

**IBM Tivoli Netcool**

**Mobilink Impact Policies**

**Innovise ESM**

**Keypoint**

**High Street**

**Slough**

**SL1 1DY**

**Tel: +44 (0) 1753 513 800**

**Author: Chris Janes**

**Title: Mobilink Impact Policies**

**Version: 0.00**

Contents

[1. Document Control 5](#_Toc266189030)

[2. Introduction 6](#_Toc266189031)

[3. General Policies 6](#_Toc266189032)

[Standard Enrichment: Priority HIGH 6](#_Toc266189033)

[Maintenance Policies 7](#_Toc266189034)

[Incident Record Policies: Priority HIGH 7](#_Toc266189035)

[Synthetic Events: Priority HIGH 8](#_Toc266189036)

[Wait/Sleep Time: Priority HIGH 9](#_Toc266189037)

[4. Correlation Policies 11](#_Toc266189038)

[DRI out of service alarms: Priority HIGH 11](#_Toc266189039)

[BSS Environmental Alarms: Priority HIGH 12](#_Toc266189040)

[Site down Alarm - Cell Alarms: Priority Medium 12](#_Toc266189041)

[Site Down Alarm – Site Down: Priority HIGH 13](#_Toc266189042)

[Multiple BTS down alarms: Priority HIGH 13](#_Toc266189043)

[RSL/GSL/MSL alarms: Priority Low 13](#_Toc266189044)

[X25 failures caused by TxN problems: Priority Medium 14](#_Toc266189045)

[Cell performance related alarms 14](#_Toc266189046)

[RSL link disconnect alarms 14](#_Toc266189047)

[Lack of events detection for each OMC: Priority Medium 15](#_Toc266189048)

[TxN environmental Events: Priority HIGH 15](#_Toc266189049)

[TxN Input power low/high/abnormal: Priority MEDIUM 16](#_Toc266189050)

[TxN External Customer Alarms: Priority MEDIUM 16](#_Toc266189051)

[R-LOS Fibre break alarm: Priority HIGH 16](#_Toc266189052)

[APS Alarm: Priority Medium 17](#_Toc266189053)

[Cable break policy: Priority HIGH 17](#_Toc266189054)

[ETH\_LOS alarm: Priority Medium 18](#_Toc266189055)

[Microwave error alarm: Priority Low 18](#_Toc266189056)

[Microwave environmental alarm: Priority Medium 18](#_Toc266189057)

[Microwave Equipment power supply alarm: Priority Medium 19](#_Toc266189058)

[Cross domain GPRS alarm: Defer to Phase 2 19](#_Toc266189059)

[Cell GPRS failure alarm 20](#_Toc266189060)

[Core signaling down C7 alarm 20](#_Toc266189061)

[CORE Media outage alarm 20](#_Toc266189062)

[CORE hardware alarm 21](#_Toc266189063)

[CORE STP Linkset down alarm 21](#_Toc266189064)

[CORE STP card isolation alarm 21](#_Toc266189065)

[CORE STP DIU down alarm 21](#_Toc266189066)

[Communication alarm 22](#_Toc266189067)

[In node down alarm 22](#_Toc266189068)

[IN processing error alarm 22](#_Toc266189069)

[IN call gaping alarm 23](#_Toc266189070)

[QoS alarm 23](#_Toc266189071)

[Equipment alarm 23](#_Toc266189072)

[IN DPC alarm 23](#_Toc266189073)

[IN environmental alarm 24](#_Toc266189074)

[IN valista issue on IN alarm 24](#_Toc266189075)

[IN VOMS alarm 24](#_Toc266189076)

[SMSC Service impacting alarms 25](#_Toc266189077)

[SGSN hardware alarm: Defer to Phase 2 25](#_Toc266189078)

[SGSN multiple C7 link down: Defer to Phase 2 25](#_Toc266189079)

[APS impact correlation 26](#_Toc266189080)

[C7 signaling correlation and multi fails in city 26](#_Toc266189081)

[XBL down alarm 27](#_Toc266189082)

[DPC/multiple C7 link alarm 27](#_Toc266189083)

[Call Gapping alarm 27](#_Toc266189084)

[Critical hardware alarm 28](#_Toc266189085)

[IN node down alarm 28](#_Toc266189086)

