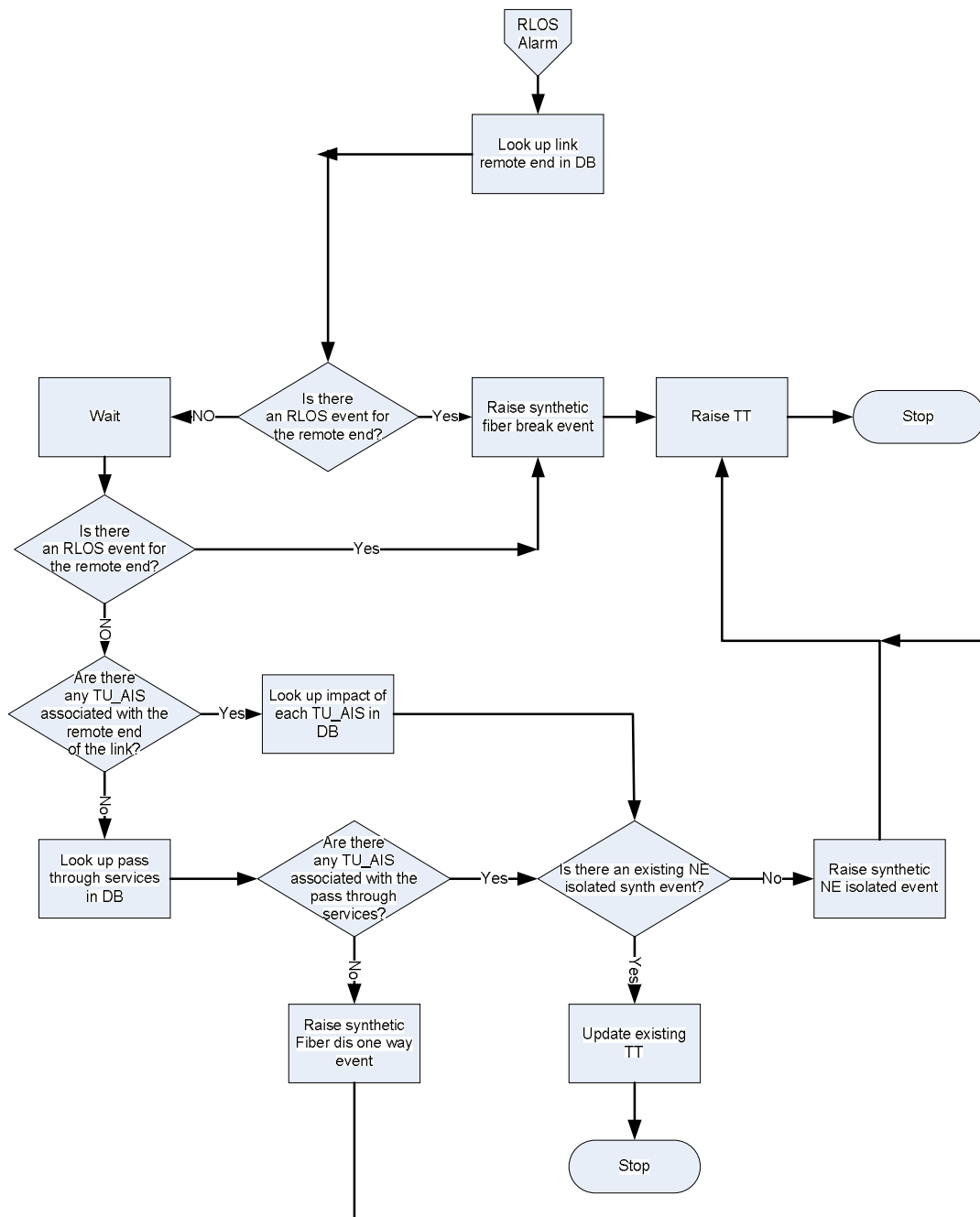
Figure 30: R-LOS Fibre break alarm handling Flow Chart

Mobilink OSS Expansion High Level Design
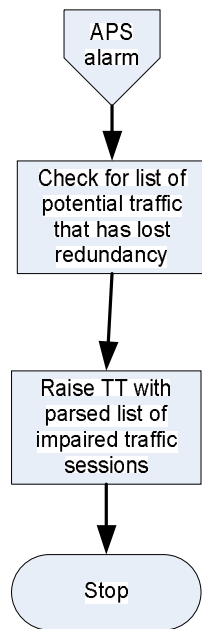
Figure 31: R-LOS Fibre break alarm handling Flow Chart

Cable Break Policy
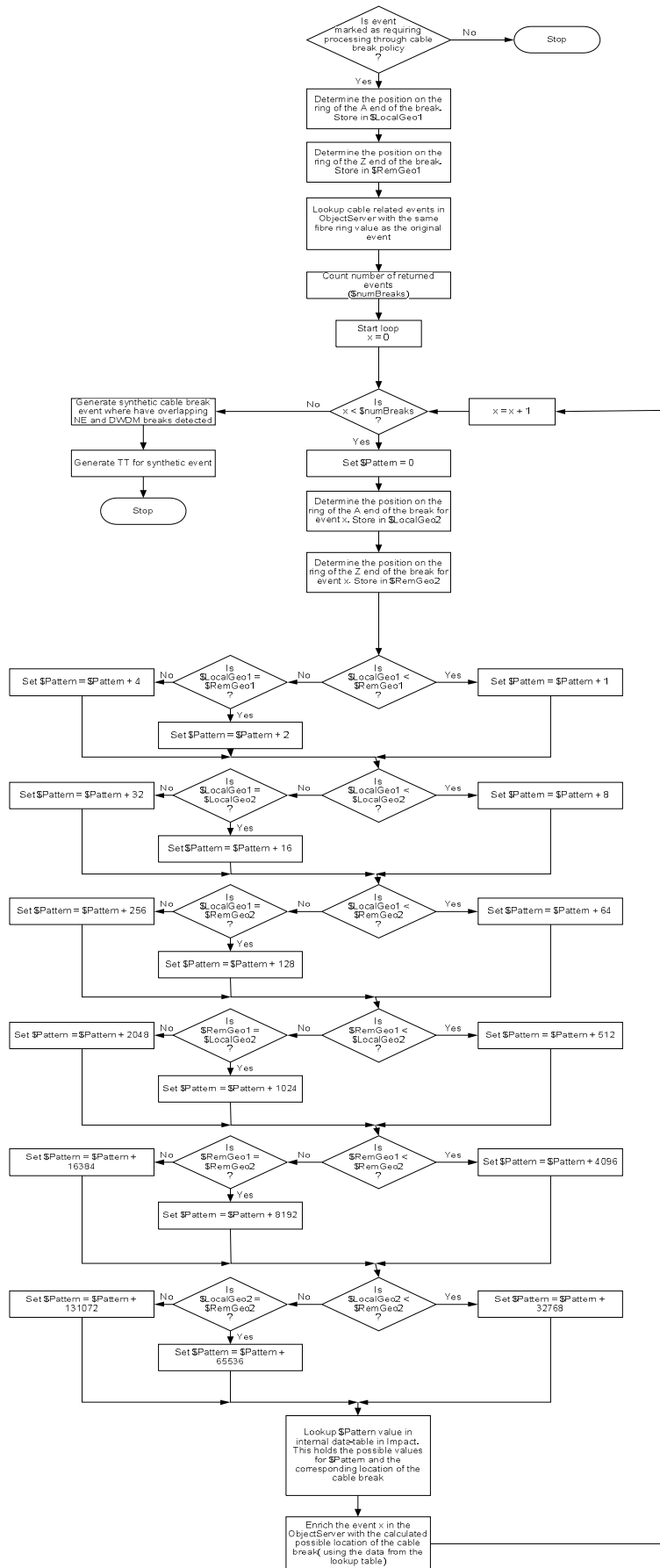
Figure 32: Cable Break Policy

Mobilink OSS Expansion High Level Design

The ETH_LOS alarm a critical alarm that depicts the Ethernet services being down. The alarm has the information of NE name, Board and Port, which is to be enriched with the information of the traffic being carried by DB and then escalated accordingly. This alarm will have a 5 minutes wait period to let it restore on its own and then create a TT in TSRM. This scenario is covered as part of the cable break policy. The data that needs to be stored in ccmdb and needs to be provided by Mobilink includes details of where the ring device is, details of overlapping rings, break points, details of the break points that overlap and where they overlap. These details need to be stored in order to identify the cable break point along with connectivity information such as domain, region and device connectivity.

Mobilink OSS Expansion High Level Design
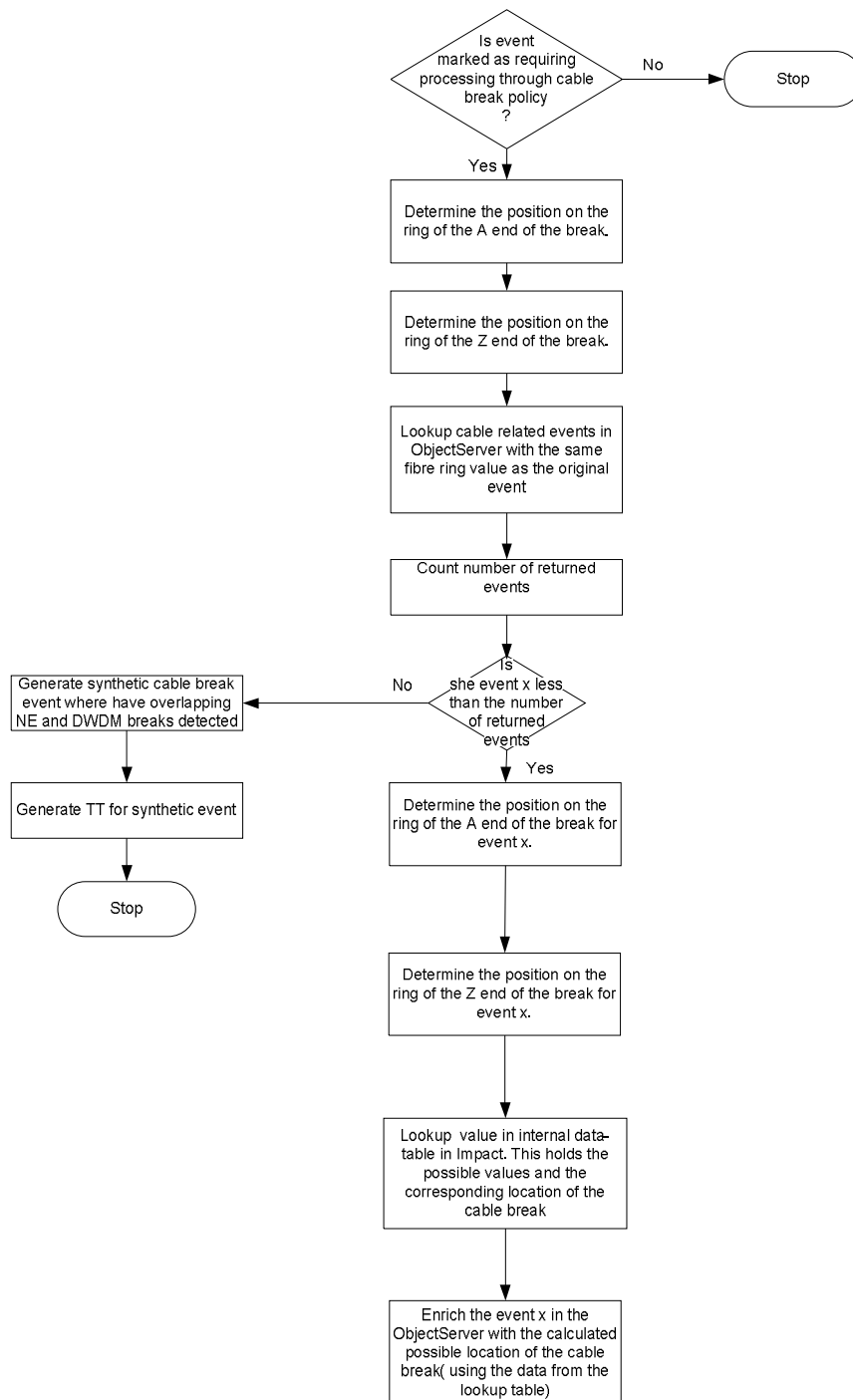
Figure 33:Simplified Cable Break Policy

Microwave error alarm handling

The following alarms are received with regard to microwave errors. The alarms can be associated together as the NE name will be same for all events.

- BER low/high alarm - Minor alarm

Mobilink OSS Expansion High Level Design

- Unavailable seconds   - Major alarm

- Rx level alarm   - Critical alarm

A single TT should be raised for these events, after allowing a 5 minute window for the alarm to clear itself, reflecting the severity of the last event received. This TT should clear when all underlying alarms have cleared. If the alarm is an Rx level alarm, it should be enriched with the number of effected channels, the capacity and type of the trunk that the alarm is associated with.
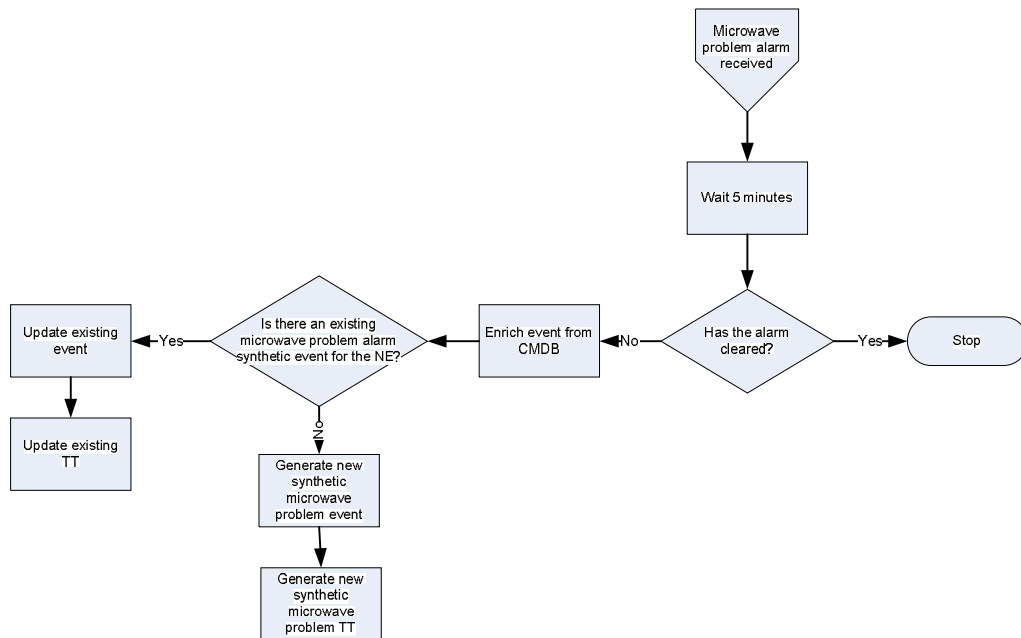
Figure 34: Microwave error alarm handling Flow Chart

Microwave environmental alarm handling

Multiple environmental alarms associated with the same microwave NE, for example GenSet alarms and Low Voltage alarms should be handled in as a single incident and not raise individual TTs. The severity of the alarm should be associated with the site type and priority from CCMDB. Mobilink are to provide the site type and priority information to associate with the severity. When all environmental alarms have cleared for the site, the incident is deemed to be closed.

Mobilink OSS Expansion High Level Design

```
                    ┌──────────────┐
                    │ Environmental │
                    │    Alarm      │
                    └──────┬───────┘
                           │
                           ▼
                    ┌──────────────┐
                    │ Enrich with site │
                    │ priority information │
                    │   from CMDB    │
                    └──────┬───────┘
                           │
                           ▼
  ┌──────────────┐    ◇ Is there an ◇   ┌──────────────┐   ┌──────────┐
  │ Look up sleep │◄─ON─│ existing TT? │─Yes►│ Update existing│►│   Stop   │
  │ time in event table│   ◇         ◇   │      TT      │   └──────────┘
  └──────┬───────┘                    └──────────────┘
         │
         ▼
  ┌──────────────┐
  │ Sleep for x time │
  └──────┬───────┘
         │
         ▼
┌──────┐   ◇ Has event ◇    ◇ Has a synthetic ◇   ┌──────────────┐   ┌──────────┐
│ Stop │◄─Yes─│  cleared? │─No►│ event been created? │─Yes►│ Update existing│►│   Stop   │
└──────┘   ◇        ◇    ◇              ◇   │      TT      │   └──────────┘
                              │
                             No
                              ▼
                    ┌──────────────┐
                    │ Create synthetic │
                    │     event      │
                    └──────┬───────┘
                           │
                           ▼
                    ┌──────────────┐
                    │ Create TT for │
                    │ synthetic event │
                    │ with details of all │
                    │ site env alarms │
                    │ currently in the │
                    │    system      │
                    └──────┬───────┘
                           │
                           ▼
                    ┌──────────┐
                    │   Stop   │
                    └──────────┘
```
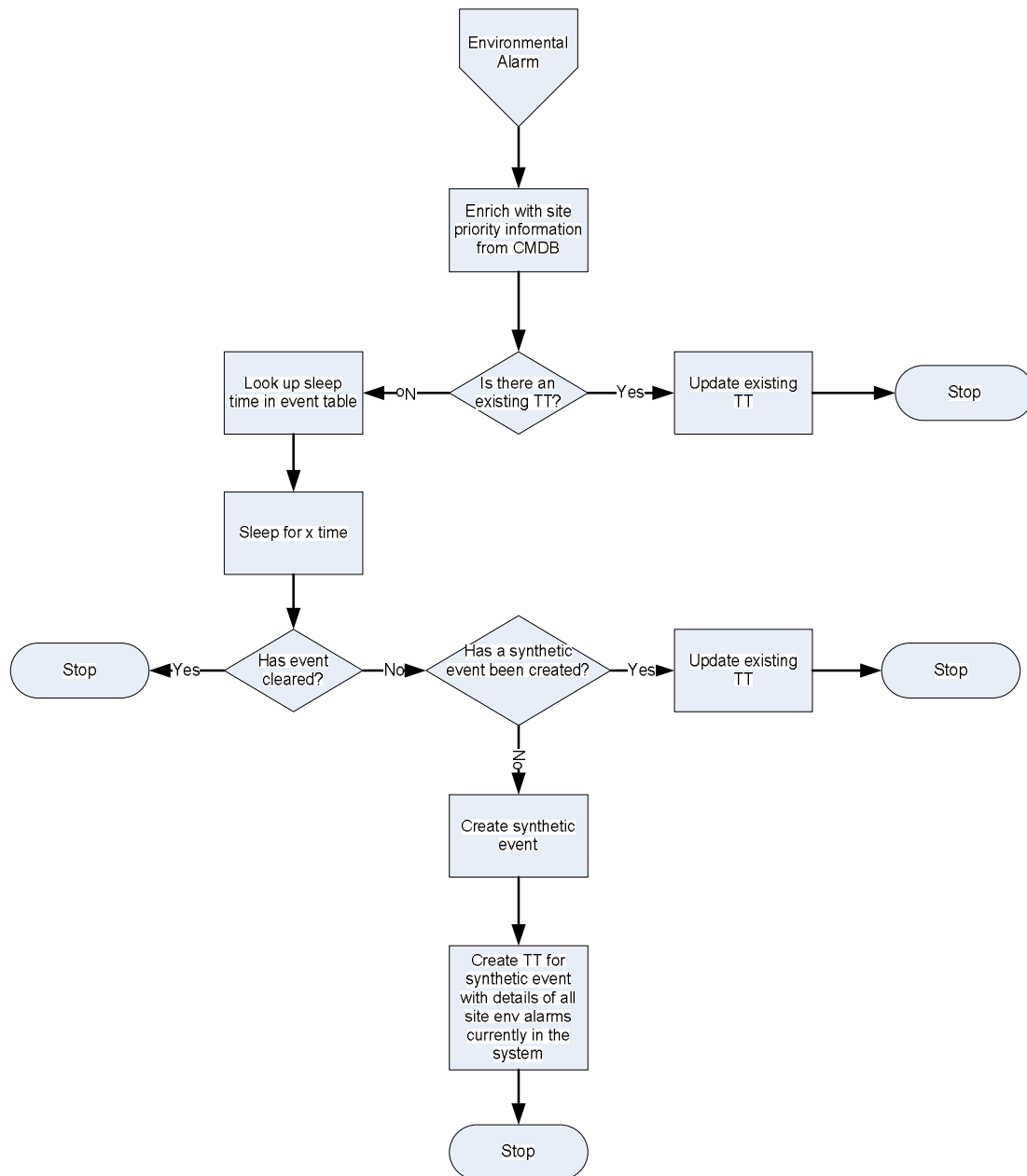
Figure 35: Microwave environmental alarm handling Flow Chart

