

Handling Alarms

DESCRIPTION

Copyright

© Ericsson AB 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Understanding Fault Management	1
1.1	Key Fault Management Concepts	1
1.2	Resolving a Fault Reported by an Alarm	1
1.3	Active Alarm List	2
1.4	Alarm and Alert History	2
1.5	Alarm Information	2
1.6	Meaning of Alarm Severity	3
2	Basic Fault Management Procedures	4
3	Advanced Fault Management Concepts	5
3.1	SNMP Target	5
4	Advanced Fault Management Procedures	5





1 Understanding Fault Management

1.1 Key Fault Management Concepts

- Fault Management encompasses fault handling and alarm handling.
- A fault is the inability of a system resource to behave as expected, for example a function in the system cannot be executed.
- Fault handling is the capability of the system to detect, perform automated recovery attempts, and report a system fault. When automated recovery attempts do not solve the fault, the fault is reported as an alarm.
- Alarm handling is the capability of the system to expose an accurate alarm status and alarm history supporting an efficient alarm resolution flow.

The `Fm` and `Snmp` Managed Objects Classes (MOCs) can be found in the Managed Object Model (MOM). For general information about the Managed Objects, cardinality, and related concepts, refer to [Managed Object Model User Guide](#).

1.2 Resolving a Fault Reported by an Alarm

The alarm resolution workflow consists of the following main steps:

- 1 Once an alarm is noticed, the user identifies it based on its Specific Problem and Source.
- 2 The user acknowledges it to indicate to other users that the problem is being worked on. This functionality can be provided by Ericsson management systems and is not further described here.
- 3 The user finds the corresponding alarm Operating Instructions (OPIs) document, for example, by performing a search in the Active Library Explorer library. Each alarm has an alarm OPI document titled as the Specific Problem. The actual lookup of alarm OPIs can be provided by Ericsson management systems and is not further described here.
- 4 To solve the problem, the alarm OPI document is to be used as follows by the user:
 - a Study the possible alarm causes, fault reasons, fault locations, and the potential service impact.
 - b Analyze the alarm information. The alarm information is visible over NETCONF and the Ericsson Command-Line Interface (ECLI).
 - c Execute the procedure to eliminate the problem and eventually clear the alarm.

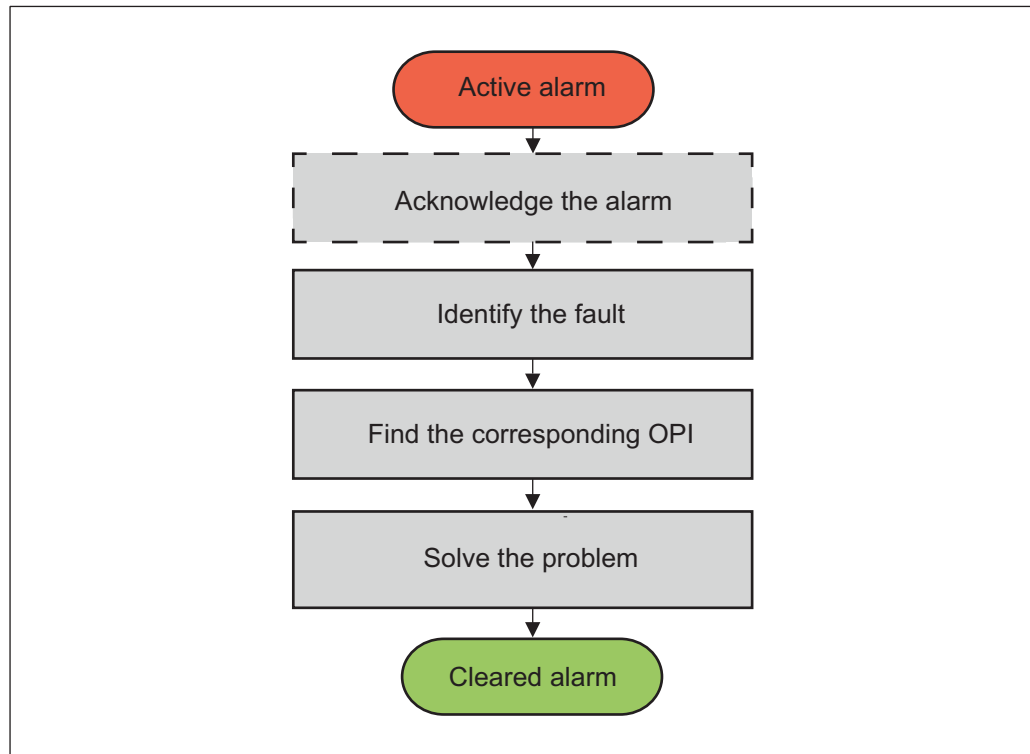


Figure 1 Problem Resolution Workflow

1.3 Active Alarm List

The Active Alarm List defines the overall alarm status of the system. It consists of all the alarms currently active that is in raised state. The overall system alarm status is qualified by the severity of the active alarms and the number of alarms. The more severe the active alarms are, the more urgent it is to resolve the underlying faults.