[Valista issue alarm: Defered 28](#_Toc266189087)

[Critical Threshold crossed alarm 28](#_Toc266189088)

[Appendix 1 – Test Plans. 29](#_Toc266189089)

[Alarm suppression during maintenance windows 29](#_Toc266189090)

[Requirement: 29](#_Toc266189091)

[Policy(s) 29](#_Toc266189092)

[Test Event source: 29](#_Toc266189093)

[Test 1 – check basic operation of the maintenance policies 29](#_Toc266189094)

[Test 2 – check sequential maintenance windows 29](#_Toc266189095)

[Test 3 – Test use of tool to take event out of maintenance 30](#_Toc266189096)

[TxN Input Power Low/High/Abnormal 31](#_Toc266189097)

[Requirement: 31](#_Toc266189098)

[Policy(s) 31](#_Toc266189099)

[Test Event source: 31](#_Toc266189100)

[Test 1 – Check Basic operation 31](#_Toc266189101)

[Test 2 – Check that no TT is raised if the event is cleared within the 5 minute window 31](#_Toc266189102)

[Test 3 - check that multiple power events for a given Node only generate 1 TT 31](#_Toc266189103)

[Core Hardware 32](#_Toc266189104)

[Requirement: 32](#_Toc266189105)

[Policy(s) 32](#_Toc266189106)

[Test Event source: 32](#_Toc266189107)

[Test 1 – Test description 32](#_Toc266189108)

**List of Figures**

**No table of figures entries found.**

**List of** **Tables**

**No table of figures entries found.**

# Document Control

**Document Prepared By:**

The following Innovise Limited personnel have prepared this document:

**Name Title**

Chris Janes Consultant

**Document Reviewed By:**

The following Innovise personnel have reviewed this document:

**Name Title**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Document Revision History:**

The following versions have been distributed:

**Version Revised and Issued By:**

0.0 Chris Janes

**Number of Copies Submitted to Customer:** 1

**Number of Copies for Innovise Limited:** 1

**Agreed and approved on behalf of Customer**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Introduction

This document has been produced to Record the process of the development of the Impact Policies that are part of the Mobilink OSS. The aim of the document is to cover the all aspects of the development of the policies including a Schedule/Plan, Testing including Test Scripts, Data Loading and the Impact Policy Requirement Questions. The design requirements are help in the High Level Design Document

# General Policies

## Standard Enrichment: Priority HIGH

**StdEnrich**

**Event Details**

All Events not in maintenance when they are first put in service

**Data Loading**

**From CMDB**

Fields required for enrichment including

Domain

Region

ManCity

CovCity

Site

OMC

ManagedObject

NE Priority

**Questions**

Many of these policies require Enrichment of events from CMDB.

What fields are enriched?

Not clear you already mentioned some fields to be enriched, what else you need. All fields to be enriched are mentioned in Device Table shared by Sehrish with Mansoor

This is in cmdb and needs to be checked by Chris

What is the Key field from the event to the enrichment – NE?

Yes based on Site Code which is a 7 digit field you can find all other fields

Where is the information for this coming from?

From dataloading and some offline tables shared by Sehrish with Mansoor

## Maintenance Policies

**Maintanence**

**Event Details**

All Events when they are first inserted and events that have been in maintenance when they a brought into service

**Data Loading**

**From CMDB**

Parent Child

Maintenance Table

*KeyField – Unique ID for this row*

*Node - Node to be put into Maintenance*

*Reason - Reason to put Node into Maint*

*MaintStart - Start of this Maintenance Period*

*MaintEnd - End of Maintenance Period*

**Questions**

Is the Key for this NodeAlias(NE), Node (ManagedObject) or something else

What are the possible reasons for Maintenance?