<u>Microwave Equipment Power Supply alarm handling</u>

Microwave equipment power supply alarms should have TTs raised for them after a specified wait period, to allow the events to clear automatically. These alarms must be checked from SGSN and if the name of the alarm 'NSE failure all NSVCs in fault' is found and the unique NSE of the BSC is found then these alarms will be correlated
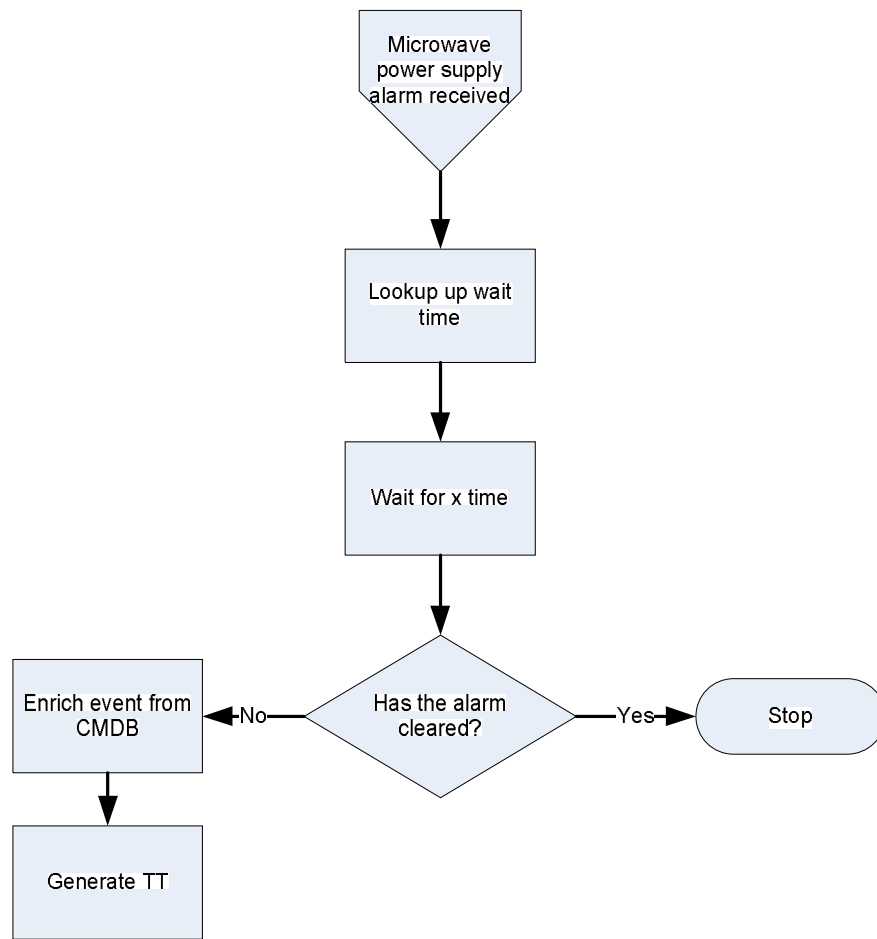
Figure 36: Microwave Equipment Power Supply alarm handling Flow Chart

Cross Domain GPRS alarm handling

The following events should be correlated together, using enrichment with BSC and DLCI information to allow them to be associated together correctly. Unless stated in the list below the DLCI information is passed with the alarm.

A single event should be raised for each for the GPRS error, and this should be updated with the information of subsequent related alarms. The TT raised for the GPRS error should only close when all underlying events have cleared.

- Loss Of Contact With GPU
    - Look up the associated BSC up via rack, shelf and GPU ids
    - Use the BSC to lookup the DLCI, to allow for correlation
- Ater Down
    - For G2 BSC – port 17 or 18
    - For evolution BSC – ports 41 or 42
    - BSC name is provided with then alarm
    - Use the BSC to lookup the DLCI, to allow for correlation
- PVC DLCI is inactive
- PVC DLCOI is unknown from the network

- PCU Down
- NSVC Dead
- NO PRP/GPS
  - BSC name is provided with then alarm
  - Use the BSC to lookup the DLCI, to allow for correlation
- Rx Level alarm
  - Look up BSC
  - Use the BSC to lookup the DLCI, to allow for correlation
- NSE Faulty
- NSVC Faulty
- NSCL Dynamic Configuration Process Failure
- NSVL Faulty
  - Look up BSC using SGSN name and NSE number from the event data
  - Use the BSC to lookup the DLCI, to allow for correlation
- Traps not yet active from EMS
- Loss Of Signal
- Rcv AIS
- Loss Of Frame
- RAI
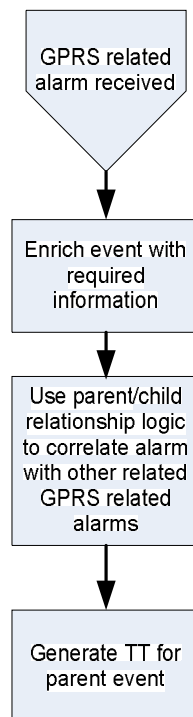
Figure 37: Cross Domain GPRS alarm handling Flow Chart

Cell GPRS Failure alarm handling

The following Cell GPRS failure events should be correlated together after 5 minutes sleep time to allow the alarm to clear. If the alarm does not clear after 5 minutes, using enrichment with BSC and to allow them to be associated together correctly.

Mobilink OSS Expansion High Level Design

- Alcatel
  - Loss of Packer Service
    - Cell level alarm provides the site code and the BSC Name
- Motorola
  - No PCDH available
    - Contains Cell ID and BSC name
    - Requires Cell name to be enriched from the CMDB
    - Site code can be extracted from Cell Id(first 4 digits of Cell-id is the Site code)

  - GPRS Unavailable
    - Contains Cell ID and BSC name. The Site code is to be extracted from Cell Id which is the last four digits of the cell-id in the alarm.
    - Requires Cell name to be enriched from the CMDB
- Huawei
  - Cell PS Service Faulty
    - Contains Cell ID and BSC name
    - Requires Cell name to be enriched from the CMDB
- SGSN
  - NSE Degraded at least one non signalling BVC in fault
    - The BSC can be looked up using NSE number and SGSN name from the event
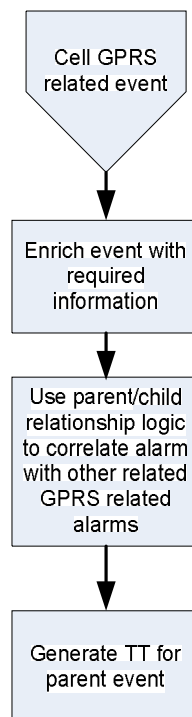
Figure 38: Cell GPRS Failure alarm handling Flow Chart

CORE Signaling down C7 alarm handling

All Signalling Down C7 alarms received should generate TTs after specified wait times, which will be held in an external database table for each linkset. The events will also be received from both ends of the connection, and so will need to be de-duplicated. The TT should contain information with regard to the linkset affected, the percentage of links down in

Mobilink OSS Expansion High Level Design

the linkset, SLC numbers and the A & Z node names this will be provided by Mobilink to include in the TT.
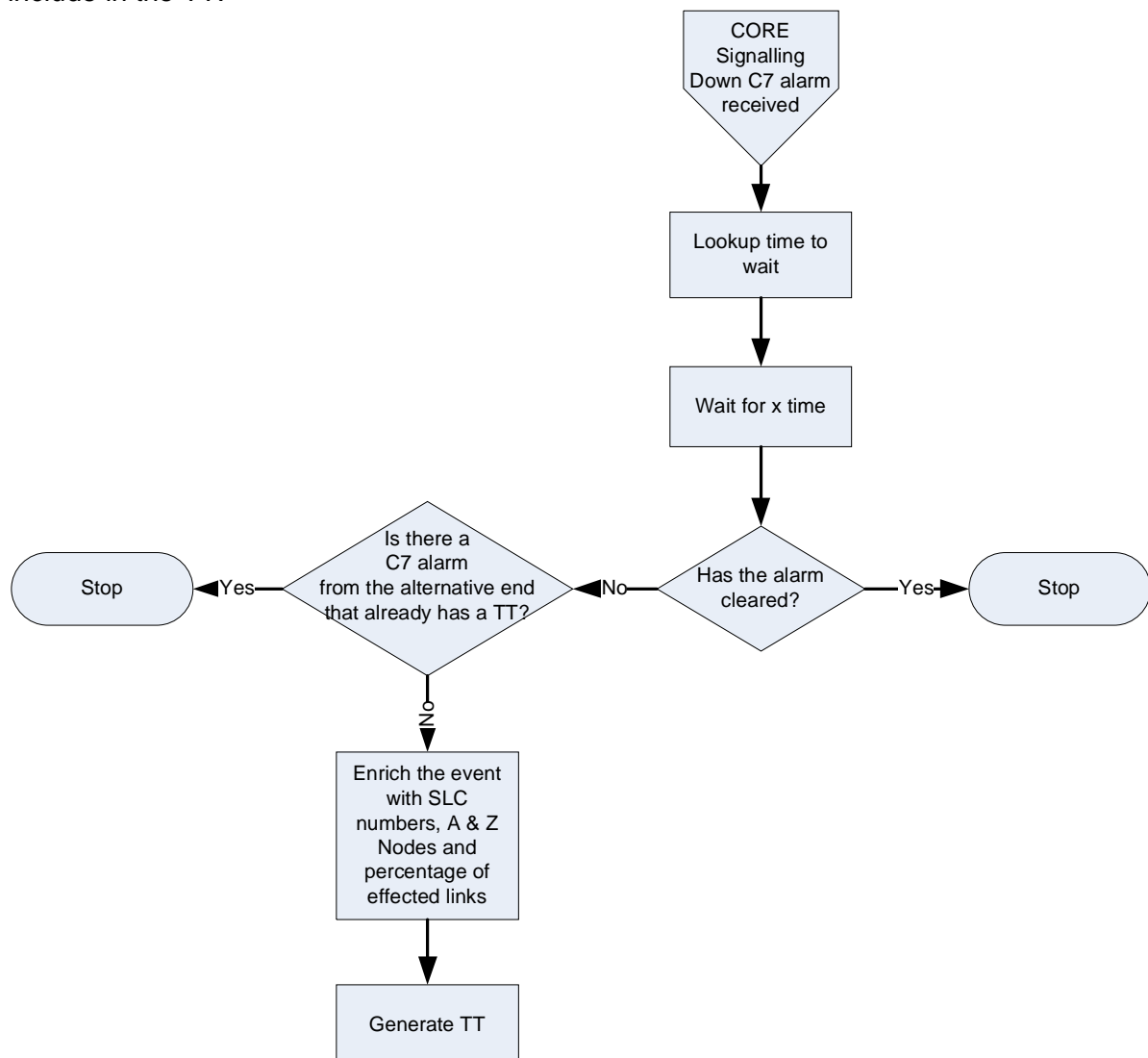
Figure 39: CORE Signaling down C7 alarm handling Flow Chart

CORE Media Outage alarm handling

A TT will be raised in TSRM when DIU alarms, which are related to media outages, are received. The TT will be raised after a specified time frame, to allow the events to clear automatically. The TT should also contain percentage of media down caused by outage.

Mobilink OSS Expansion High Level Design
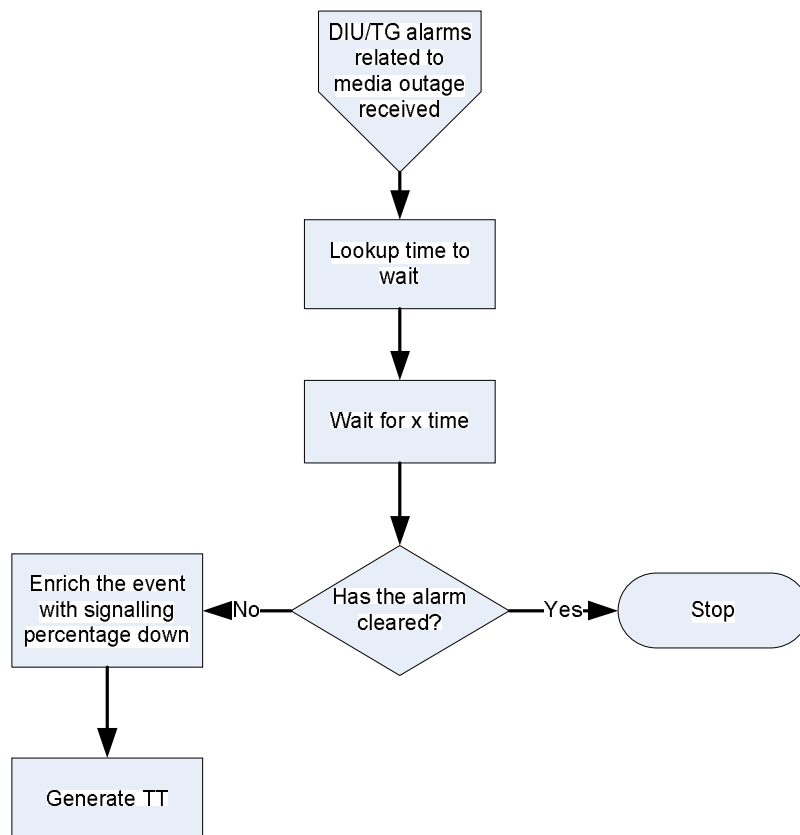
Figure 40: CORE Media Outage alarm handling Flow Chart

CORE Hardware alarm handling

Multiple environmental alarms associated with the same CORE NE, for example GenSet alarms and Low Voltage alarms, should be handled in as a single incident, and not raise individual TTs. The severity of the alarm should be associated with the site type and priority which is to be provided by Mobilink for environmental alarms. When all environmental alarms have cleared for the site, the incident is deemed to be closed.

Wapda and GenSet failure alarms should be correlated to create a single TT in TSRM. Power alarms appear in the category of Trunk System alarms and Msoft alarms for Suth NEs.

Mobilink OSS Expansion High Level Design
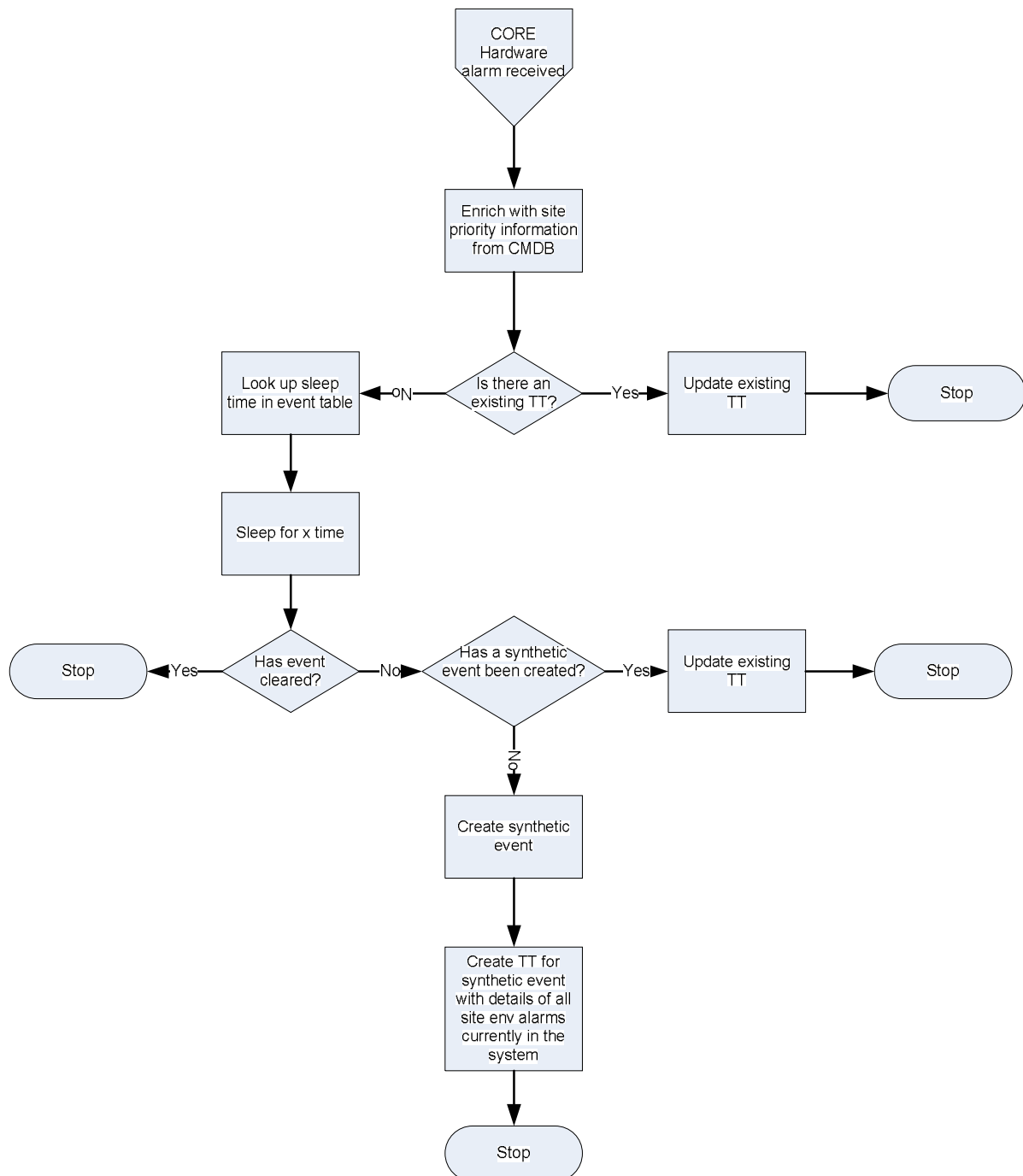
Figure 41: CORE Hardware alarm handling Flow Chart

Various hardware alarms of different vendor MSCs are maintained in a sheet and alarms are then mapped as Critical Hardware Alarm. The sheet will be provided by Mobilink to enrich from the CCMDB database. A TT also needs to be created for these as well.