**MaintainenceEnd**

**Event Details**

Events that are in maintenance as they reach the end of their maintenance window

**Data Loading**

None

**Questions**

## Incident Record Policies: Priority HIGH

**CreateTT**

This policy Creates a TT within TSRM when the MaximoStatus flag is set to 1,2 or 3

**Event Details**

**Data Loading**

None

**Questions**

**ParentTT**

This Policy updates the child event with TT details from the Parent Event. This is required as the TT Details are not available on creation of the parent (may take up to 30 seconds)

**Event Details**

Event that has Parent Event details but no TT associated with it

**Data Loading**

None

**Questions**

**UpdateTT**

**Event Details**

**Data Loading**

None

**Questions**

**ClearTT**

This policy closes a TT when MaximoStatus is set to 11

**Event Details**

Event where MaximoStatus set to 11

**Data Loading**

None

**Questions**

When an event with an associated TT clears should this Resolve/Clear the TT

Yes AS PER AGREEMENT THIS SHOULD Resolve the TT, and the operator would enter the reason and then close the TT. (More explain)

**ClearEventFromTT**

This Policy will set an event to clear when certain TT are closed within CMDB

**Event Details**

Details passed from the ticket (Incident Record Reference)

**Data Loading**

**Questions**

## Synthetic Events: Priority HIGH

**ClearSyntheticEvents**

This policy is to clear ‘Parent’ events when all of its children have been set to clear.

**Event Details**

Event set to clear (Severity = 0) and for whom a parent exists.

**Data Loading**

None

**Questions**

What clears the Synthetic Events?

In our understanding a synthetic event is produced in response to two three events, so that a single correlated TT is created for all of them rather than 2-3 separate TT’s. So the synthetic event should clear when all the underlying events resulting in that synthetic events clears.

## Wait/Sleep Time: Priority HIGH

**GetSleepTime**

This policy returns the Sleep/wait time for some events dependent upon Site Code.

**Event Details**

N/a.

**Data Loading**

None

**Questions**

We need to look up Sleep time in event table

Where is this table?

We would give you an offline table, having the site code for each site and its Level, then another table called time table, would have alarm text and time for each alarm for different levels, according to the time of the day ( Night/Morning). You can upload excel sheet into a DB table using script

What is the schema of the table?

‘Lookup’ Table

DEVICE\_TYPE

MANAGING\_CITY

COVERAGE\_CITY

IDENTIFIER\_NAME

DEVICE\_VENDOR

OUTSOURCE\_CONTRACTOR

LAT

LAG

CELL\_PRIORITY

COVERED\_AREA

Level

Where in this table is ManagedObject which is required so we can extract the site code from this?

‘Sleep Time’ Table

Level

Alarm Type

Timing

Day or Night

What is the Key field from the event?

The Sleep Time would depend on 7 digit site code of the Object on which Event is occurring. The site code can be obtained from the managed object name itself

Who is supplying this information?

We would tell you how to extract this information from Object name

How do we extract this information?

Is there a default value should we be unable to find the sleep time in the table

YES a default value will be used, and if we do not need to create a TT for a site we would indicate that by putting a negative value in Sleep Time.

What is the Default time?

# Correlation Policies

## DRI out of service alarms: Priority HIGH

**Event Details**

See Question Below

**Data Loading**

**From CMDB**

**DRI Density**

**Questions**

How can we identify DRI Out Of Service alarm events

We need to check DRI Density from CMDB,

Where will this data be?

The data would be in CMDB as you said after dataloading. How this data can be obtained from EMS is via simple scripts/output files/ direct connection to DB etc. (Being discussed with Mansoor ) already

What will its key field in the event be?

Combination of DRI Number, BTS Name, BSC Name and Cell name

Where is the information coming from including details of where to run the command and credentials?

This should be covered in detail in data loading.

How can we Check DRI Status?

By logging into the relevant EMS and issuing simple commands. Commands is already shared.

For.e.g

Establish a ssh session with Motorola OMC enter username/password, rlogin into the NE in question and issue command

state <site id> dri <dri id>

How can we reset a DRI?

By logging into the relevant EMS and issuing simple commands. Commands is already shared.

For.e.g

Establish a ssh session with Motorola OMC enter username/password, rlogin into the NE in question and issue command

reset\_device <site id> dri <dri id>

After resetting DRI(s) how long should we wait before checking DRI Status?

5 Mins

How can Lock/Unlock a DRI

By logging into the relevant EMS and issuing simple commands. Commands is already shared.

For.e.g

Establish a ssh session with Motorola OMC enter username/password, rlogin into the NE in question and issue command

lock <site id> dri <dri id>

unlock <site id> dri <dri id>

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## BSS Environmental Alarms: Priority HIGH

**Event Details**

See Question Below

**Data Loading**

**From CMDB**

Site Type

Site Priority

Area

Address

SleepTime

**Questions**

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

Please list the subsets of alarms

Please define the required severity for alarms for each site type/ site priority

## Site down Alarm - Cell Alarms: Priority Medium

**Event Details**

See Question below

**Data Loading**

**From CMDB**

Number of cells at Site

**Questions**

How can we identify Site down Alarm - Cell Alarms events

How would we know if all cells are down?

For Motorola and Huawei you get a specific alarm indicating all cells are down, string is already shared.

For Alcatel you need to count the number of cells on which this alarm comes and compare it with total no of cells for that BTS from CCMDB

When a partial site down goes to a full site down should we generate an additional event or Update the existing Partial Event down to be a Full Site down Event

Update the existing one, and follow the same path while events clear that is degrade from full to partial site down if some events clear

If we have to generate a additional Full site down event what should we do with the Partial Site down

Update the existing one

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## Site Down Alarm – Site Down: Priority HIGH

**Event Details**

Motorola - “Last RSL Link Failure”

Alcatel - “LOSS\_OF\_ALL\_CHAN” alarm from each of the cells at a site.

Huawei - “LAPD OML Fault” alarm

**Data Loading**

**Questions**

Where in the event will we find the text supplied to identify the events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## Multiple BTS down alarms: Priority HIGH

**Event Details**

See Question below

**Data Loading**

**From CMDB**

Connectivity Information

**Questions**

How can we identify BTS down alarm events?

We need to look up wait time in event table

See ‘Wait/Sleep Time’ Policy

## RSL/GSL/MSL alarms: Priority Low

**Event Details**

See Question below

**Data Loading**

**Questions**

How do we identify RSL, GSL and MSL alarm events?

What command do we need to issue to Motorola EMS to gather number of associated links and how do we issue this onto the EMS

Already shared

How do we know if all the links on a GPROC are down?

From Commands you will get info of all links running on a GPROC and alarms on all of them means all links on GPROC are down.

If this goes to the state of this goes from some links down to all links down what should we do?

Update the same TT to all links down or GRPOC is down

## X25 failures caused by TxN problems: Priority Medium

**Event Details**

Motorola

See Question below

Alcatel

See Question below

**Data Loading**

Cross-connect info from a Mobilink external DB

**Questions**

How can we identify a X.25 Circuit Down alarm event from Motorola Equipment?

How can we identify a BSC unreachable alarm event from Alcatel Equipment?

How can we tell that all OMLs down for a given BSC

From the alarm string which is already shared for all vendors

## Cell performance related alarms

**Event Details**

Motorola

No calls on cell

CSR below threshold

Alcatel

Zero Calls on Cell

Zero terminating calls

Huawei

Cell long time no access

**Data Loading**

**Questions**

Where in the event will we find the text supplied to identify the Motorola events?

Where in the event will we find the text supplied to identify the Alcatel events?

Where in the event will we find the text supplied to identify the Huawei events?

We need to look up Wait time in event table

See ‘Wait/Sleep Time’ Policy

If the alarms are coming in from the same BSC, this should also be mentioned in the TT. Does this mean that we should count the number of these alerts and that we should mention it in the TT if it is greater than a threshold? If so what should this threshold be?

Timing fixed to 5 Minutes for X25 failures

## RSL link disconnect alarms

**Event Details**

See Question below

**Data Loading**

**From CMDB**

Site data

**Questions**

How can we identify RSL link disconnect alarm events?

**Please note that RSL link is specific for Motorola , for Alcatel you will get a BTS Audit O&M alarm when a slave DCS cabinet goes down you need to treat that alarm with the same policy, for Huawei also you will get an alarm whose string would be shared and it needs to be treated in same policy**

## Lack of events detection for each OMC: Priority Medium

**Event Details**

Event for a given OMC can be identified by the OmcEms field in the event

**Data Loading**

**Questions**

Please list all OMC’s to be checked

All BSS OMCR’s need to be checked, details of all EMS to be monitored is already shared.

Please List the wait time associated with each OMC

5 Mins-2 Hours depending on the OMC in question

Please can you give us this information?

Is the period between checks the same for all OMC’s?

YES

What should this period be?