Mobilink OSS Expansion High Level Design
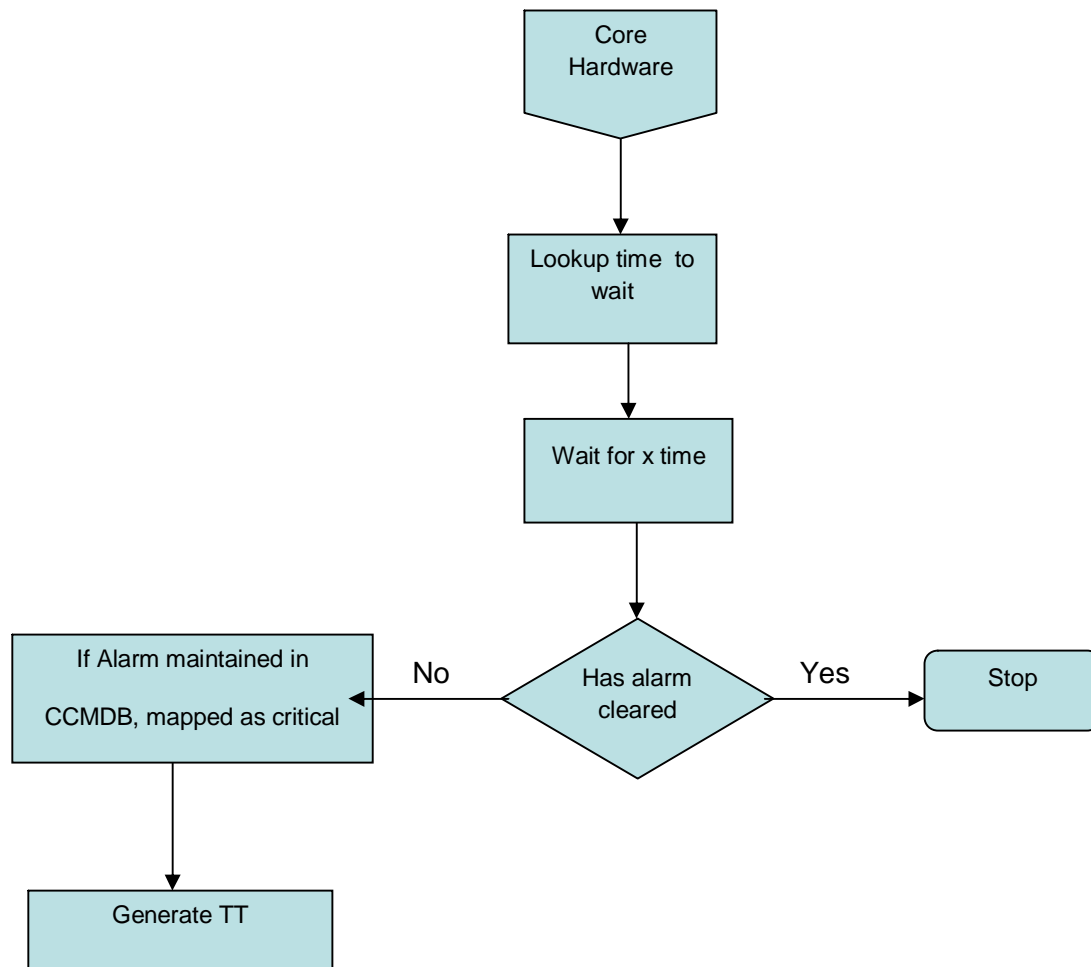
Figure 42: CORE Hardware alarm handling Flow Chart

CORE STP Linkset down alarm handling

CORE STP Linkset down alarms should be correlated together. The effected linkset name is contained within the sub-resource name within the alarm. A single TT should be raised for the correlated alarms. This TT should reflect the percentage of links down caused by the linkset down, which will update as more events are correlated. Where the link is a high speed link (HSL), it will be given a higher priority in the TT.

Mobilink OSS Expansion High Level Design
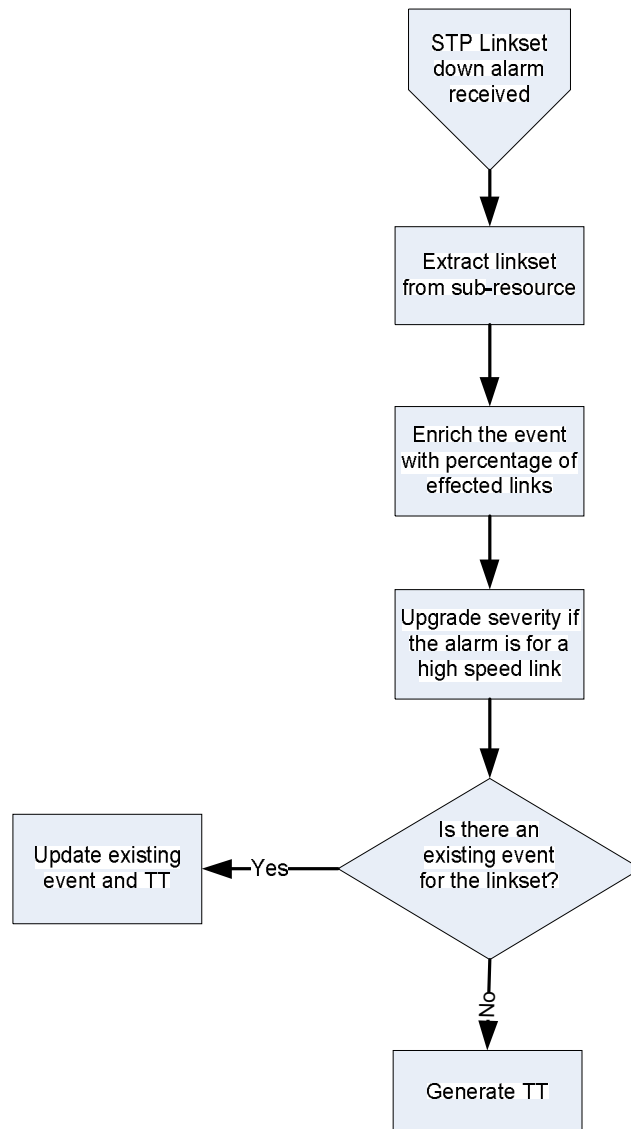
Figure 43: CORE STP Linkset down alarm handling Flow Chart

CORE STP Card Isolation alarm handling

CORE STP Card Isolation alarms indicate a major failure and will have many linkset down alarms associated with them. A TT should be raised for the card Isolation alarm, and the subsequent Linkset Down alarms marked as children of that event. The Linkset Down alarms that need to be marked as children of the event need to be identified by Mobilink. Any Linkset down that already had a TT raised for it before the card isolation event occurred will be left to be closed normally when the associated card isolation event clears.

Mobilink OSS Expansion High Level Design
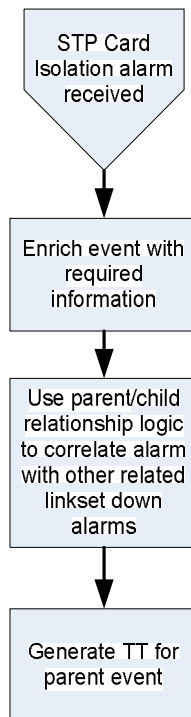
Figure 44: CORE STP Card Isolation alarm handling

CORE STP DIU Down alarm handling

CORE STP DIU Down alarms should be correlated with services that are down. The event should be enriched with the far end MSC equipment details by looking up the local MSC Equip and Amet Port values from the triggering alarm. This lookup will take place against a table created by Mobilink from data currently held in a spreadsheet.

Mobilink OSS Expansion High Level Design
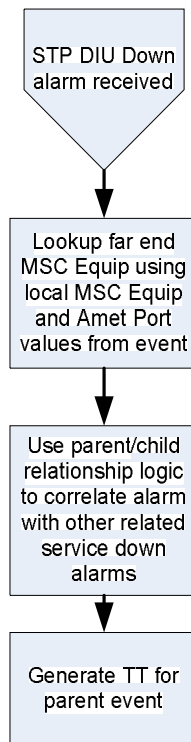
Figure 45: CORE STP Card Isolation alarm handling Flow Chart

Communication alarm handling

CORE STP DPC Down alarms indicate total loss of connectivity with a BSC. There is no direct connectivity to BSCs with STP nodes. STP nodes have direct signaling connectivity with different Core NEs e-g MSCs, IN Nodes, SMSCs, MMSC, SGSN, HLRs etc. So there will be DPC alarms when complete connectivity with specific NE is down. These events should be correlated based on the point code of the NEs which will have TT raised within 5 minutes of alarm occurrence.

In case of a DPC Down Alarm towards a BSC all Link Down Alarms and X25 Alarm from BSC will be considered as child event of this DPC Alarm and separate TT will not be generated but as soon as this DPC Alarms Clears and X25 Alarm Still exist on BSC then its separate TT should be created
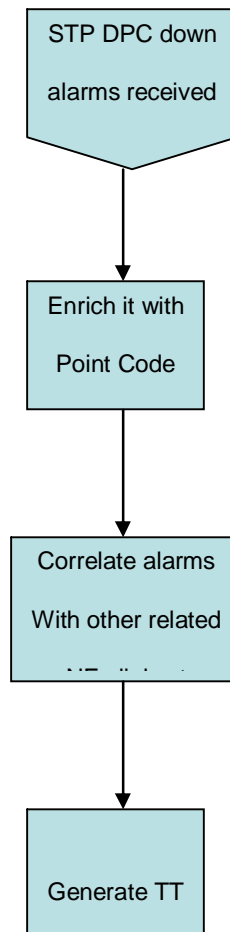
Figure 46: CORE STP Card Isolation alarm handling Flow Chart

IN Node Down alarm handling

IN Node Down alarms should have a TT raised for each instance immediately. A number of events are associated with the Node Down event as child events, and these should be suppressed from TT generation when a Node Down event exists. Where a pair of IN nodes fail, DPC Down alarms will be received from the INs and STPs involved. A single TT should be raised for this occurrence. This TT should clear as soon as one of the DPC Down alarms clears

IN Processing Error alarm handling

IN Process Error alarms should generate a TT within 10 to 15 minutes after alarm occurs for each instance of the alarm

Mobilink OSS Expansion High Level Design
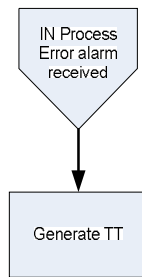
Figure 47: IN Processing Error alarm handling Flow Chart

IN Call Gaping alarm handling

IN Call Gaping alarms should generate a TT within 3 to 5 minutes once 100% threshold event is received, assuming the alarm has not cleared in that time period. This event and TT are cleared when a 70% threshold alarm is received from the same device.
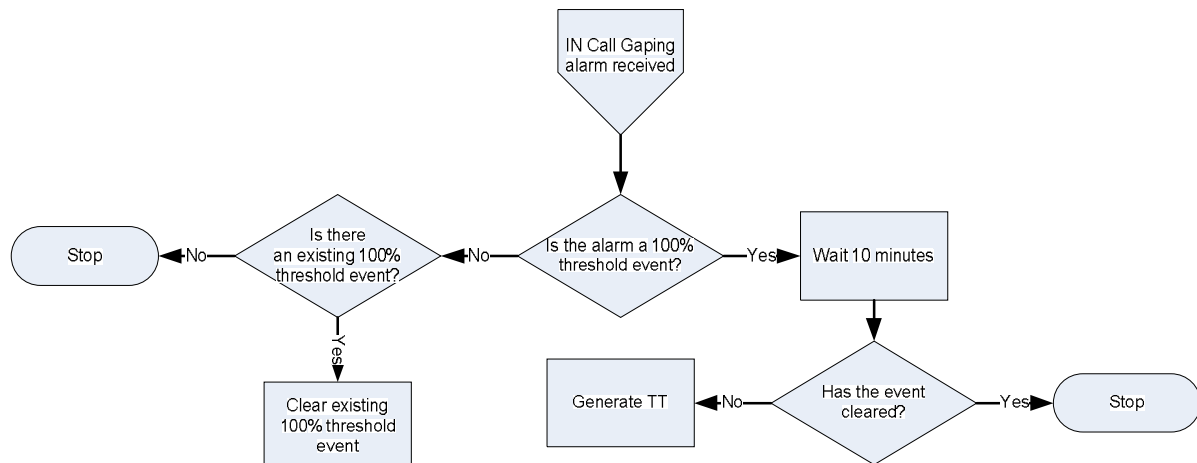
Figure 48: IN Call Gaping alarm handling Flow Chart

QoS alarm handling

IN Critical Threshold Crossed alarms should generate when predefined monitoring thresholds for disk space are crossed. The monitoring is to be done via an agent running on the monitored servers. A TT should be generated after 5 minutes.
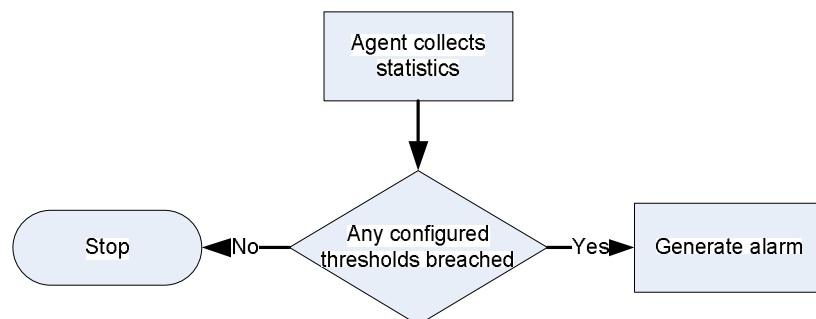
Figure 49: QoS alarm handling Flow Chart

Mobilink OSS Expansion High Level Design

Equipment alarm handling

Certain IN Critical Hardware alarms are generated when particular memory module (DIMM) errors are detected. Where the event relates to multiple DIMM failures, the underlying individual failures should be associated as child events of the parent multiple failure event. The child events will be identified by Mobilink to store in the ccmdb.
 As there is no clearing event for these, these events should be cleared when the associated TT is closed. This is the opposite action to all other events.
 For non-DIMM related critical hardware related event, TTs should be created after a specified wait time, to allow short-term events to clear without TT generation
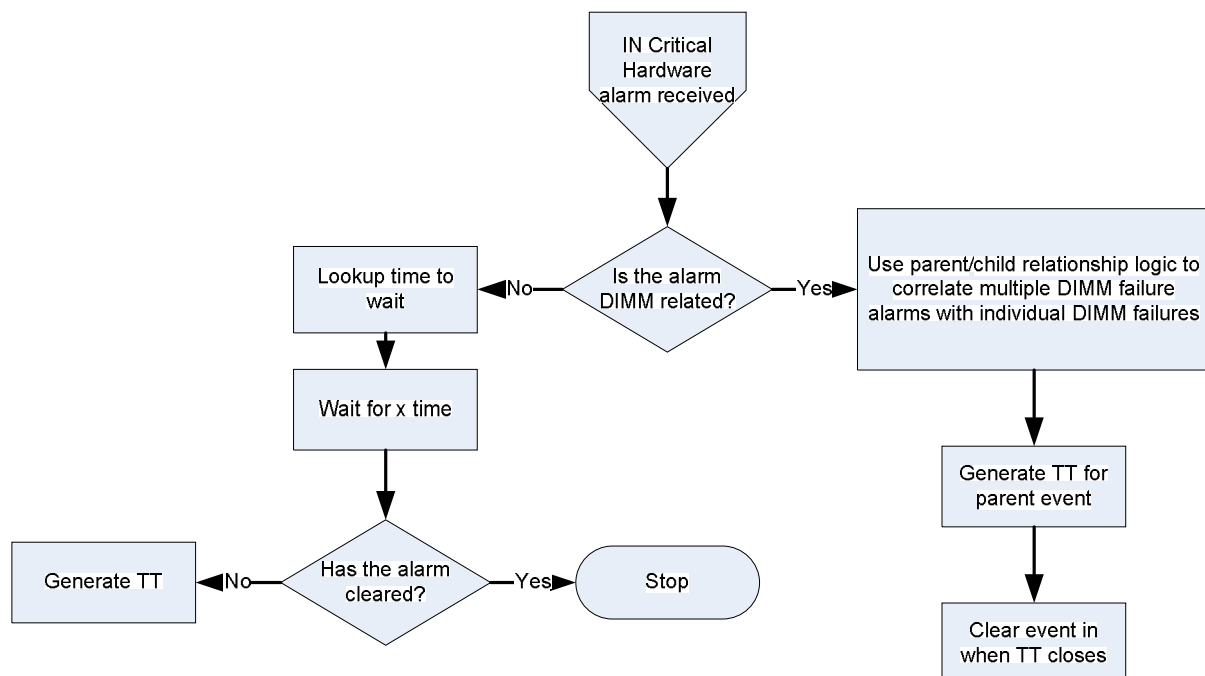
Figure 50: Equipment alarm handling Flow Chart

IN DPC alarm handling

IN DPC alarms received should generate TTs after specified wait times, which will be held in an external database table for each linkset. The events will also be received from both ends of the connection, and so will need to be de-duplicated. The TT should contain information with regard to the linkset affected, the percentage of links down in the linkset, SLC numbers and the A & Z node names.
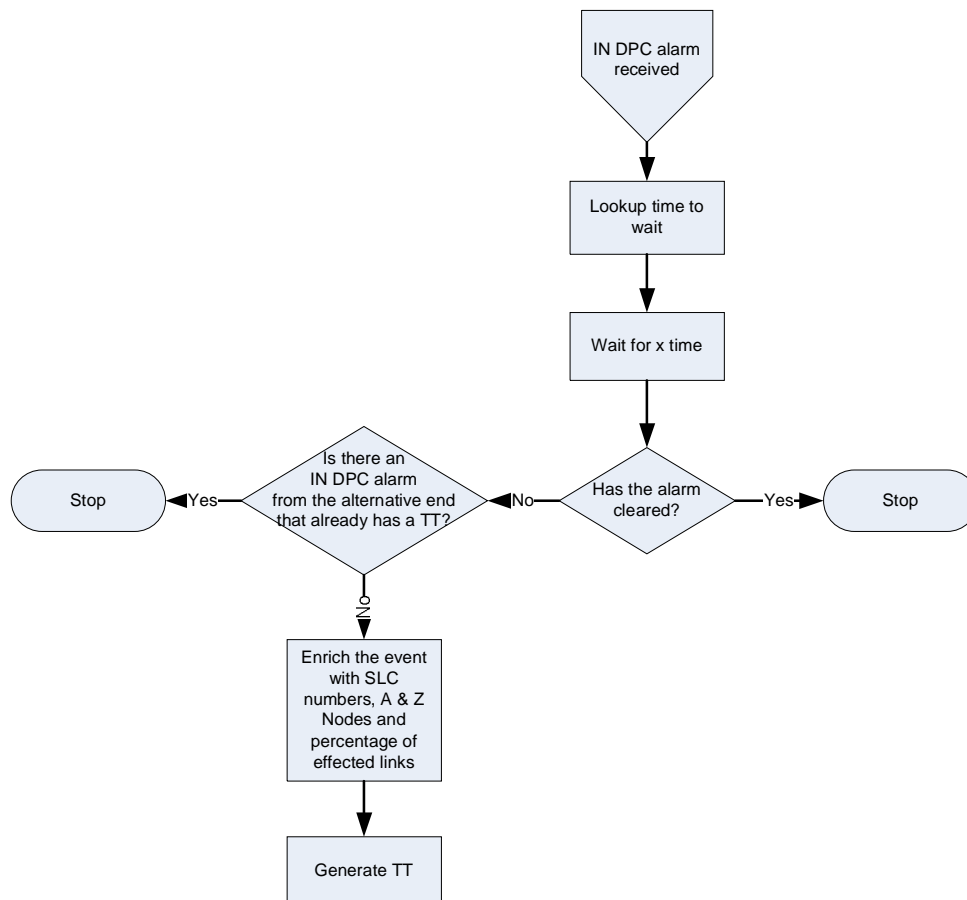
Figure 51: IN DPC alarm handling Flow Chart

IN Environmental alarm handling

IN Environmental alarms should have TTs created after a specified wait time, to allow "Mopnet Connection Lost" and "MopnetConnection restored" alarms to indicate that issue is normal without TT generation. If the issue persists a single TT should be generated. A time threshold should be defined during which if the alarm reappears then a new TT should be created.