Continuous Check, if no event is received from any OMC for 3 minutes an alarm should be generated. For some OMC you might get a clear alarm showing OMC disconnection

## TxN environmental Events: Priority HIGH

**Event Details**

See Question below

**Data Loading**

**From CMDB**

Site information

Site co-ordinates

**Questions**

How can we identify TxN environmental alarm events

Just to clarify, these events ‘share’ the same parent events as the BSC Power Events

The events are different from BSC Power events, so treat them differently. Only thing you need to do is if a TXN Node is co-located with a BSS Node and both have environmental alarms 1 TT should be created and both alarms associated to them.

What Co-ordinate information should be enriched into this?

No co-ordinate information is needed from name of TXN Node you can deduce the name of the co-located BSS equipment

## TxN Input power low/high/abnormal: Priority MEDIUM

**Event Details**

See Question below

**Data Loading**

**Questions**

How can we identify TxN Power alarm events (abnormal/High/low)?

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## TxN External Customer Alarms: Priority MEDIUM

**Event Details**

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

**Data Loading**

**From CMDB**

Customer

**Questions**

Where in the event can we find the text supplied to identify the events?

How do we associate given alarms to given external Customers

The ports have been labeled as “Ext”, so their relevant trails and alarms will have this tag with them.(association criteria was already shared with Giles)

## R-LOS Fibre break alarm: Priority HIGH

**Event Details**

See Questions below

**Data Loading**

From CMDB

Details of the NEs and DWDM elements positions on the fibre rings

( coordinates will be provided with in a day or so)

Wait Time

**Questions**

How do we identify ‘RLOS’ events?

How do we identify ‘ASP-IND’ events?

We need to look up Wait time in event table

See ‘Wait/Sleep Time’ Policy

We can have wait time as 2miutes.

## APS Alarm: Priority Medium

**Event Details**

See Questions below

**Data Loading**

**From CMDB**

List of potential traffic that may have lost redundancy

**Questions**

How do we identify APS events?

We check ‘list of potential traffic that has lost redundancy’

Where is this list held?

(this data will be taken out from script files of network…already explained to Giles)

How do we check for lost redundancy?

(The traffic that is being passed through the lines card(which are in break state) has actually lost redundancy. Already explained to Giles)

## Cable break policy: Priority HIGH

**Event Details**

See Questions below

**Data Loading**

**Questions**

How do we identify an ETH\_LOS event?

How will an event be marked as requiring Processing through this policy?

(If it is under LDI or DWDM subnet, then this criteria is applicable. Already explained to Giles)

How can we determine the ends of the break?

(By the alarms being reported. Already explained to Giles)

Where will the information for the internal impact table to locate the location of the break be coming from and when?

By knowing the coordinates and then finding minimum distance, the alago was developed by Giles)

The Algorithm requires the data to work – the question was when will this data be supplied?

## ETH\_LOS alarm: Priority Medium

**Event Details**

See question below

**Data Loading**

Lost traffic

Domain

Region

Lost connectivity

**Questions**

How can we identify an ‘ETH\_LOS’ event?

How do we know what traffic is being carried on the alerting Ethernet

From data base.

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## Microwave error alarm: Priority Low

**Event Details**

BER High Alarm

Enterprise ‘pasolinkNeoStd’

Specific Trap ‘308’

BER Low Alarm

Enterprise ‘pasolinkNeoStd’

Specific Trap ‘309’

Unavailable seconds

See Questions below

Rx level Alarm

See Questions below

**Data Loading**

Effected channels

Capacity of Trunk

Type of Trunk

**Questions**

How can we identify ‘Unavailable seconds’ events

How can we identify ‘Rx level Alarm’ events

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## Microwave environmental alarm: Priority Medium

**Event Details**

See Questions below

**Data Loading**

**From CMDB**

Site Type

Site Priority

SleepTime

**Questions**

How can we identify Microwave Environmental alarms events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

Sleep time was decided to be 10 minutes

Please define the required severity for alarms for each site type/ site priority

## Microwave Equipment power supply alarm: Priority Medium

**Event Details**

See Questions below

**Data Loading**

**Questions**

How can we identify Microwave Power supply alarms events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