Mobilink OSS Expansion High Level Design
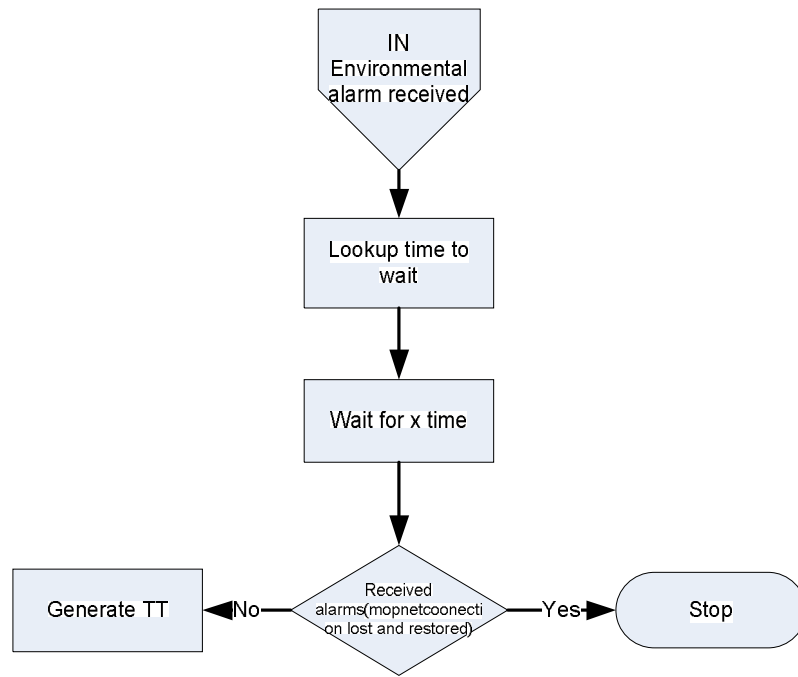
Figure 52: IN Environmental alarm handling Flow Chart

<u>IN Valista Issue on IN alarm handling</u>

IN Valista Issue on IN alarms are generated for particular thresholds. The >100 per mill and >200 per mill events associated with the same IN should be suppressed, with their severity and summary text altering to show the last breached threshold. In order to pick up frequently erroring lower threshold alarms, a mechanism for detecting the repeat occurrences of these events at a certain threshold within a specified time period should be implemented.

For >300 per mill events should have TTs created after a specified wait time, to allow short-term events to clear without TT generation. For >100 and >200 should not be included in TT generation

Mobilink OSS Expansion High Level Design
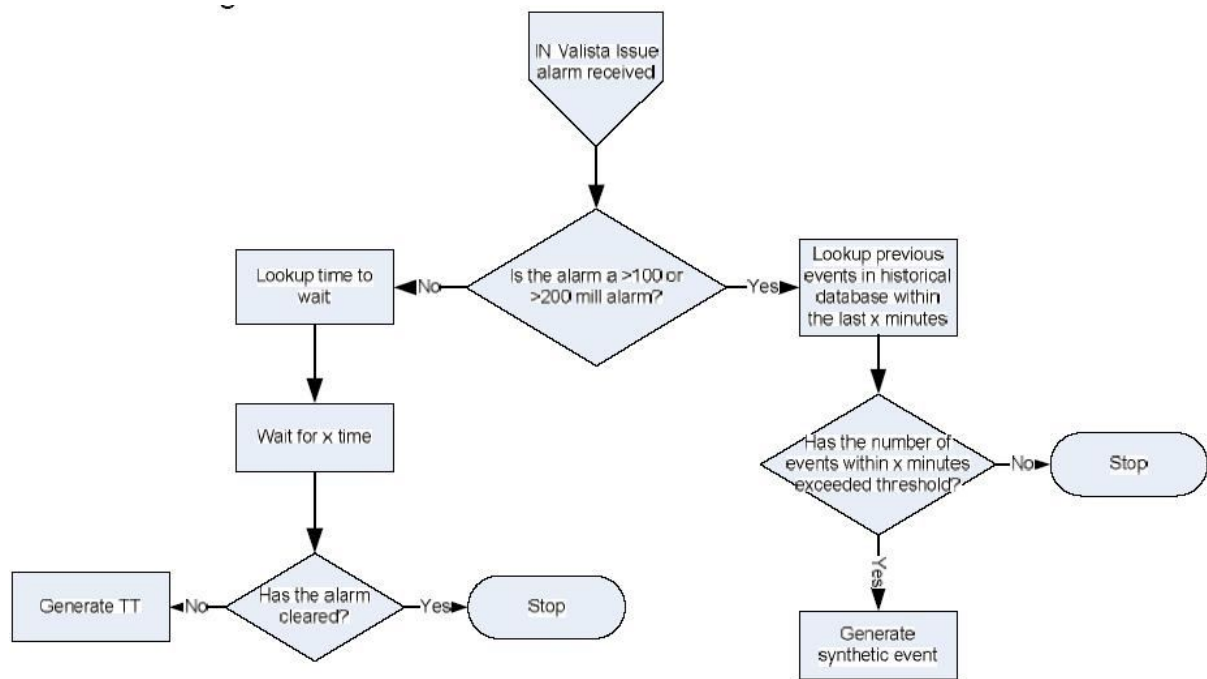
Figure 53: IN Valista Issue on IN alarm handling Flow Chart

IN VOMS alarm handling

IN VOMS alarms should have TTs created after a specified wait time, to allow short-term events to clear without TT generation
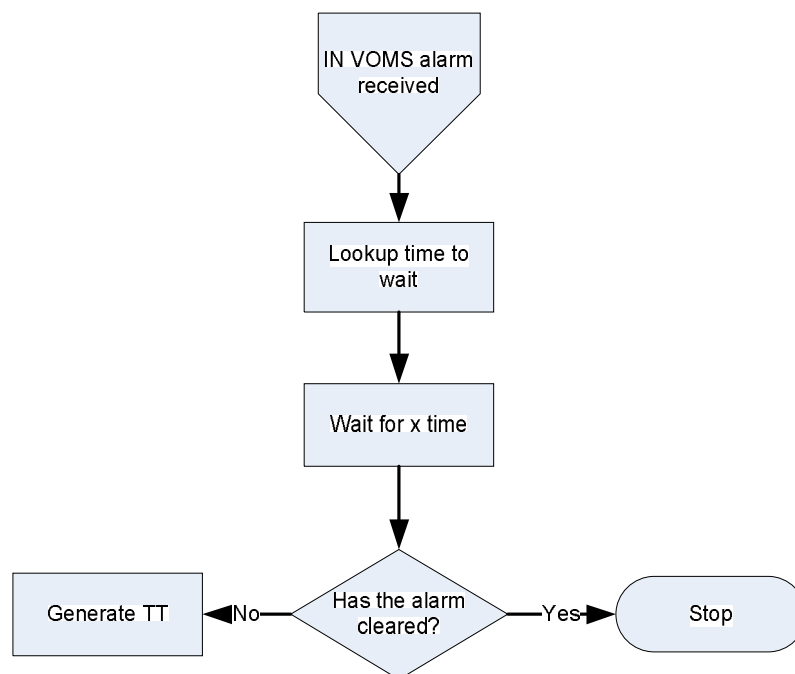
Figure 54: IN VOMS alarm handling Flow Chart

Mobilink OSS Expansion High Level Design

SMSC Service Impacting alarm handling

The following SMSC Service Impacting alarms should have TTs created after a specified wait time, to allow short-term events to clear without TT generation:

- Restarting Entity
- Entity is in Blocked State
- Entity Not Responding

SMSC Node Down events should be correlated as child events with the parent DPC Down events from the associated STP. This can be determined from the point codes of the devices.
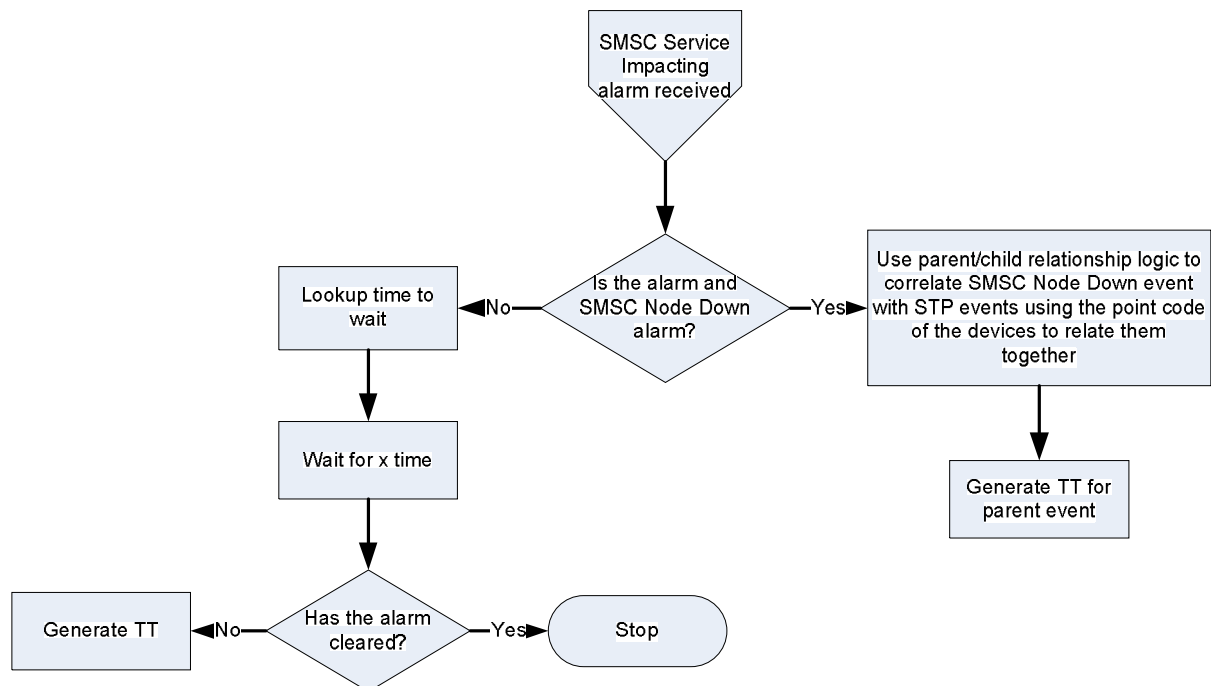
Figure 55: SMSC Service Impacting alarm handling Flow Chart

SGSN Hardware alarm handling

SGSN Hardware alarms should have TTs created after a specified wait time, to allow short-term events to clear without TT generation

Mobilink OSS Expansion High Level Design
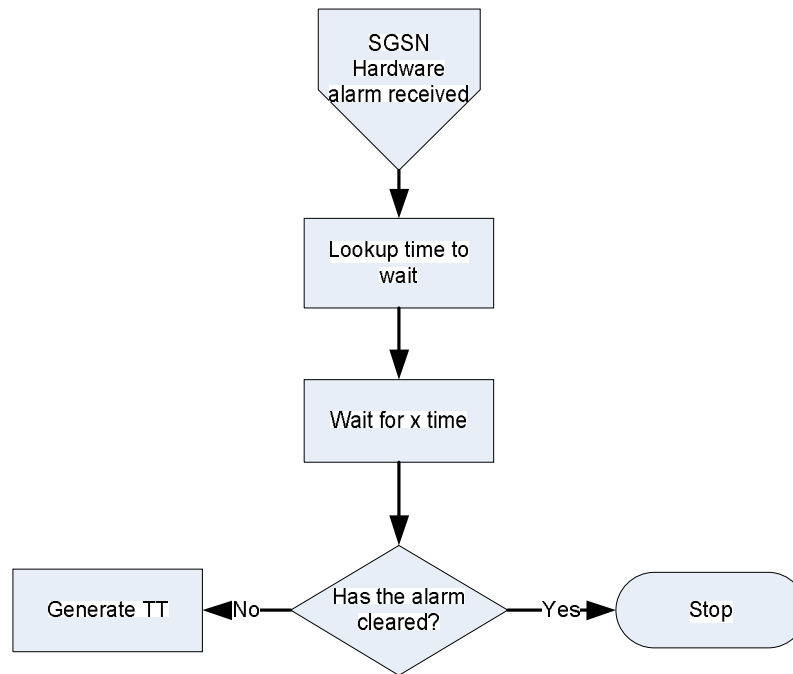
Figure 56: SGSN Hardware alarm handling Flow Chart

SGSN Multiple C7 Link Down alarm handling

SGSN Multiple C7 Link Down alarms received should generate TTs after specified wait times, which will be held in an external database table for each linkset. The events will also be received from both ends of the connection, and so will need to be de-duplicated. The TT should contain information with regard to the linkset affected, the percentage of links down in the linkset, SLC numbers and the A & Z node names. This information is to be provided by Mobilink.

For SGSN alarms In OMCCN and OMCPS: Additional Text contains the name of the alarm 'NSE failure all NSVCs in fault' which is critical alarm and its Friendly name contains the NSE of the BSC(which is unique). Then these alarms are to be co-related with the BSS side alarms.

Alarms for Alcatel are shown Below:

- BSC GPRS service lost(comes with Rack, Shelf, and GPU information but the Friendly name contains the name of BSC,which allows co-relation)
- BSS BVCSig of this GPU is broken(comes with Rack, Shelf, GPU information but the Friendly name contains the name of BSC,which allows co-relation)
- BSS GSL is broken(comes with Rack, Shelf, GPU information but the Friendly name contains the name of BSC,which allows co-relation)
- LapDLink is broken(Friendly name contains BSC Name and LAPD number[which in turn refers to Ater number] and from the BSC Name correlation can be applied)
- Loss of contact with GPU(Friendly name contains the information of Rack,Shelf and GPU information which can be mapped against BSC Name,which allows co-relation)

Mobilink OSS Expansion High Level Design

- No reply from SGSN(Friendly name contains the information of NSE, which is mapped against a particular BSC, which allows co-relation).
- PVC DLCI is inactive(Friendly name comes with the name of Shelf,GPU and also the value of PVC DLCI, which can be mapped to get the name of BSC and correlation can be applied).
- PVC DLCI is unknown from the network(Friendly name comes with the name of Shelf,GPU and also the value of PVC DLCI, which can be mapped to get the name of BSC and correlation can be applied).

Alarms for Motorola are shown below:

- Last GBL Failed(comes with the name of BSC and hence correlation can be applied)
- Last GSL Failed(comes with the name of BSC and hence correlation can be applied)
- Last TRAU GDS Failed(comes with the name of BSC and hence correlation can be applied)
- Last PCU Failed(comes with the name of BSC and hence correlation can be applied)
- NSVC Failure(comes with the name of BSC and hence correlation can be applied)

Mobilink OSS Expansion High Level Design

```
                          ┌──────────────────┐
                          │ SGSN Multiple    │
                          │ C7 Link Down     │
                          │ alarm received   │
                          └────────┬─────────┘
                                   │
                          ┌────────▼─────────┐
                          │ Lookup time to   │
                          │ wait             │
                          └────────┬─────────┘
                                   │
                          ┌────────▼─────────┐
                          │ Wait for x time  │
                          └────────┬─────────┘
                                   │
         ◇ Is there an             │
         SGSN Multiple C7 Link     ◇ Has the alarm
   Stop ◄─Yes─ Down alarm ◄──No── cleared? ─Yes─► Stop
         from the alternative end that
         already has a TT?
                  │
                  No
                  │
         ┌────────▼─────────┐
         │ Enrich the event │
         │ with SLC         │
         │ numbers, A & Z   │
         │ Nodes and        │
         │ percentage of    │
         │ effected links   │
         └────────┬─────────┘
                  │
         ┌────────▼─────────┐
         │ Generate TT      │
         └──────────────────┘
```
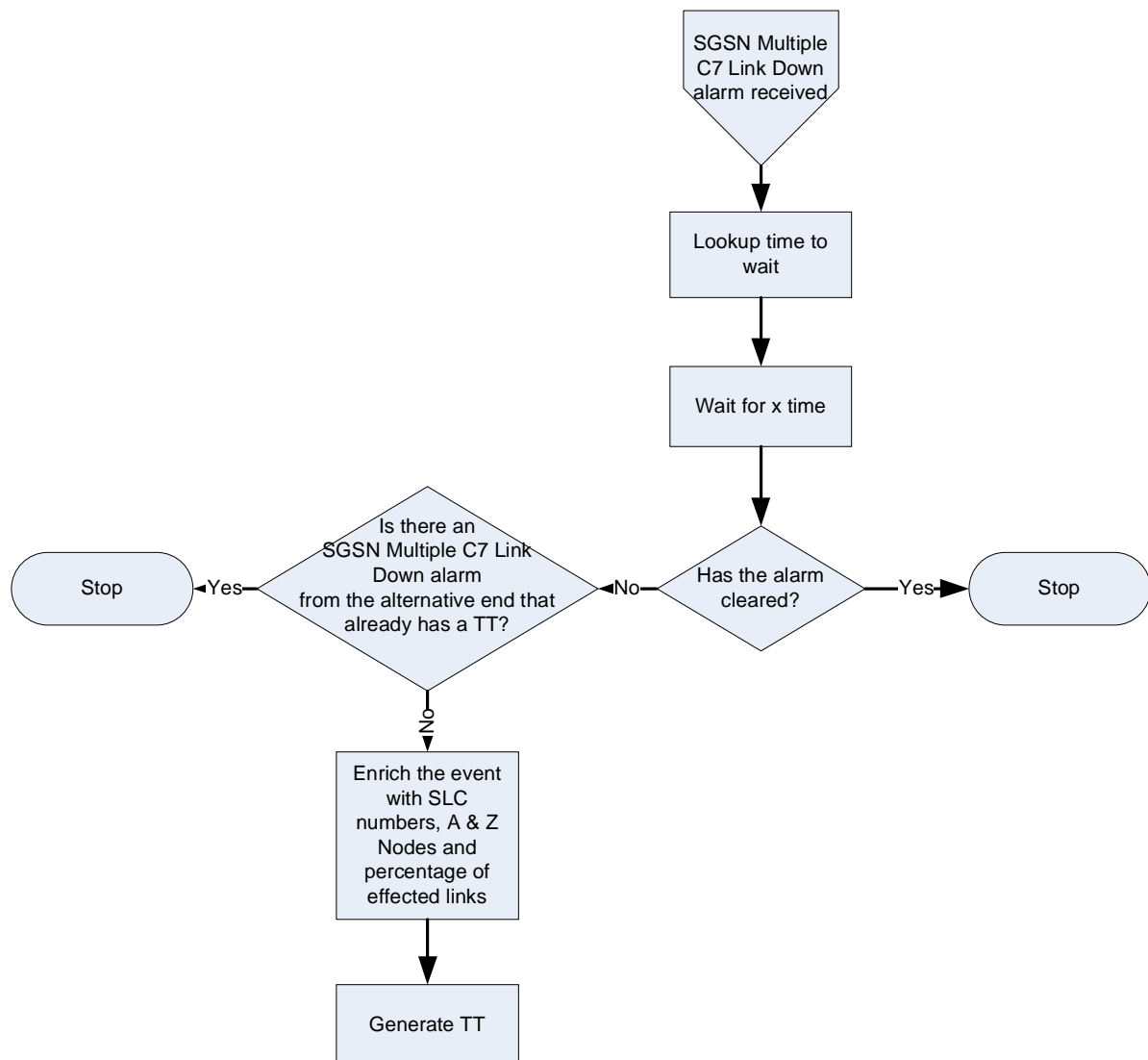
Figure 57: SGSN Multiple C7 Link Down alarm handling Flow Chart

APS impact correlation

When an APS event is received it indicates that trails have switched paths through the network. The impact of these to external customers should be enriched into the event by looking up the NE that the APS alarm is associated with in the topology table maintained by Mobilink. Any trail where the NE is the sink or source of a trail, or where the NE is in the positive path for the trail will have been potentially been effected. Trails for external customers will have a flag field within their name, and these are the trails to be recorded against the TT generated.
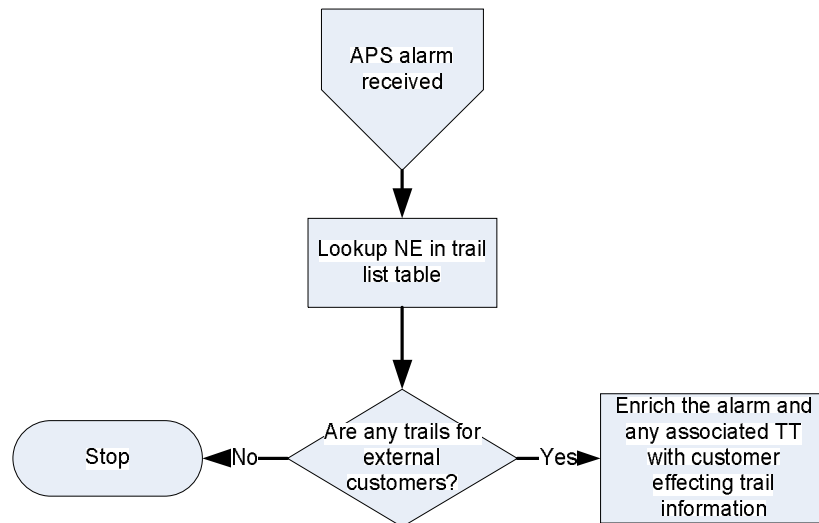
Figure 58: APS impact correlation Flow Chart

C7 signaling correlation and multi fails in city

Where there are multiple C7 signalling alarms being received within the same area/city they should be correlated together to a single synthetic event, with an associated TT for that event.
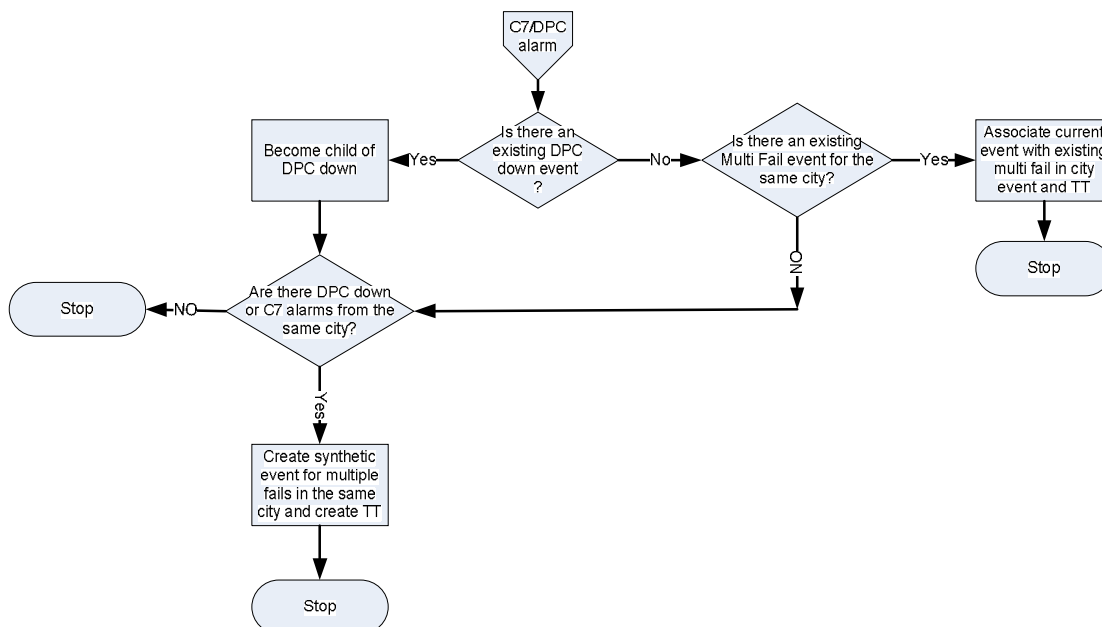
Figure 59: C7 signaling correlation and multi fails in city Flow Chart

Mobilink OSS Expansion High Level Design

Alarm suppression during maintenance windows

During periods where a site is under preventative maintenance any events received during the period of the maintenance window should be suppressed from views and also prevented from generating TTs during the maintenance window period. Once the maintenance window has expired, any events still outstanding should be unsuppressed and TT raised as appropriate for the alarm type.
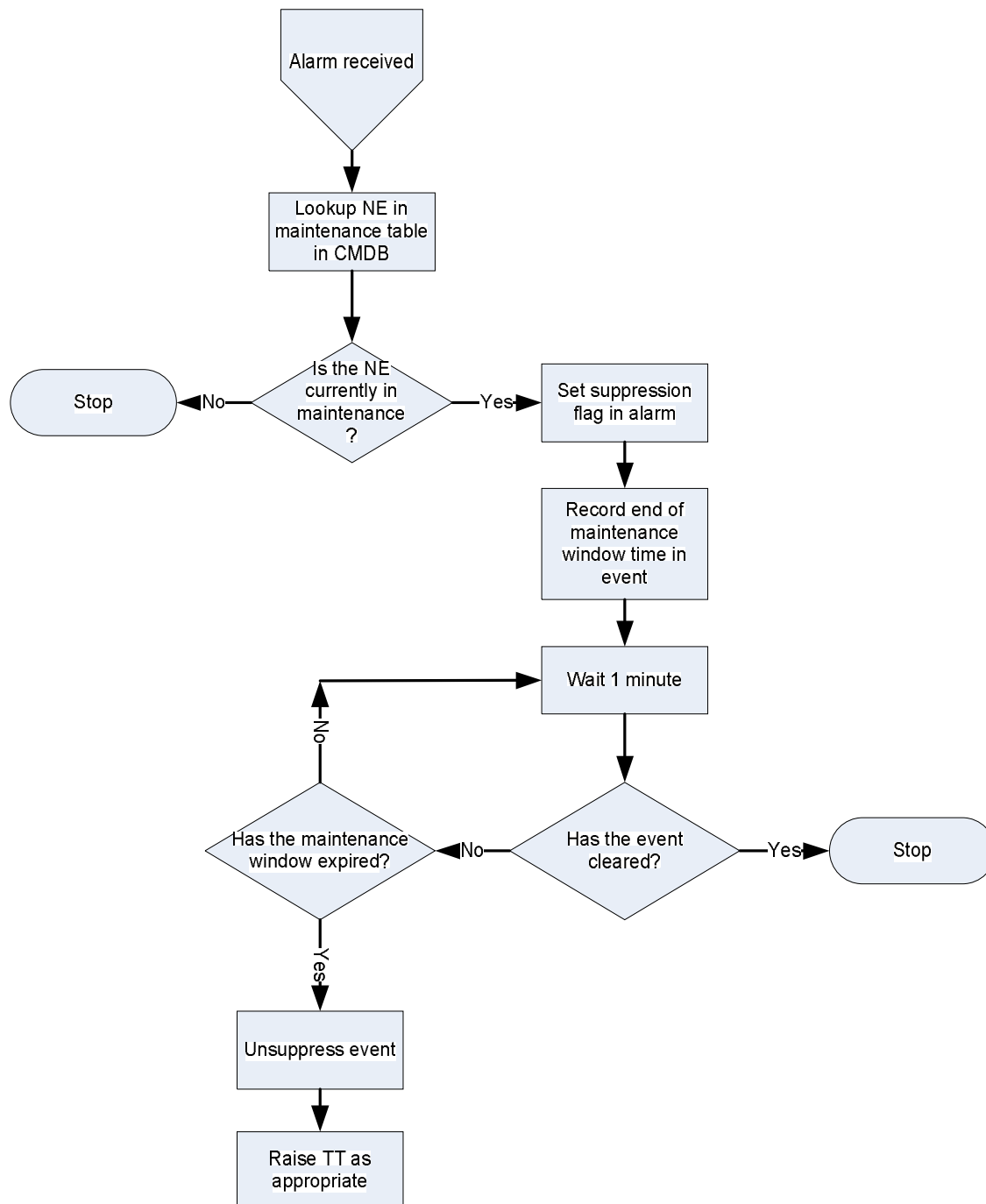
Figure 60: Alarm suppression during maintenance windows Flow Chart

Mobilink OSS Expansion High Level Design

<u>XBL Down Alarm Handling</u>

If the XBL Link down alarm is received from BSC a check needs to be made for corresponding Port Down link and for C7 links Equipped on the port. To check the port on which the XBL down is equipped the commands 'disp_eq 0 xbl <xbl_id> is run, this shows the port and disp_mms 0 <mms_id> is then issued to show the links equipped on the port. If the C7 Links exists and the Link is down this alarm needs to be suppressed and TT created for C7 Link Alarm. If the C7 Links don't exist and the alarm from corresponding RXDCR is found both alarms will be correlated and a single TT will be raised. If the RXDCR alarm is not found a separate TT will need to be generated.

If the XBL Link Down alarm is not received from the BSC and the alarm on RXCDR is found on BSC on the same link both alarms need to be correlated and a single TT needs to be generated otherwise a separate TT should be created if alarm is not found on RXCDR. The commands will be provided by Mobilink to create this correlation.

Mobilink OSS Expansion High Level Design
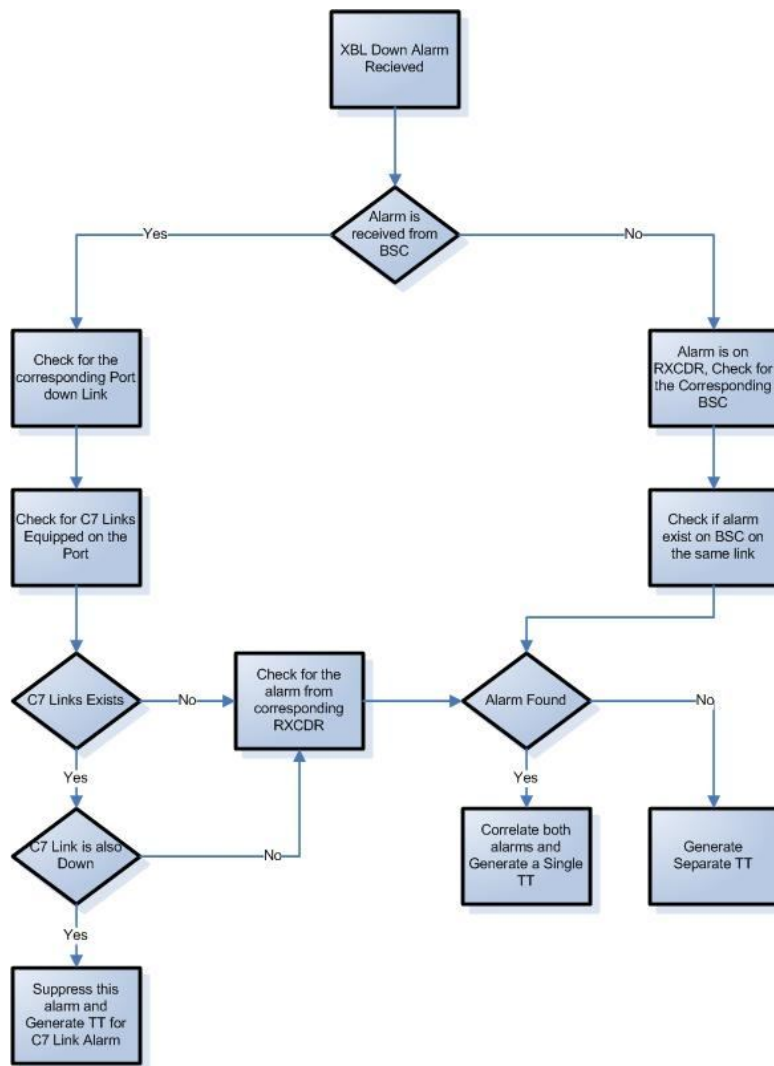
Figure 61: XBL Down Alarm Handling Flow Chart

DPC/ Multiple C7 Links Alarm Handling

When IN Links down with STP the b/m alarm appears at IN end. If 2 or more links are down of the same linkset the alarm should be correlated with STP domain alarms and single TT is to be created after 10 minutes. If a single link is down a TT is not required.

Mobilink OSS Expansion High Level Design
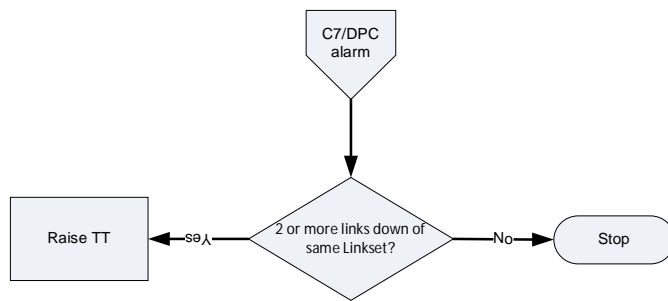
Figure 62: DPC/ Multiple C7 Links Alarm Handling Flow Chart

Call Gapping Alarm Handling

When IN works at 100% of its capacity the alarm 'Intp TlmProcGroup_513:Limit ID 01340G2081CccGL_GlobalLimit has reached 100% of effective limitation [Severity: Major]' appears. A TT should be raised for this alarm after 5 min with the classification of Call Gapping Alarm in the TT
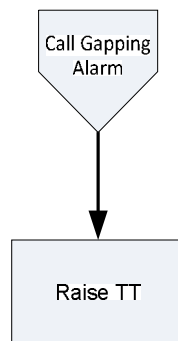
Figure 63: Call Gapping Alarm Handling Flow Chart

Critical Hardware Alarm Handling

When critical Hardware Alarms are received (Mobilink to provide alarm details) A TT should be raised after 10 minutes of the alarm occurrence.
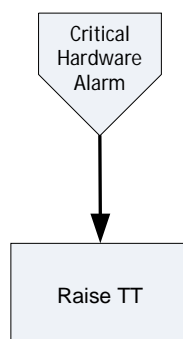
Figure 64: Critical Hardware Alarm Handling Flow Chart

Mobilink OSS Expansion High Level Design

IN Node Down Alarm Handling

A Communication Alarm TT should be raised immediately if any of the alarms occur. When Node is down, Links down with STP too. C7 Link alarms at STP and IN end will be correlated with Node Down scenario.

IN Node Down Alarms include:

- resourceMonitoring: Netmon error for NE 'KHI_IN12': Node 'in2ce1-core2' down , [critical]
- in9ce2:in9ce2: UDP connection failed for LAN IP address 192.168.17.182, in9ce1:in9ce1: UDP connection failed for LAN IP address 192.168.17.181, [critical]
- RtpNm01:RtpNmShutdownNode() called for node CE_01 from RtpShutDownNode01 - timeout = 90000 millisecs., [critical]
- RtpAccYaat01:Audit [RtpAcc04: 13-16] found critical error [DIFF_ATOMICID] [critical]
- [RtpAccSam04-DB: 114374556, RtpAccPam04: 114480421]
- RtpEvtHdl01:connection to dispatcher 'RtpLogOmni01' disconnected, (RtpErrno 1154) [critical]
- "SIGNALWARE: in6ce1.DR: /export/home/omni/bin/dr: in6ce2 inaccessible"
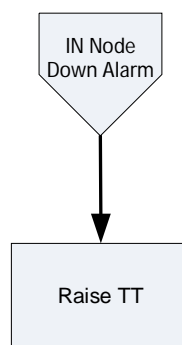
Figure 65: IN Node Down Alarm Handling Flow Chart

Valista Issue Alarm Handling

Valista issues occur at Jazzload Valista Server or M2M server at IPD. When a PayWorkerProc_260 alarm occurs a TT should be raised after a 5 min wait time. The TT classification should be QOS

Mobilink OSS Expansion High Level Design
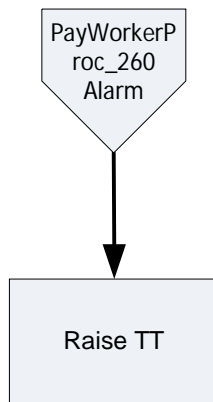
Figure 66: Valista Issue Alarm Handling Flow Chart

Critical Threshold Crossed alarm Handling

Multiple directories and files are created on IN at runtime. When any of these directories reach threshold an alarm is sent. When these alarms a received a TT should be raised with the classification of QOS alarm in the TT after 5 minutes.
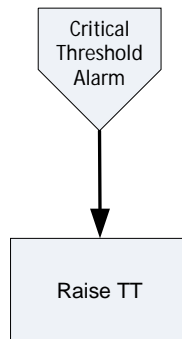
Figure 67: Critical Threshold Crossed alarm Handling Flow Chart

6. Network State Management

6.1 Overview Of Current State Management Process

Currently within TeMIP users login to a single view and can view all alarms based on severity. The alarm list can be filtered and a single alarm list can be opened by a user at any one time. This alarm list constantly changes and it is difficult to follow the list of events. Alcatel Motorola and Huawei BSS alarms are currently displayed in TeMIP.

Mobilink OSS Expansion High Level Design
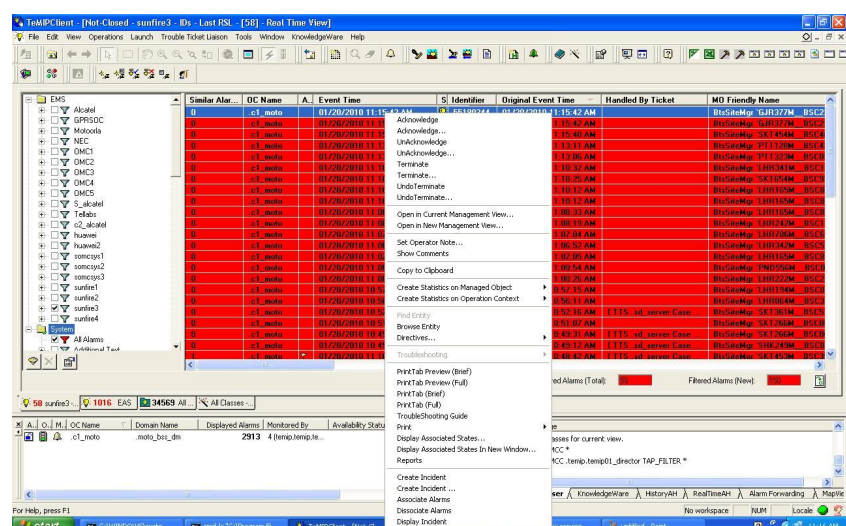
Figure 68: TeMip Alarm List

Users currently log in to the EMS's to view alarm information from the EMS for other alarms such as Alcatel DPC and Huawei EMS alarms.

Figure 69: Huawei Alarm List

6.2 Overview of Proposed State Management Solution

Netcool probes will collect alarm information from the EMS's and pass it to Netcool OMNIbus once the alarm information is processed within the correlation layer Objectserver users can view the alarms in an event list within Netcool Webtop.

Users can also login to OMNIbus and view saved filters the default OMNIbus filters are shown below.