Sleep time was decided to be 5minute

## Cross domain GPRS alarm: Defer to Phase 2

**Event Details**

Loss Of Contact With GPU

Ater Down

PVC DLCI is inactive

PVC DLCOI is unknown from the network

PCU Down

NSVC Dead

NO PRP/GPS

Rx Level alarm

NSE Faulty

NSVC Faulty

NSCL Dynamic Configuration Process Failure

NSVL Faulty

Traps not yet active from EMS

Loss Of Signal

Rcv AIS

Loss Of Frame

RAI

**Data Loading**

**From CMDB**

GPRS

BSC Name

BSC Rack

BSC Shelf

DLCI

**Questions**

How do we identify these events

## Cell GPRS failure alarm

**Event Details**

Alcatel

Loss of Packer Service

Motorola

No PCDH available

GPRS Unavailable

Huawei

Cell PS Service Faulty

SGSN

NSE Degraded at least one non signalling BVC in fault

**Data Loading**

**Questions**

How can we identify the required events

## Core signaling down C7 alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How do we identify CORE Signalling down C7 Alarm events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

How do we find out the Alt end of the link?

Where do we find

SLC numbers

A&Z Nodes

Percentage of effected links

## CORE Media outage alarm

**Event Details**

See questions below

**Data Loading**

**Questions**

How do we identify DIU alarms, which are related to media outages,

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

How do we find ‘Signal Percentage Down’?

## CORE hardware alarm

**Event Details**

See questions below

**Data Loading**

**From CMDB**

Site Type

Site Priority

**Questions**

How do we identify Core Hardware Alarms?

Please define the required severity for alarms for each site type/ site priority

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## CORE STP Linkset down alarm

**Event Details**

See question below

**Data Loading**

Linkset information

**Questions**

How do we identify Core STP Linkset Alarms?

How do we find ‘Percentage of effected links’?

How do we know if it’s a high speed link?

What Priority should the event have when it is a HSL

What Priority should the event have when it is not a HSL

## CORE STP card isolation alarm

**Event Details**

See Question below

**Data Loading**

Linkset information

**Questions**

How do we identify Core card isolation Alarms?

## CORE STP DIU down alarm

**Event Details**

See Question below

**Data Loading**

Far end MSC equipment

**Questions**

Where do we lookup MSC Equip?

When will we be issued with this spreadsheet?

How will this table be maintained?

## Communication alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How do we identify Core STP DPC Down Alarm events?

Where do we find Point code?

How can we identify the BSC associated with these alarms

## In node down alarm

**Event Details**

**Data Loading**

**Questions**

How do we identify an ‘In node down alarm’ event?

How do we identify the ‘Pair’ to this event?

What events should be associated with the Node Down event as child events?

How do we identify associated DPC Down alarms?

## IN processing error alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How do we identify IN processing error alarms?

TT should be generated within 10 – 15 minutes after alarm – We will raise the TT after 10 minutes

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## IN call gaping alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How do we identify IN Call gapping alarms?

Alarm should generate a TT within 3-5 minutes – We will raise a TT after 3 minutes

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## QoS alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How do we identify IN Critical Threshold Crossed alarms?

Does the Agent only send an event in when there is a problem?

If this is the case are there resolution events?

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## Equipment alarm

**Event Details**

See questions below

**Data Loading**

**Questions**

How can we identify IN Critical Hardware Alarm Events?

How can we further identify DIMM related Events?

IS it all these events that need to be cleared when the associated TT is cleared or just the DIMM related events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## IN DPC alarm

**Event Details**

See questions below

**Data Loading**

SLC Numbers

A & Z Node Names

**Questions**

How do we identify IN DPC alarm events?

How do we know the total number of links in the linkset?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

How do we find out the Alt end of the link?

Where do we find

SLC numbers

A&Z Nodes

Percentage of effected links

## IN environmental alarm

**Event Details**

See questions below

**Data Loading**

Wait time

**Questions**

How do we identify IN environmental alarm events?

How do we further identify “Mopnet Connection Lost” and “MopnetConnection restored” alarm events?

Does a “MopnetConnection restored” event resolve a “Mopnet Connection Lost” event?

Is the time allowed for a Mopnet event to be resolved the same as the wait times for the other IN environmental events?

We need to look up Wait time in event table

See ‘Wait/Sleep Time’ Policy

## IN valista issue on IN alarm

**Event Details**

See questions below

**Data Loading**

**Questions**

How can we identify IN Valista Issue on IN alarm events?

We are required to check for historical events for last ‘x’ minutes –

What is ‘x’?