Mobilink OSS Expansion High Level Design
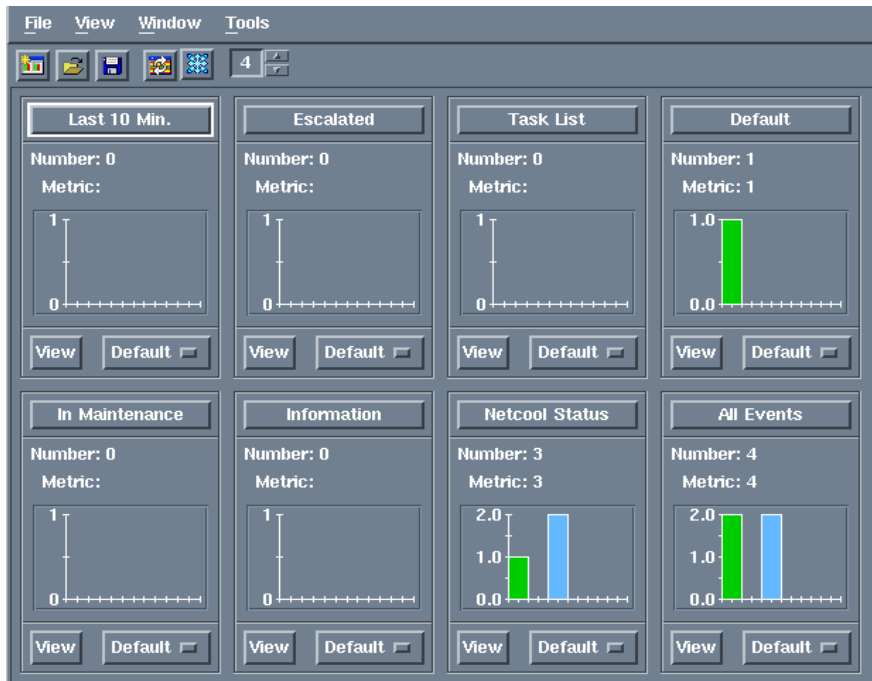
Figure 70: Netcool OMNIbus Default Filters

New Alarms that appear will be displayed at the top of an event list. Within the Active Event list users can filter the events by severity on the single view. For example if a user needs to view only Indeterminate events (purple) they need to click on the purple button within the active event list.
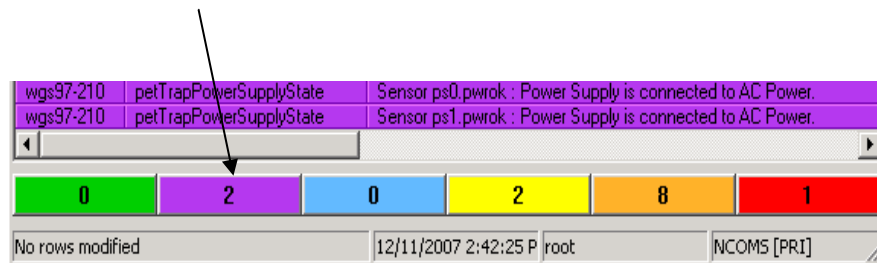
Figure 71: Event Severity Filter in AEL

The Active Event List has the functionality to enable users to export alarms lists to csv files. The Active Event List will also have an option to associate alarms with Trouble Tickets.

6.2.1   Maps and Service Views

A GIS Co-ordinate map is required, the map that will be used for this integration will be Google Earth based. A TBSM service view can be configured to create a map with GIS co-ordinates. The co-ordinates will need to be stored within the cmdb

database and TBSM will look up the co-ordinates to update the map. A filter will also be displayed on this page to show alarms for which GIS co-ordinates are not available. These alarms will be filtered by device type.
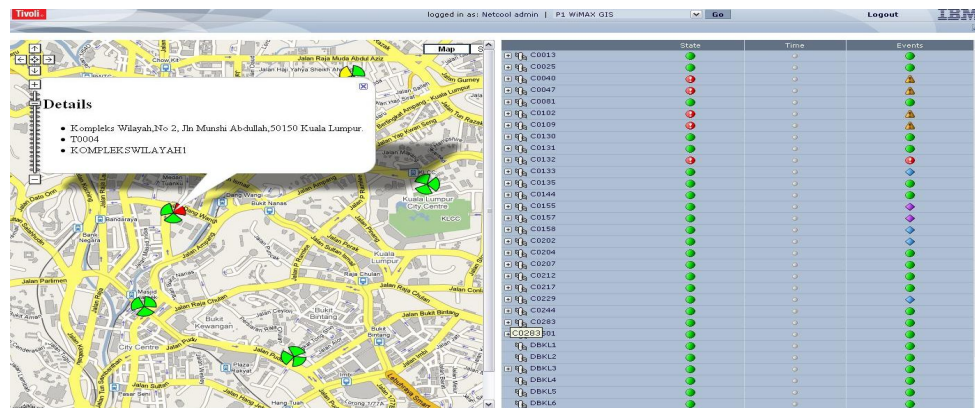
Figure 72: TBSM GIS View

A TBSM service view can show the hierarchical structure of BSC, broken down to Cell level to show the root cause of events with parent child relationship. Users will be able to drill down to cell level to see the alarm that is the root cause.

BSC Hierarchical structure (Business Service View):
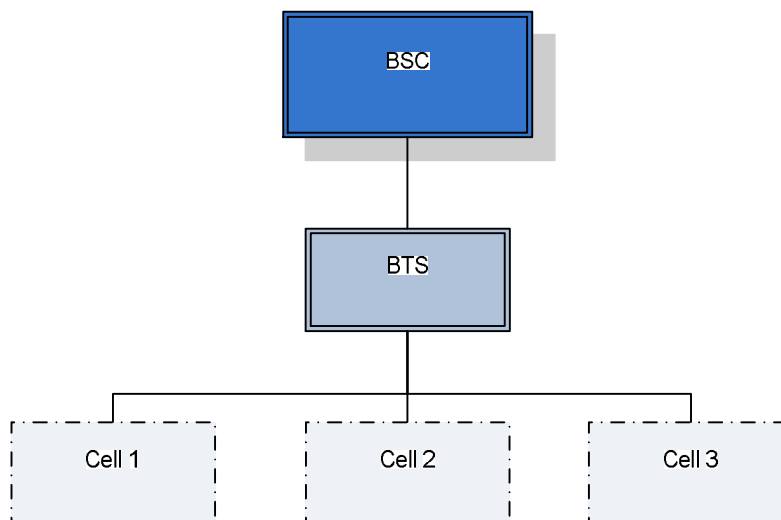
Figure 73: TBSM BSC View

A Netcool Webtop filter view can display alarms that have not cleared within a certain period of time, the user can then delete these alarms from the Objectserver this will then be updated within the journal of the alarm.

Mobilink OSS Expansion High Level Design

6.2.2 Automatic Fault Resolution

A Netcool Webtop CGI tool can be configured to run external commands for alerts, these tools will be made available from the Event List right click option.

For TRE alerts, these commands will restart the TRE. Users will be able to right click on the event in the event list and select the tool to execute the command. Once tool executes a success message will be shown in the window otherwise users can look into the journal of the alarm to see the reason the tool failed to execute.

A batch command file is currently used to run against events (batch_rlogin Batch_rlogin NE_name). Within Impact this command file can be stored in a temporary file and deleted after use.

The other commands that will be configured to run from Netcool Webtop CGI scripts include:

- Reset / Lock / Unlock after logging in to BSC and changing access level

    - reset_dev siteid devicename deviceid
        - reset_dev 1 dri 1 1
    - lock siteid devicename deviceid
    - unlock siteid devicename deviceid
- Core commands which include:

STP commands

- rept-stat-trbl - shows all active alarms on STP Node
- rept-stat-ls:lsn= - shows links status in linkset
- rept-stat-sccp - shows STP cards and CPU utilization
- rtrv-slk:loc=2301- shows links status on specific card location
- rept-stat-e1:loc=2301 - shows E1s/DIUs status on STP Cards
- rtrv-rte:dpcn=8388-aa - shows DPC direction/name of DPC alarms

Siemens MSCs commands

- STATPORT - shows DIU direction and status
- STATTRUNK - shows trunk group status
- DISPSIGLINK - shows all links at MSC towards different direction
- DISPC7DLLTG - shows DIUs at which links are configured
- DISPC7TGREL - shows trunk group and DPC relationship
- DISPNUC - checks NUC status

Alcatel MSCs commands

- QMCIL - shows DIU direction and status

Mobilink OSS Expansion High Level Design

- CTIN - shows trunks status in specific DPC
- FSMIN- shows all links at MSC towards different direction
- LDIL - checks NUC status

Huawei MSCs commands

- DSP N7DLNK - shows links status at MSC towards any DPC
- LST N7DLNK - shows all links at MSC towards different direction
- DSP OFTK - shows trunks status
- DSP TDMSTAT - shows DIU status
- LST SPC   - checks NUC status
- LST TKCBYTID- shows relationship between CIC and DIU

IN Nodes commands

- df-k -IN Disk and Directories capacity
- dkmirror-Al - IN node system Disks status online or mirrored
- sar 1 5 - avg Cpu utilization
- uptime- last active node time

6.3 Outage Management

Maintenance windows to be included in CMDB design are the following types

- o Work Order
- o ECRF – Engineering Change Request Form (OVSD integration)
- o Preventative Maintenance Cycles

- Tool is required to insert emergency change windows into CMDB
- Parent/child relationships to be carried through maintenance windows
- Tool to end maintenance window early
- Impact policy to read maintenance window data for event
- Maintenance flag set to allow filtering in views and TT creationField for maintenance window times in Objectserver
- Different flag values to indicate differing reasons for outage window (i.e. planned works, power schedule – exact details to come)
- If alarm still outstanding at end of window, flag to be reset to allow Ops to view and TT to be created
- Reports based on flag value and time windows, including for events outstanding at expiry of maintenance window.

Mobilink require the ability to view the Preventative Maintenance type to be added to the alarm. This will need to be configured in the probe rules to associate alarm with the Preventative Maintenance type.

7. Trouble Ticketing & Resolution

7.1 Overview of Current Work Order Flow

Mobilink have fault resolution process to handle events or incident on Mobilink Network, which is currently managed by HP Service Desk application. Mobilink resolution process is not based on ITIL (Information Technology Infrastructure Library) incident management and only level 1 escalation is currently carried out by the service desk application and according to the Mobilink team, the HP Service Desk application does not support multi-level escalation for approval or rejection, so they mostly maintain it by email for higher level approval or by using different portal to escalates email for ticket life cycle. Following is the fault management process overview:

Events are forwarding from TEMIP system to Service Desk and initially HLO receive the open incident request which is automatically raised based on event field criteria. HLO assign the incident to OAN department for resolving it and also HLO decides to send incident request to Out Source vendor and raised the Work Order for them and send email to all concerned. Below is a flow chart showing the current Work Order Process Flow
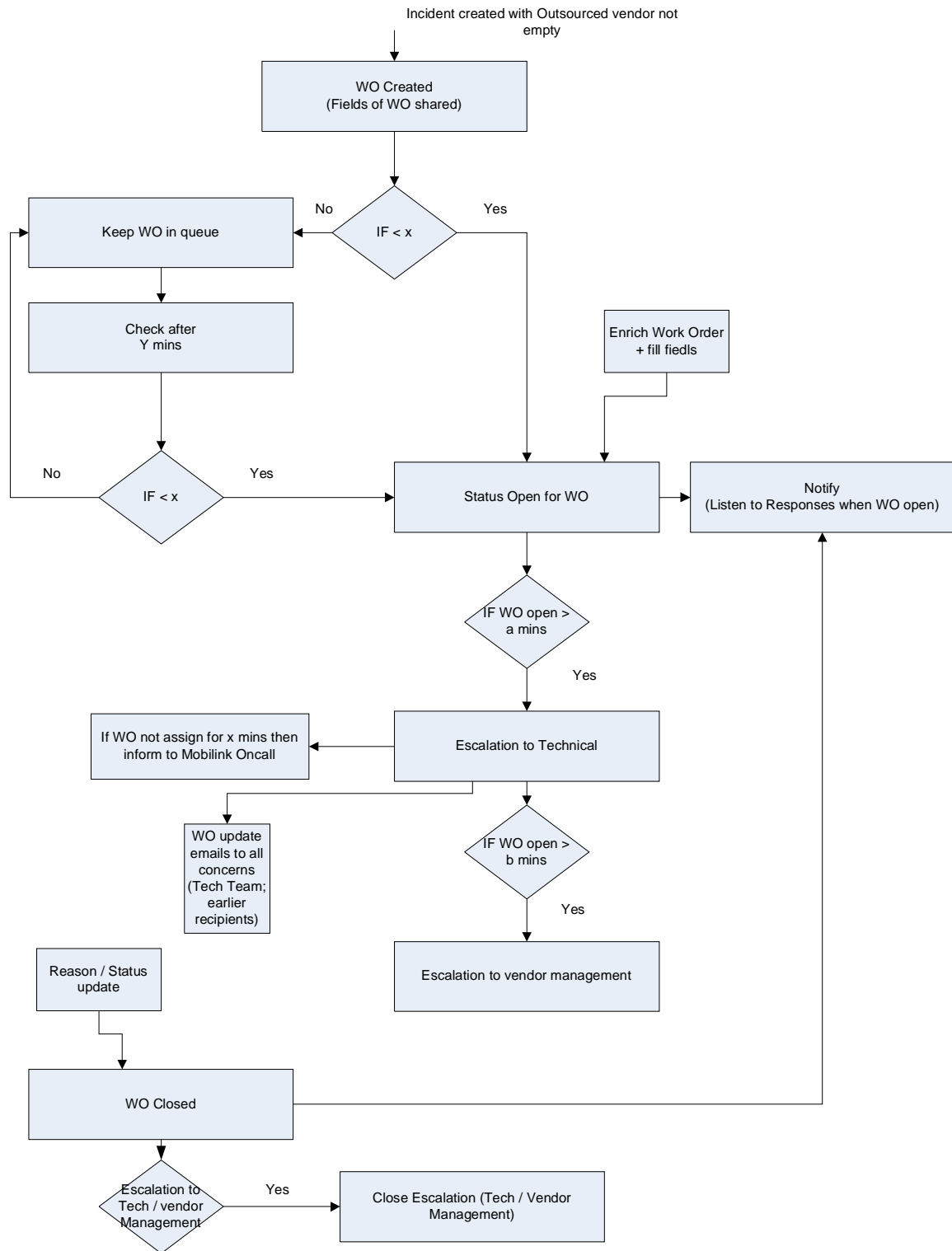
Figure 74: Work Order Process Flow

Mobilink OSS Expansion High Level Design

7.2 Overview of Proposed Trouble Ticketing Solution

The purpose of the Incident Management process is to focus on the restoration of a service affected by any real or potential interruption which has impact upon the quality of service.

As a result of the successful implementation of the Incident Management Process:

- IT service is rapidly restored
- Multi-level escalation would be achieved
- Customization of Incident Application
- Knowledge base will build and help for resolving similar issues or faults
- Major or Small Changes would be recorded for historical Reporting
- IT service availability is sustained at a high level
- Workarounds to resolve similar service interruptions are created
- Potential improvements to services may be identified
- Communication history logs for whole ticket life cycle are created

Service Level Agreement will be achieved between vendors or department as per Mobilink requirement

- Incidents can be raised by many processes.
- While responding to an incident, it is possible that a change request might be created, which would be handled by Change Management. In addition, an incident may be raised during the processing of a change request.
- When a fault is detected by Event Management, an incident may be raised and submitted to Incident Management. Once the incident is resolved, the incident record is closed and Event Management is notified.
- Problem Management looks at groups of related incidents to determine if there is a root cause to those related incidents. During incident closure problems may be raised where there is an underlying or ongoing problem needing Root Cause Analysis and problem resolution.
- Request Fulfillment is the user-facing process for the Service Desk. When a request is recognized as an incident, it is routed to Incident Management.
- The resolution of incidents is important to the management of service levels in Service Level Management.
- The resolution of incidents may involve the implementation of changes using Change Management.

Problem Management Workflow:
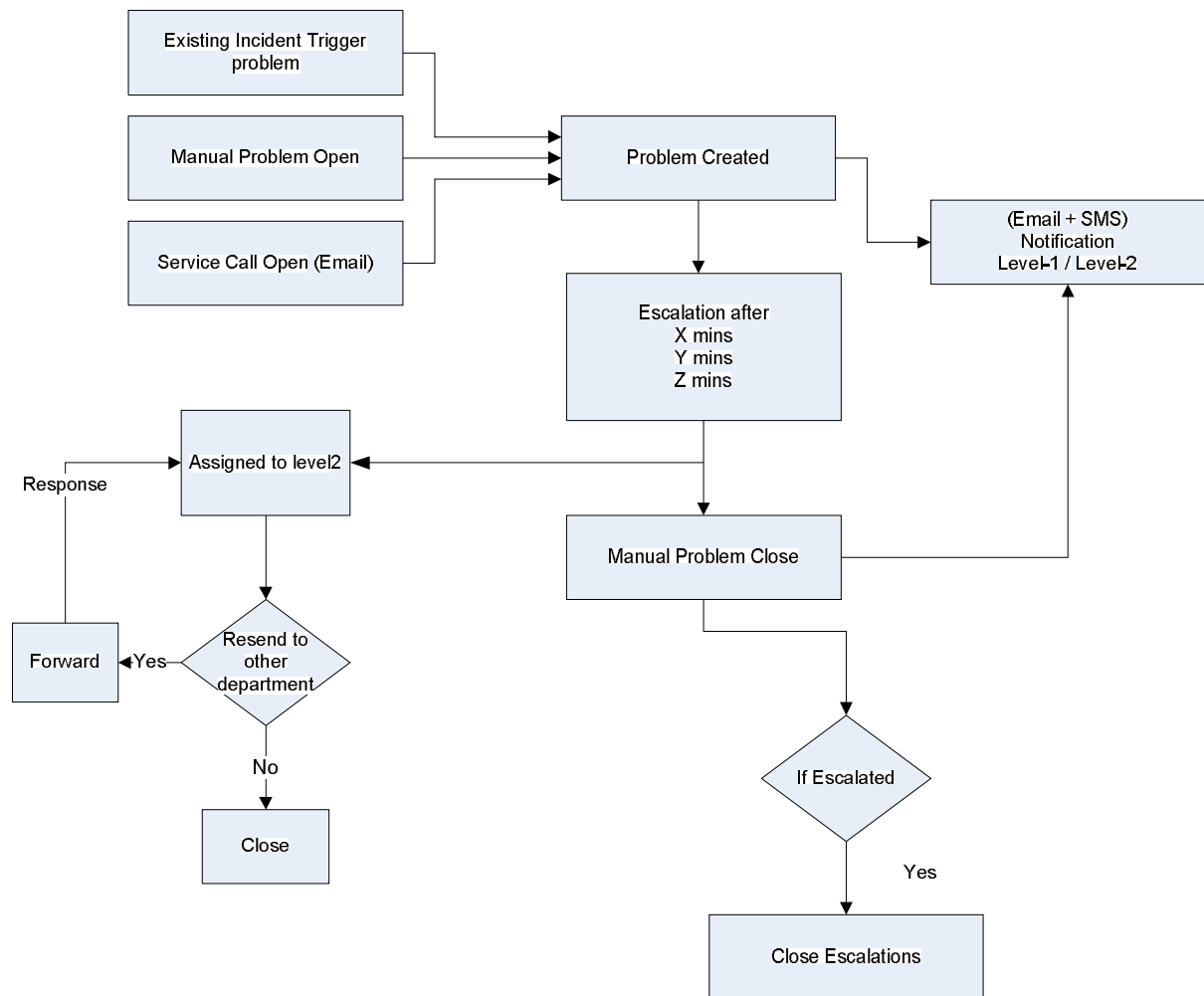
Figure 75: Problem Management Workflow

7.2.1   Trouble Incident Definition

An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident.

7.2.2   Trouble Incident Handling Process Flow

The below diagram shows the overview for Incident Management process based on ITIL guide lines for Mobilink Fault Management.
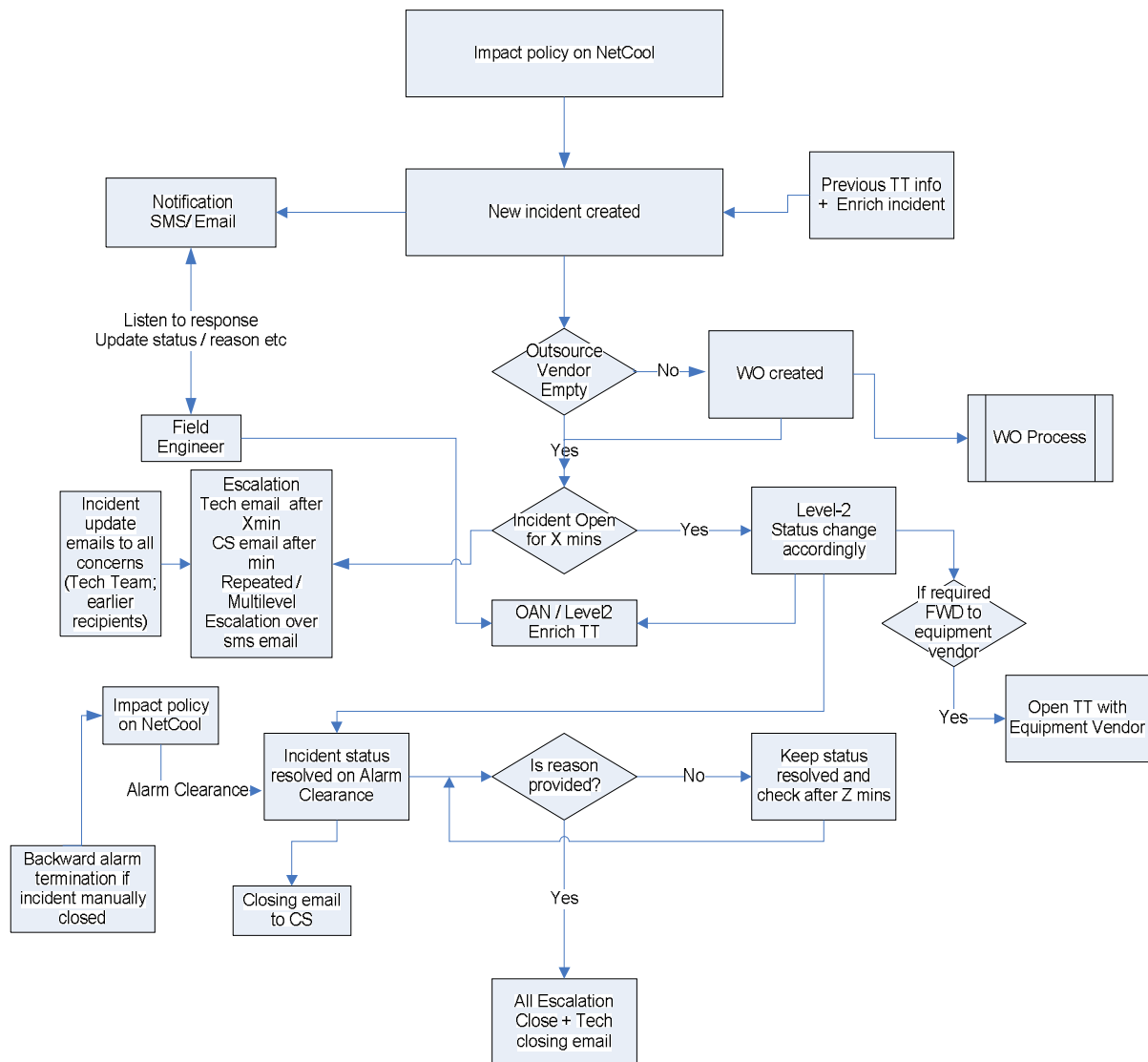
Figure 76: Mobilink Incident Management

7.2.3 Automatic Trouble Incident Creation

Incident can be reported by users or raised via Fault Management system. In the proposed solution the Incident Management system is tightly integrated with Fault Management, so Fault Management system can raise the Incident ticket automatically based on pre-defined fields or attribute in the event data, which are prioritize events to establish appropriate action or response, especially responding to conditions that could lead to potential faults or incidents and open trouble ticket to resolve the incidents according to incident management process.

Mobilink OSS Expansion High Level Design

7.2.4   Incident Fields in TSRM

The following fields will be included for Incident Management. This will be configured in TSRM so users can view these fields.

Number	Field Name	Field Description
1	Incident ID	Unique ID for each Incident
2	Requester Name	
3	Requester Workgroup	
4	Incident Description	
5	Incident Open Time	
6	Incident Priority	
7	Incident Impact	
8	Alarm Severity	Transferred from Alarms
9	Alarm Details	Transferred from Alarms
10	List of Affected MO's	Transferred from Alarms
11	Failure Reason	User entered reason text
12	Summary of Repair Actions	
13	Work Assignment Time	
14	Work Completion Time	
15	Incident Close Time	

Table 5: Incident Fields

7.2.5   Assignment Policies

The assignment policies on different stages of Incident Management would be like

- Determine Appropriate Person to Fix the Fault
  - Where is the Incident?
  - What technical knowledge is required?
- Record the Assignee in Incident Management
  - Select the Role and Assign to the Incident
- Notify the Assignee
  - Email
  - Through TSRM
  - Telephone Call
  - Through TelAlert SMS
- Notify Affected Parties / Services
  - Users of these services can be notified via the Service Desk
  - E.g. Broadcast email

7.2.6   Email Escalation Policies

Following are the email escalation policies which are based on Mobilink requirement.

Mobilink OSS Expansion High Level Design

- Emails are escalated based on ticket opening time.
- W-mint of time email will send to team Lead
- X-mint of time emails will send to Regional Management
- Y-mint of time emails will send to National Management
- Z-mint of time emails will send to CTO
- Emails send to CS Team as well
- X-mint of time emails will send to OV (Manager) in case if ticket is pending at OV
- Y-mint of time emails will send to OV (GM) in case if ticket is pending at OV
- Closing status on incident updates all concerns people or department
- Email templates should have history of log of tickets.
- Communications history logs for different stages of tickets would require.
- Mobilink have a provision to send emails or notification manually

7.2.7   Trouble Incident Update Notification

Incident Management work flow will be configured to send update notification to all those concerned during ticket life cycle according to the Mobilink requirement, which are as follows

- Communications notification will contain history logs for different stages of tickets.
- Incident work flow has provision to send notification to concerned groups or roles during ticket life cycle.

7.2.8   Preventative Maintenance Work Process Flow

Mobilink has to implement a multi-level approval process for PM activity like Incident, Problem and Change Management and they also require email notification at every stage of PM life cycle.

As result of successful implementation of PM workflow

- PM Activities are introduced in a timely and controlled manner.
- The site engineer would inform about the PM Activity by Email
- Mobilink Team can assign the priority on PM by manually.
- Mobilink can generate report for PM activities based on their start and finish date or time.
- The process will create Work Order automatically for PM activities.

The following process diagram shows an overview of PM work flow:
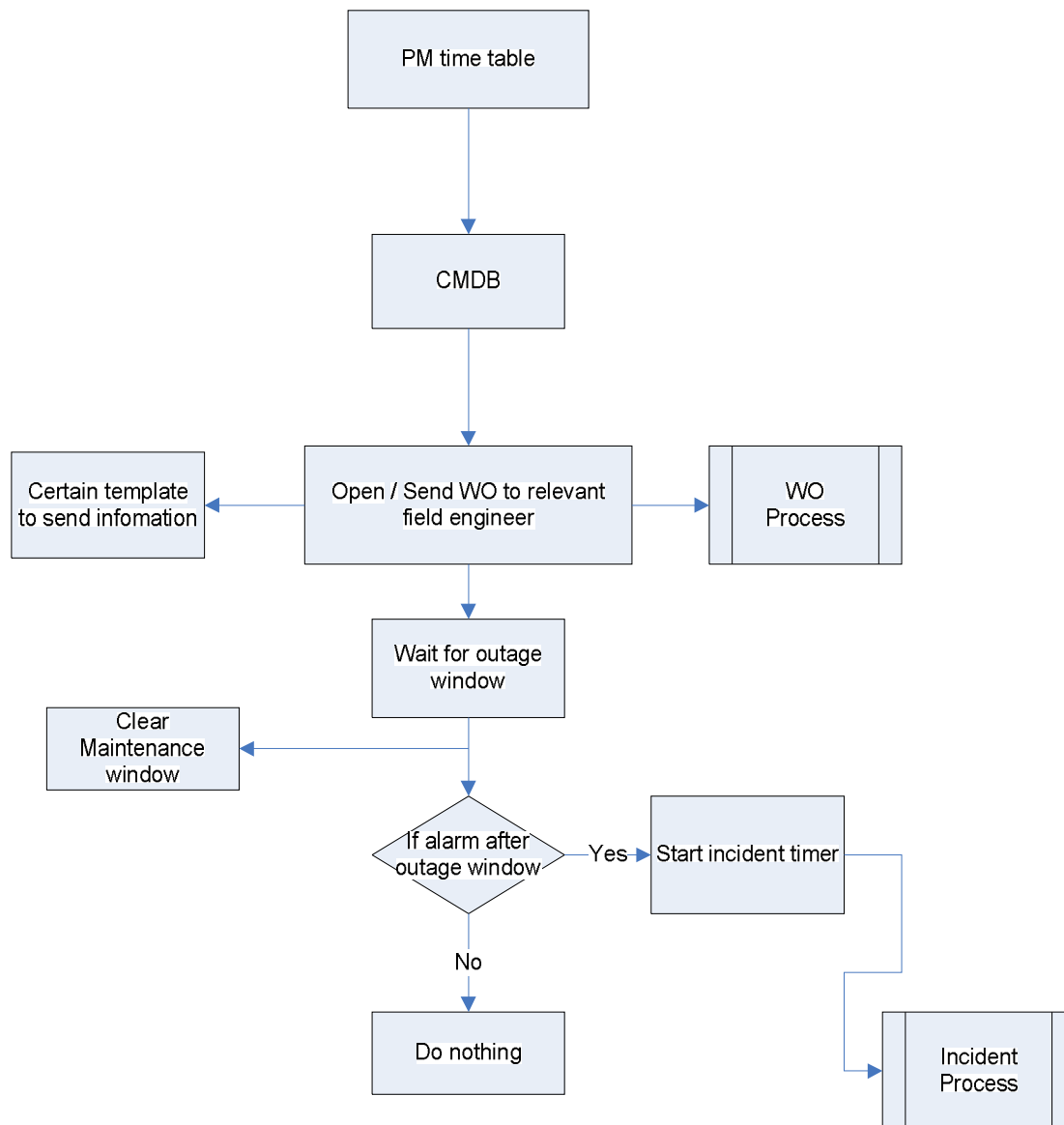
Figure 77: Preventative Maintenance Workflow

Mobilink OSS Expansion High Level Design

7.2.9   Escalation Policies

External Notification

It was identified from the requirements capture that a TelAlert integration is required. TelAlert integration will be carried out with Netcool to pass event information to TelAlert for it to handle the roistering of escalations and the generation of sms and email alerts.

Once alarm information is passed to TelAlert and an e-mail or sms notification is sent a confirmation alarm will be received in the event list once Mobilink configure TelAlert to send a confirmation message to Netcool for 2-way communication. Mobilink will be required to configure TelAlert to send messages to Netcool OMNIbus.

Mobilink would like the ability for users to send an email or sms into the system with a TT number of NE ID and get back TT information or current alarms for the NE within TSRM. TSRM can be configured to send e-mail alerts.

7.2.10 Knowledgebase

A Knowledge base is required. This is a part of TSRM / CCMDB process and will be populated after TSRM / CCMDB processes implementation. The buildup of the knowledge will be managed by Mobilink to include fault resolution. As each resolution is made it should be noted within the knowledgebase by the user who resolved the issue. The knowledgebase contains text based information records and a workflow cannot be attached with it but can be customized within the application to add any resolution diagram or workflow with open incident before closing it. This is dependent on Mobilink's workflow or policy to handle the incident.

8. Configuration Change Management

8.1 Overview of the Proposed Configuration Change Management Solution

The purpose of the Change Management process is to achieve the successful introduction of changes to Mobilink environment. Success is measured as a balance of the timeliness and completeness of change implementation, the cost of implementation, and the minimization of disruption caused in the target system or environment. The process also ensures that appropriate details of changes to IT resources (assets, CIs) are recorded.

The below points details Mobilink's proposed change management process.

1. Every user logins from his Mobilink ID and address book must be synchronized with the application, allowing the change form to read data from Mobilink address book (Employee Name, Phone Number, reporting manager, department etc).

2. On the change form if Network Change Management approval required check box is enabled, then change form submitted to NCM domain.

3. Initiator will request the change to their respective TM (Team manager) for the internal approvals mentioned on the address book and in some cases NCM fixed the TM as per NCM requirement. secondly their should be concept of multiple TM selection like primary , secondary, thirdly as if primary TM Is not available so secondary TM approves the activity.

4. Initiator has access to add multiple executors on the change form and activity status is considered as Implemented / closed once all the respective executor departments executes at their respective ends.

5. TM will have the access to reassign the change back to originator for more info and disapproved status.

6. Once Change is approved by TM, then Change form submitted to NCM team for further approvals / review and Initiator will not allow changing the form.

7. NCM will reassign the form back to initiator for further requirements if any, on reassigning to initiator respective TM is updated via system/email/sms.

8. NCM have access to change any field status in the change form.

9. Application will highlight the conflicts (NE and child levels) within change form and on separate window as well. If conflict found then change form is rescheduled or cancelled.

Conflict management (This should be through NE codes like if Initiator selected KHI349-Jackey Trade from the NDBS (Network data base sheet) and if this NE is already selected by another Initiator then conflict is highlighted.

Initiator will have the option for multiple NE selections as well and application will check their conflict accordingly.

10. On submitting the change form: it's automatically submitted to next level management (Directors) according to the activity criteria (Access domain, Core domain) and further if Service Impact / Revenue loss then submitted for CTO approvals. Same criteria of multiple approving (point 3 in above) authorities apply, that if primary authority is not available so secondary can approve. Secondly if we have multiple approving authorities of same domain or other

then if any authority disapproves the single activity then this activity is considered as disapproved even the second authority approves the activity.

11. Final status of the activity after higher management approvals is only updated to NCM domain via email/ sms/system and NCM have authority to inform the concerning teams via sms/ email (proper designed email format with recipients list) and update the activity status over system.

12. Export the data in two ways like export in excel and customize email format with the recipient's lists. And recipients list are fetch from Mobilink address book.

13. For closings: referred to implement part of WO system (Figure in below).

14. Customized extraction of reports on daily/monthly/yearly basis.

15. Searching criteria: Searching criteria should be very strong that any Change ID/ NE's / Originator & executor details/ activity type etc search can be done through this system as like as any field / output field will be searched from the change form.

16. Problem to change.

17. The ECRF system is independent from any portal/system. (Unlimited field, no character limitations, no field restriction) and System admin team will have access to add/ delete/ modify the change form fields according to the requirements.

18. Network level Notifications would be displays on new ECRF window or main page of the change process system.

19. For an emergency activity customized sms is submitted to team manager for approvals, once approved then same sms is floated to required team members and NCM for further upper level management / Directors level approvals. Secondly there should be any pop ups over the service desk for any emergency activity. Secondly NCM team will have an access that when they forwarded the sms to change application system then the respective activity status is updated on the application for further proceedings.

20. Team manager/ upper Management/NCM approvals can be through sms/email/system by any format method.

21. Any event change can trigger the email/sms notifications and logs were maintained accordingly.

22. There would be flexibility on the system that multiple security checks / ownerships will be implemented like extraction of reports is only extracted by system admin / ncm team or users. System admin team has access to implement any security checks at any user level.

23. All the change forms are kept under the history and fetched by any user level or admin level.

8.2 Change Management Process flow diagrams

The flow chart shown below shows the workflow required for the Mobilink change management process.

Figure 78: Mobilink Change Management Flow
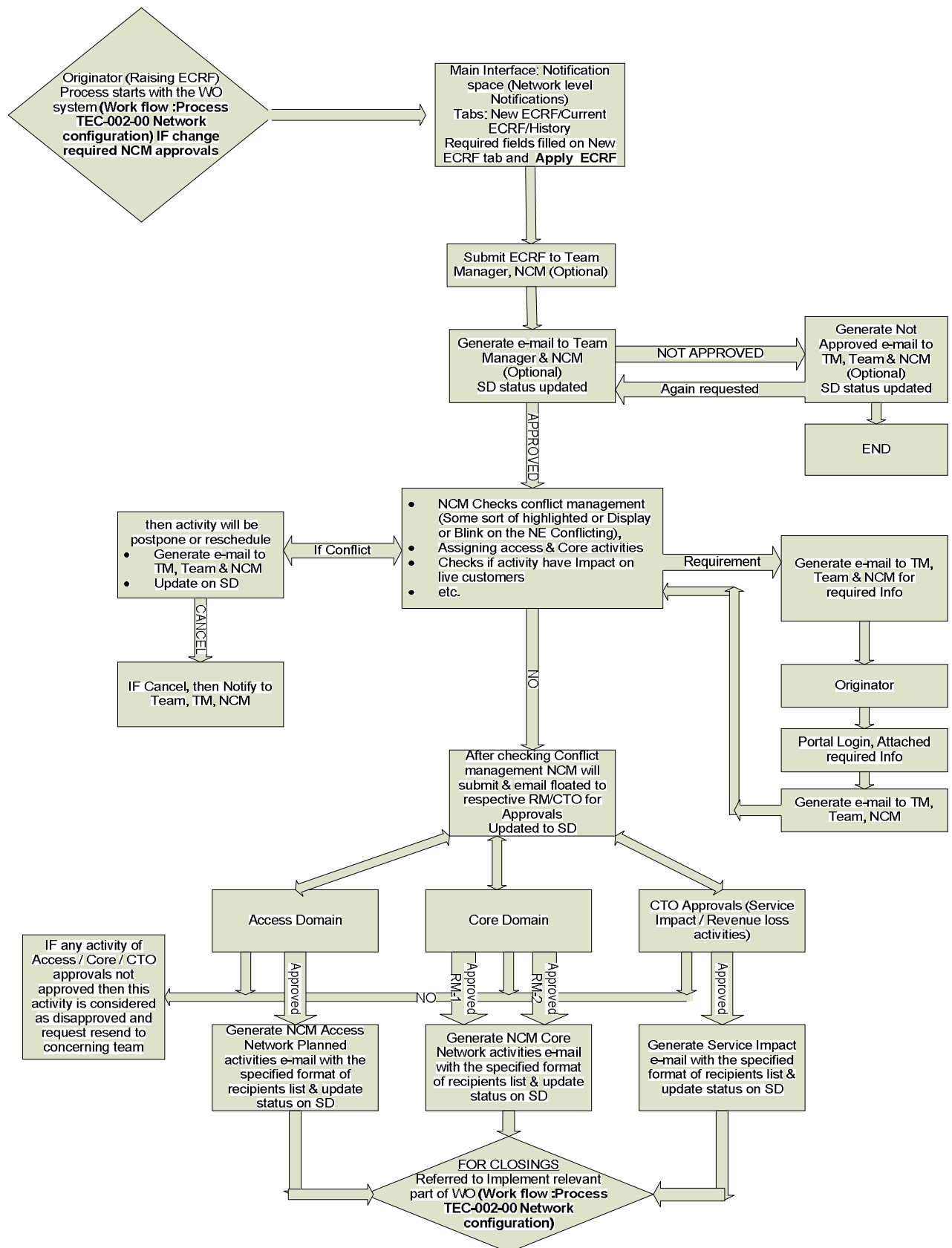
Figure 79: Mobilink Change Forms Flow Chart

Mobilink OSS Expansion High Level Design

9. Reporting

9.1 Overview of the Current Reporting Process

Currently Excel reports are used for network data. TeMIP has the functionality to export alarm list data to a report. Users are currently exporting the alarm information that is required and then presenting the data onto a excel spreadsheet.

9.2 Overview of the Proposed Reporting Solution

Users can create event based reports within Netcool reporter by selecting the event type from the GUI. Reporter will generate the reports from the alarm information that is stored in the oracle database or available in the Objectserver. The alarm details are passed from there Objectserver to the Oracle database from the oracle gateway that will be installed and configured. Tivoli Common Reports (TCR) can be configured to create alarm reports that show statistics of the alarm and graphs for users to view. Report data that is not available as part of the alarm or in the database will be uploaded into the database by Mobilink.

Below are the reports that will be configured.

Power Issue Reporting

This report shows, Low voltage alarms, Genset alarms and RSL alarms. Reporter will be configured to allow users to select these alarms and generate a report showing these alarms.

Core site IU level outage report

Users will have the option to select the alarm DI Alarm to generate a report showing DI alarms for core site IU level outage report.