We are required to generate a synthetic event if a threshold is breached,

What is this threshold?

How can we tell if it’s a >100 mill, >200 mill or >300 mill event?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## IN VOMS alarm

**Event Details**

See questions below

**Data Loading**

**Questions**

How can we identify IN VOMS alarm events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## SMSC Service impacting alarms

**Event Details**

Restarting Entity

Class = 100007

See questions below

Entity is in Blocked State

Class = 100007

See questions below

Entity Not Responding

Class = 100007

See questions below

**Data Loading**

**Questions**

Where in the event will we find the Text supplied to identify the event?

How can we further identify ‘Node Down’ events?

How can we find the Parent DPC for these events?

How can we find the associates STP for these events?

Where can we find the point code for these events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## SGSN hardware alarm: Defer to Phase 2

**Event Details**

See question below

**Data Loading**

**Questions**

How can we identify SGSN hardware events?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

## SGSN multiple C7 link down: Defer to Phase 2

**Event Details**

Alcatel

BSC GPRS service lost

BSS BVCSig of this GPU is broken

BSS GSL is broken

LapDLink is broken

Loss of contact with GPU

No reply from SGSN

PVC DLCI is inactive

PVC DLCI is unknown from the network

Motorola

Last GBL Failed

Last GSL Failed

Last TRAU GDS Failed

Last PCU Failed

NSVC Failure

**Data Loading**

LinkSet

No Links in Linkset

SLCNumbers

A&Z Nodes

**Questions**

How do we identify SGSN Multiple C7 Link Down alarm events?

Where in the event will we find the Text supplied to identify the event?

We need to look up Sleep time in event table

See ‘Wait/Sleep Time’ Policy

How do we find out the Alt end of the link?

Where do we find

SLC numbers

A&Z Nodes

Percentage of effected links

## APS impact correlation

**Event Details**

**Data Loading**

**Questions**

How can we identify APS events?

Topology Table

Where is it?

What is its schema?

What is the key field from the event?

What field should be enriched?

How do we know which trails are associated with which customer?

How can we find if the trail is a sink or source of the trail of if the trail is in a positive path?

## C7 signaling correlation and multi fails in city

**Event Details**

See questions below

**Data Loading**

**Questions**

How do we identify C7 signalling alarm events?

How is the City/Area to be defined for these events?

## XBL down alarm

**Event Details**

See questions below

**Data Loading**

**Questions**

How can we identify XBL down alarm events?

How do we issue the ‘disp\_eq 0 xbl <xbl\_id>’ and ‘disp\_mms 0 <mms\_id>’ Commands?

Against what?

Do we need any connectivity details?

How can we find out if a C7 link exists

How can the corresponding RXCDR be found?

## DPC/multiple C7 link alarm

**Event Details**

See questions below

**Data Loading**

Linkset

Number of links in a linkset

**Questions**

How can we identify DPC/ Multiple C7 Links Alarm Handling Events?

How is this correlated to a STP Domain?

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## Call Gapping alarm

**Event Details**

‘Inp TlmProcGroup\_513:Limit ID01340G2081CccGL\_GlobalLimit has reached 100% of effective limitation’ See questions below

Severity = Major

**Data Loading**

**Questions**

Where will this event originate from?

Where in the event will the text string given be found?

Other Events have differing wait period for Day/Night, should this event? If so what should the timings be?

## Critical hardware alarm

**Event Details**

See question below

**Data Loading**

**Questions**

How can we identify the critical hardware alarms?

Other Events have differing ait period for Day/Night, should this event? If so what should the timings be?

## IN node down alarm

**Event Details**

See question below

**Data Loading**

**Questions**

Are the strings give to Identify these events exact strings or are there elements in them that may vary? If so please define which parts of the string will not change.

What will the source of these’s events be?

## Valista issue alarm: Defered

**Event Details**

See question below

**Data Loading**

**Questions**

How can we identify a ‘PayWorkerProc\_260’ event’?

## Critical Threshold crossed alarm

**Event Details**

See question below

Other Events have differing ait period for Day/Night, should this event? If so what should the timings be?

**Data Loading**

**Questions**

How can we identify these events?

Other Events have differing ait period for Day/Night, should this event? If so what should the timings be?

# Appendix 1 – Test Plans.

## Alarm suppression during maintenance windows

### Requirement:

The requirement requires that all new events are checked against a table held in CMDB. If it or its parent is found to be in a maintenance period then the event should be flagged to show that it is in Maintenance, the reason for this and the time that this maintenance period ends

Tool is required to insert emergency change windows into CMDB

Tool to take the event out of its maintenance period early

### Policy(s)

Maintenance

This policy checks all new Events and if the Node or the parent Node are within a maintenance window sets the OS field MaintFlag to show the reason and OS field MaintEnd to show the end of the maintenance window. If the Event is not in a maintenance window then MaintFlag is set to 1, allowing further policies to run against this event

Maintenance End

This policy runs every 15 seconds checking events that have MaintFlag set to show that it is in a maintenance window and checks if it is has reached the end of the maintenance window. If it has reached the end of the maintenance window it resets the MaintFlag to 0 causing it to be checked again by the Maintenance Policy in case there are any further maintenance windows affecting this event.

### Test Event source:

Any Event can be used to check these policies

### Test 1 – check basic operation of the maintenance policies

1. Enter an record into the maintenance table for the Node of the test event for a 5 minute period
2. Insert the test event
3. Using an AEL that shows suppressed events see the event arrives and that it is placed in maintenance, checking the correct value is displayed for MaintFlag and that the end of the maintenance window appears in MaintEnd
4. After 5 minutes check that the event comes out of maintenance (MaintFlag = 1) and that any further required policies run

### Test 2 – check sequential maintenance windows

1. Enter a record into the maintenance table for the Node of the test event for a 5 minute period
2. Enter a record into the maintenance table for the Node of the test event for a 5 minute period that starts just before the first window ends.
3. Insert a test event
4. Check the correct values are displayed for MaintFlag and MaintEnd(End of first maintenance window)
5. After 5 minutes check that the correct values are displayed for MaintFlag and MaintEnd(End of second maintenance window)
6. After a further 5 minutes check that the event comes out of maintenance (MaintFlag = 1) and that any further required policies run

### Test 3 – Test use of tool to take event out of maintenance

1. Enter an record into the maintenance table for the Node of the test event for a 5 minute period
2. Insert the test event
3. Check the correct values are displayed for MaintFlag and MaintEnd
4. Right Click the event and select the end maintenance tool
5. Check that the event comes out of maintenance (MaintFlag = 2) and that any further required policies run

## TxN Input Power Low/High/Abnormal

### Requirement:

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.

### Policy(s)

TxnInputPower

This policy checks all TxN power events. If the event has not cleared after 5 minutes generates a new TT if there isn’t already one raised for a TxN power event from the same node. If there is a TT for a TxN power event it will use the same TT

### Test Event source:

TxN Power High Event

TxN Power Abnormal event

Note: if these events cannot be generated by ML then it may be necessary to use synthetic events. If this is the case the ML should certify that the synthetic events are suitable for this testing

### Test 1 – Check Basic operation

1. Insert TxN Power High Event
2. Check Event appears in a suitable AEL
3. After 5 minutes check that a TT is raise

Following this test clear the alert and it’s associated TT

### Test 2 – Check that no TT is raised if the event is cleared within the 5 minute window

1. Insert TxN Power High Event
2. Check Event appears in a suitable AEL
3. Clear the Event
4. After 5 minutes check that no TT has been raised

### Test 3 - check that multiple power events for a given Node only generate 1 TT

1. Insert TxN Power Abnormal Event
2. Check Event appears in a suitable AEL
3. After 5 minutes check that a TT is raised – make a note of its reference
4. Insert TxN Power High Event
5. Check Event appears in a suitable AEL
6. Check the event has the same TT reference as the TxN Power Abnormal Event
7. Check the TT has been updated to show the additional event

## Core Hardware

### Requirement:

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.

### Policy(s)

CoreHardware

This policy initially identifies the sub group of core hardware alerting before enriching the event. I then checks to see if there is an existing TT for that sub group, if there is it, it update the TT.

If event has not cleared after a delay then a synthetic event with an associated TT is raised with details of the parent event and of the TT being put in the child events

CoreHardwareClear

This policy checks any Core Hardware events when they are set to clear. If they are last child event of a sub group it sets the parent event to clear

### Test Event source:

### Test 1 – Test description