Signaling Link Alarm

This report can be created by select the signaling link alarm from Reporter to show all signaling link alarms in a report.

RSL alarm report

Reporter can be configured to allow users generate alarm based reports for RSL alarms.

Down DRI reports

Down DRI reports show all problematic DRI information. This report can be generated from Netcool Reporter and can be configured to show the BSC name, Site name and DRI status of the alarms.

Mobilink OSS Expansion High Level Design

Down TRX Reports

Reporter can be configured to allow users to generate a report base on TRX alarms showing only major and minor alarms on TRX's for all OMC's.

BSS Network Report

The BSS Network Report shows information of PCUs, MFS, RXDCR, MSCs, RTF's, BSCs, Sites, Cities on a regional basis. Reporter will need to configured to allow users to generate the BSS Network report based on region/ city information

Nationwide Cell Level GPRS Report

This report shows information of down gprs at BSC level. The status of GPRS is also required as well as MFS, Shelf, Rack and GPU. Reporter can be configured to allow users to generate this report.

Secondary Path Report

Showing information of any one of the two MMS paths that are down. This report can be generated from TCR to show alarm statistics. TCR will be configured to allow users to generate alarm reports that show MMS paths are down.

GPRS Report

This report contains information of down PCUs, GBL, GDS and GSL of the network. Reporter can be configured to allow users to generate this report showing alarms for PCUs, GBL GDS and GSL.

Nationwide Cell Level Report

This report should show the status of GPRS, MFS Shelf, Rack and GPU at the Cell level and contain information of the associated BSC name, Site name, Cell name and Alarm status information for Motorola NE's and Alcatel NE's. Reporter can be configured for users to generate this report by the GUI interface. If the alarm does not contain cell name, BSC name and Site name then this information will need to be stored in the Oracle database for reporter to pull this information to create the report.

Trouble Ticketing statistics Report

A report showing TT statistics is required, this can be configured in TSRM for user to view and export TT statistics reports.

Inventory Level Report of Network

The report data needs to be held in the ccmdb and users can view Inventory level report of complete Network from cmdb.

Radio Configuration Report

A radio config report showing number of radios (DRI or TRX) will be configured in TSRM for users to view Radio Configuration alarm details.

Network Unavailability Report

This report should show the reason of the alarm that has been included by the user against the Trouble Ticket. This report can be configured in TSRM to show the alarm details such as Alarm Occuring, Alarm Clearing, Total Down Time on cell level, value of NUR, Availability/ Unavailability and also include the reason of the alarm.

Change Management Workflow Report:

Mobilink require reports which would generate by scheduled and email automatically in HTML format. They need open and close tickets report for each person who handover the shift to other and also can system send email automatically this can be configured within the ccmdb.

NUR/Down site reports

These reports can be generated from TSRM and provide the outage reasons from the TT in TSRM for NUR / Down sites.

Reporter will be configured to allow users to select a time period to create reports for alerts that occurred within the specified time period.

A requirement for Trouble Ticket Alarm reports was identified. Netcool Reporter will be configured to allow users to create reports for alarms which have a Trouble ticket raised against them.

Down Site Report

This report should show all the down sites based on vendors. Reporter can be configured to show alarms indicating down sites in the reports. Mobilink will need to provide the vendor details associated with each alarm and store in the database in order to configure Reporter to show the vendor based report.

10.   Server Monitoring

Mobilink wish to monitor CPU, Memory, error logs and processes for the following servers

IN Servers:

Location	Entity	IP Addresses	Managing EMS	OS
ISB	IN6-ISB	10.13.1.1; 10.13.1.4	Advantage comm1	Solaris 9
ISB	IN7-ISB	10.13.1.51; 10.13.1.54	Advantage comm1	Solaris 9
ISB	IN8-ISB	10.13.1.102; 10.13.1.104	Advantage comm1	Solaris 9
ISB	IN9-ISB	10.13.1.151; 10.13.1.155	Advantage comm1	Solaris 9
ISB	IN10-ISB	10.13.4.1; 10.13.4.4	Advantage comm2	Solaris 9
KHI	IN11-KHI	10.14.4.1; 10.14.4.5	Advantage comm2	Solaris 9
KHI	IN12-KHI	10.14.5.35; 10.14.5.37	Advantage comm2	Solaris 9
KHI	IN13-KHI	10.14.5.65; 10.14.5.68	Advantage comm2	Solaris 9
KHI	IN14-KHI	10.14.5.99; 10.14.5.102	Advantage comm3	Solaris 9
KHI	IN15-KHI	10.14.5.131; 10.14.5.134	Advantage comm3	Solaris 9
KHI	IN16-KHI	10.14.4.163; 10.14.4.168	Advantage comm3	Solaris 9
KHI	IN17-KHI	10.14.5.193; 10.14.5.198	Advantage comm3	Solaris 9
LHR	IN18-LHR	10.12.5.35; 10.12.5.38	Advantage comm3	Solaris 9
LHR	IN19-LHR	10.12.5.71; 10.12.5.73	Advantage comm4	Solaris 9
LHR	IN20-LHR	10.12.5.100; 10.12.5.101	Advantage comm4	Solaris 9
FSD	IN21-FSD	10.23.5.35; 10.23.5.38	Advantage comm4	Solaris 9
FSD	IN22-FSD	10.23.5.72; 10.23.5.73	Advantage comm4	Solaris 9
FSD	IN23-FSD	10.23.5.99; 10.23.5.102	Advantage comm4	Solaris 9
ISB	VOMS	172.27.100.37; 172.27.100.39	Advantage comm5	Solaris 9
ISB	Advantage comm1	10.13.1.10		Solaris 9
ISB	Advantage comm2	10.13.4.20		Solaris 9
KHI	Advantage comm3	10.14.2.30		Solaris 9
LHR	Advantage comm4	10.12.2.5		Solaris 9
ISB	Advantage comm5	172.27.100.49		Solaris 9
ISB	CX	10.13.5.249; 10.13.4.240; 10.13.4.230; 10.13.4.235	Advantage comm2	Solaris 9
ISB	IPD	10.229.6.99; 10.229.6.102; 10.229.6.105	Advantage comm2	Solaris 9
ISB	IPD-LB	10.229.6.164; 10.229.6.165	Advantage comm2	Solaris 9
ISB	M2M	10.200.70.33;10.200.70.35	Web GUI	Linux
ISB	UCP/RB application servers	10.200.75.10;10.200.75.12	Web GUI	Linux
ISB	UCP/RB MGw server	10.200.75.14;10.200.75.16; 10.200.75.18	Web GUI	Linux
LHR	Voice mail server	10.12.7.10	Web GUI	Linux

Table 6: Mobilink IN Server List

VAS Servers:

Node	Entities	No. of Servers	OS	Vendor
PSA	HP 9000 rp4440	2	HP-UX	Acision
D2CP	HP ProLiant DL360	2	Linux	Vollubill
ADM		2	Linux	Invigo

Mobilink OSS Expansion High Level Design

GPRS Core	WN 1200	2	?	Alcatel
	Senteon : SunFire V240	2	Sun Solaris	Alcatel
	Vigilon : SunFire V240	1	Sun Solaris	Alcatel
	DNS : HP ProLiant DL320	4	Sun Solaris	Alcatel
	SGSN : ALPHA SERVER DS 10	14	HP-UX	Alcatel
	WAP GW : HP ProLiant DL 380	2	Linux	Alcatel
	HP 9000 rp4440	1	?	Alcatel
	ATCA	1	?	Alcatel
	OMCPs(HP rp5430)	1	?	Alcatel
	OMCCN (HP Server)	1	?	Alcatel
OMG	HP DL385 G2 (Hydrogen)	1	Linux	Acision
	HP DL385 G2 (Arsenic)	1	Linux	Acision
	HP DL385 G2 (Germanium)	1	Linux	Acision
BT	HP ProLiant DL385 G2	2	Linux	Acision
MMSC	SunFire X4100 Server	7	Linux	Acision
Gcash	Dell PowerEdge 2950	6	Linux	Utiba
CRBT	URP 8100	6	Linux	Huawei
	MGW	6	Linux	Huawei
	ISB USDP DB HP rx2660	1	Linux	Huawei
	ISB CALL DB HP rx2660	6	Linux	Huawei
Valista	HP Proliant ML350 Server	1	Linux	Multilynx
	HP Proliant DL380 Server	4	Linux	Multilynx
	HP Proliant DL580 Server	3	Linux	Multilynx
	IBM Server P6	3	Linux	Utiba extention
	IBM System x3550 (HMC)	1	Linux	Utiba extention
Byte Mobile	Sunfire X4200 Server	2	?	Tech access
OTA	SunFire V440	1	Sun Solaris	SunOS 5.9
KPI	SIM Server HW-S336-PERP	1	Linux	ArgoGroup
	Monitor Agent HW-X1000-PERP	4	Windows Xp	ArgoGroup
	Siemens EDGE modem -HW-X1000-MC75-PERP	4	Windows Xp	ArgoGroup
	Remote SIM Multiplexer emulator chip HW-X1000-RSIM	4	Windows Xp	ArgoGroup
	Monitor Master Quality Manager	1	Windows Xp	ArgoGroup
	Device manager Xpress X-3200	1	Windows Xp	ArgoGroup
ODP	ODP Server HP Proliant DL-380	2	Linux	Cibenix
	ODP Server HP Proliant DL-160	2	Linux	Cibenix
CMS	HP Proliant DL360 G5 Server	3	Linux	Interact
	HP Proliant DL380 G5 Server	7	Linux	Interact
Video Streaming	HP Proliant DL360 G5	2	Linux	Interact
	HP xw6400 Server	4	Linux	Interact
	HP Proliant DL380 Server	2	Linux	Interact
	Sierravideo Systems Server	1	Linux	Interact

Table 7: Mobilink VAS Server List

HLS Servers:

Server Type	No. of Servers	OS
Front end servers	54	Solaris 8
Back end servers	58	Solaris 8
Management servers	2	Solaris 8
Root DSA Servers	2	Solaris 8
Transaction Log Servers	4	Solaris 8

Table 8: Mobilink HLS Server List

Server Room Servers:

Equipment Type	Quantity
CISCO 2800	15
CISCO 3600	7
CISCO 3700	8
CISCO CATALYST 3550	2
CISCO CATALYST 3560	1
CISCO CATALYST 3560G	2
CISCO CATALYST 2950	2
DELL PowerEdge 6000	1
DELL Tower CPU	2
HP 9000 rp 3440	1
HP DC 2700 Micro Tower	1
HP ML 570 G3	1
HP ML 570 G4	1
HP J5600	1
HP ML 350	1
HP ML 370	2
HP ML 370 G5	2
HP Workstation	1
HP XW4100	1
HP XW4300	1
Phoenix Tower	1
SF 280R	3
SF V210	1
SF V440	4
SF V490	6
SF V890	1
SUN Enterprise 3500	2
SUN Netra 440	2
SUN StorEdge 3500	4
SUN V880	3
Sunblade 150	6
Sunblade 2500	1
HP Compaq DC7100	6
Vanguard 6500	4

Table 9: Mobilink Server Room Server List

Mobilink OSS Expansion High Level Design

Tivoli Monitoring will be configured to forward events to the Objectserver when status and severity changes occur for a situation and when new situations occur. The EIF probe will installed and configured to forward events from ITM to the Objectserver. Tivoli Monitoring is also required for Open VMS platforms as well. Currently ITM agents do not support this platform.

11. Network Discovery

Mobilink require Network Discovery for the following networks

- Alcatel BSS Network Discovery
- Huawei BSS Network Discovery
- Motorola Network Discovery
- TXN Network Discovery
- Huawei T2000 Network Discovery
- SDH Network Discovery
- NEC Network Discovery
- Siemens MSC Network Discovery
- Huawei MSC Network Discovery
- NSN MSC Discovery
- Tekelec STP Discovery

A solution is currently being established for Network Discovery as devices are not snmp based and this is not a out-of-box functionality.

12. Data Loading

Currently the data is exported in csv format for Alcatel BSS. The device count information as well as the connectivity of BSC section and Cell section will need to be loaded within ccmdb. For each BSC information for BTS and BSC link data will also need to be loaded.

OPC and DPC information which is currently held in hexadecimal format needs to be uploaded into ccmdb after it has been converted to base 10 as this will allow Huawei BSC to Motorola MSC connections to be related to each other

Topology data is currently held in an Informix database. This data needs to be uploaded from the Informix database to the ccmdb.

Trail connectivity information is extracted in csv format from the EMS's. For T2000 there is a single file with topology data (NWCfg_LocalNM.txt). This file also contains

information that is not required such as single stream, customer and protect subnet. Other information like definitions for nodes and fibres will be uploaded

SDH Trails are currently extracted from a csv file and Sink and Source information give trail ends. This also needs to be uploaded into the ccmdb. Working routes will be kept external and used only for reference in Impact policies.

Only management network information is held within a Database server that uses MySQL. As no data relative to traffic running over the microwave network is held Mobilink need to compile tributary connectivity to store near end far end information for links between microwave NE's within the ccmdb. This can then be used for root cause analysis within impact.
TADDM needs SNMP based network for discovering devices, application and their relationship but Mobilink network is a Non-IP network and cannot be discovered by TADDM discovery process.

Mobilink have different vendor NMS system by which they can download devices and their relationship in CSV file format but the process of data fetching from NMS system are different for every vendor NMS but this is decided that Mobilink will provide all devices data and their relationship on CSV format.

To overcome this requirement, TADDM will configure with Discovery Library Adaptor, which provides an integration mechanism for communicating and sharing information about discovered resources and relationships within the Mobilink network.

The following sequence describes the DLA information flow for Mobilink:

- Mobilink NMS System has information for discovered resources and their relationships.
- That information would be deliver to CSV format
- DLA creates an IDML representation of the NMS application data (resources and relationships). The DLA can also request discovery updates, as required.
- DLA can use bulk load program to upload information to TADDM CMDB database.
- After uploading the DATA into CMDB then IBM Tivoli Integration Composer can populate data from TADDM to CCMDB database.

13.   User Administration

From the requirements gathering phase it has been understood that Active Directory authentication configuration is required. The default OMNIbus users will remain and additional users will authenticate via active directory.
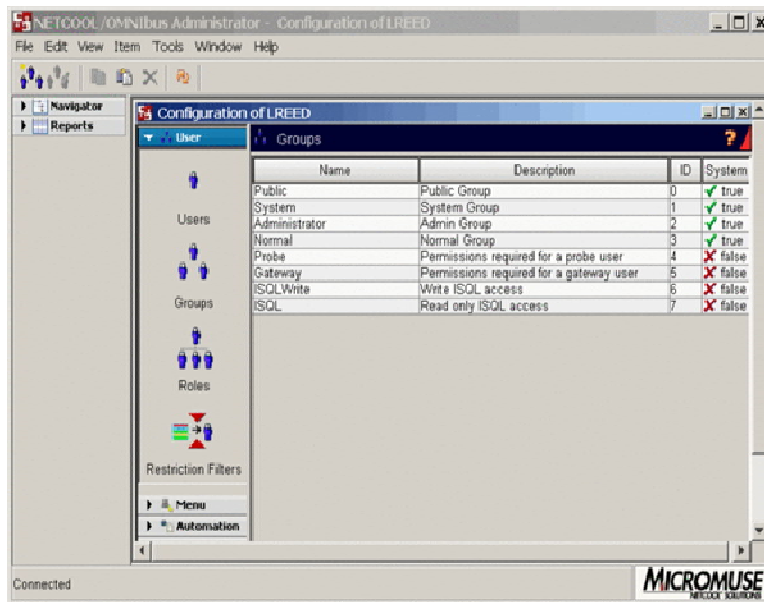
Figure 80: Netcool OMNIbus Users and Groups

14. System Start-up and Shutdown

Netcool/OMNIbus process control enables processes to be monitored and automatically restarted if they exit unexpectedly. Process control will be configured to manage the restart of components if they exit unexpectedly. Start-up scripts will be configured on all servers to ensure that all processes startup at system boot. The correct manual procedure to start-up and stop the processes will be provided within the handover documentation for all the products deployed.

Process Control can be managed by Administrators from the Administrator GUI as well as the configuration file located on the server.
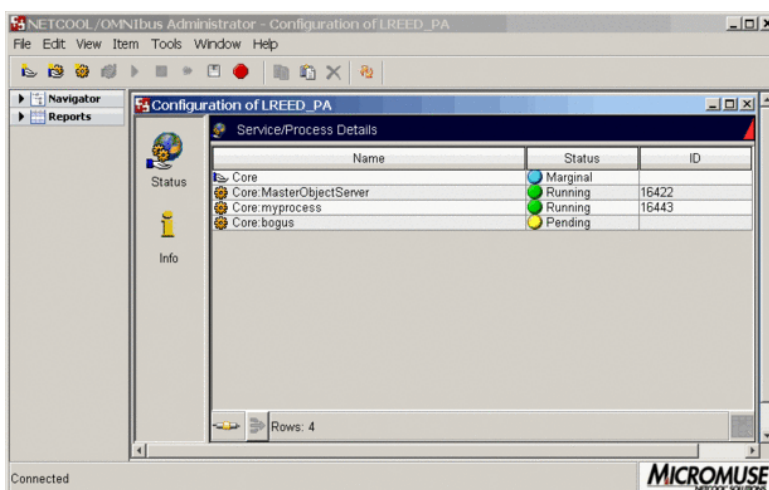

Figure 81: Netcool OMNIbus Process Control GUI

Mobilink OSS Expansion High Level Design

15.   Backup Policy

The purpose of this backup policy is designed to protect data within Mobilink‟s environment to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope

Pre-Go Live
The Operating System backups will be performed via SCRIPTS, and taken on an internal hard drive or DVD. This activity is a „one-off‟ and only needs to be performed at the beginning of the project. The back-ups of the O/S post-live will be performed on demand, as and when changes to the O/S are made i.e. when the O/S version is upgraded or Service Packs are installed.
Restoration of the O/S will be done via a USB drive that Innovise will provide.
As for the Applications and Meta Data (configuration data), Innovise ESM will perform backups via SCRIPTS. This will ensure project BASE-LINES are in place in the event of system failures, and restoration to a previous state (DATE STAMPED), are available.

Post Go Live
A full back up of practice data will be taken once a fortnight including: All clinical records and system audit trails, this includes all data held on the NOC area of the network. We expect some automation in backup with minimal manual intervention.
• Data to be backed up:
• Files stored in all Databases
• Table Spaces in all Databases
• Tickets, CI‟s, Assets, Alarms and Events

Note: Applications will only be backed up on demand: only after configuration changes, fix packs are uploaded or any other application changes are made.

Frequency and Timing of Backups

Pre Go-Live backups will be on-demand and falls under the responsibility of the Innovise Project Manager, to maintain. Post-Live backups will be performed every two weeks. If for maintenance reasons, backups are not performed on a scheduled day, they shall be done on the following day.

Restoration

Users that need files restored must submit a request to the Innovise ESM Support Desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Verification of Backup Status

A designated member of Mobilink staff must check the backup status on the system first thing each morning, and report any failures to the NOC administration Team.

Mobilink OSS Expansion High Level Design

House-keeping of the System Backup

Regular maintenance will be done by Innovise ESM, of the backup device to ensure it is kept in good working order. The ability to restore data from backups shall be tested once per month.

Managing Backup Failure

- In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:
- Note any messages / information on the server monitor.
- Contact the Innovise ESM Team to report the failure.
- Report the failure to the NOC Administration Team.
- Record the failure in the backup log and any actions taken as a result.
- If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out.

Archiving of Data

Archives are made at the end of every year in December. Data associated with Events data etc are archived every six months after they have left the organization.

Practice Software

Only the following member(s) of staff are authorized to load software onto any part of the practice network: [name of staff]. Any other member of staff found to be loading software without authorization may be subject to disciplinary procedures.