1.4 Alarm and Alert History

All alarm state changes including cleared states are recorded in the Alarm Log. All alerts are recorded in the Alert Log.

1.5 Alarm Information

An alarm includes information usable for identification and cause analysis.



Table 1 Description of Alarm Information

Alarm Information	Description
Major Type	The combination of Major Type and Minor Type, which are two numbers, identifies an Alarm Type, which is an alarm category, within the ME. The Alarm Type is the same in different versions of the ME.
Minor Type	
Source	The Distinguished Name (DN) of the alarming object. Managed Object (MO) Instance is applicable only to alarms belonging to a managed area, else Source is used.
Specific Problem	Provides further refinement to the information given by Probable Cause and is unique within the ME. Specific Problem is the same in different versions of the ME. The alarm OPI document title exactly matches its value.
Event Type	The general category for the alarm. The values are defined by ITU-T X.733 and X.736 according to RFC 3877.
Probable Cause	Qualifies and provides further information on the reason for the alarm. The values are defined by ITU-T X.733, X.736, M.3100, and GSM 1211 and are included in ERICSSON-ALARM-PC-MIB.
Additional Text	Provides extra textual information. Normally runtime-related information.
Perceived Severity	Provides guidance on the severity of the problem, that is, possible service impact and urgency to act. The value can be changed owing to deployment scenarios or the operation situation. Perceived Severity is to be interpreted according to the Ericsson definition of the 3GPP Perceived Severity values.
Event Time	The time when the alarm was updated, that is, the time for the latest alarm information change or severity change.

1.6 Meaning of Alarm Severity

Table 2 Ericsson Definition of 3GPP Perceived Severity Values

Severity Level	Description
Cleared (1)	Used to clear a previously reported alarm.
Indeterminate (2)	Not used.
Critical (3)	Indicates that a condition that affects service has occurred and an immediate corrective action is required. Such a severity can be reported, for example, when an MO becomes out of service and its capability must be restored. This severity requires an immediate action, even outside working hours.



Table 2 Ericsson Definition of 3GPP Perceived Severity Values

Severity Level	Description
Major (4)	Indicates that a condition that affects service has occurred and an urgent corrective action is required. Such a severity can be reported, for example, when a service degrades in the MO capacity and its full capability must be restored. This severity requires an immediate action within working hours.
Minor (5)	Indicates that a fault condition that does not affect service has occurred. A corrective action is required to prevent a more serious fault such as a service-affecting fault. Such a severity can be reported when the detected alarm condition does not currently degrade the MO capacity. This severity requires an action at a suitable time, or at least that a close observation of the situation continues.
Warning (6)	Indicates that a potential or impending fault affects service, before any significant effects have appeared. Corrective action is based on a scheduled maintenance basis.

2 Basic Fault Management Procedures

— Check Alarm Status

- The alarm status is checked to assess the number, the severity, and the nature of the active alarms, as part of preventive maintenance or problem resolution activities.
- The alarm history is checked to get a chronological list of the recorded alarm state changes up to current time.
- The alert history is checked to get a chronological list of the recorded alerts up to current time.

For further details, refer to [Check Alarm Status](#).



3 Advanced Fault Management Concepts

3.1 SNMP Target

An SNMP Target defines information about where and how to send an SNMP Notification. This consists of destination information and SNMP parameters.

4 Advanced Fault Management Procedures

— Change Alarm Type Severity

The user can experience that an alarm default severity does not properly reflect the actual severity of the problem. For example, an alarm with severity Major is instead to have severity Minor. The user can configure an alternative severity in the Alarm Type to supersede the default severity. For further details, refer to [Change Alarm Type Severity](#).

— Change Heartbeat Interval

The default heartbeat interval for the push mechanism is 60 seconds. The user can change the value to zero to disable the push heartbeat mechanism during maintenance operations. The user can change the heartbeat value to a smaller or higher value according to the organization monitoring policy. For further details, refer to [Change Heartbeat Interval](#)

— Create SNMP targets

SNMP targets contain the necessary information to report SNMP notifications to the corresponding management systems.

Create SNMPv1, SNMPv2C, and SNMPv3 targets are supported.

They can then be Deleted, Disabled, or Enabled.

For SNMPv2C and SNMPv3 targets, either an unacknowledged SNMP message mechanism (TRAP) or an acknowledged SNMP message mechanism (INFORM) can be chosen. For SNMPv3 targets, the User-based Security Model (USM) related authentication and privacy mechanisms can be configured. SNMPv1 and SNMPv2C targets support only configuration of community as the authentication mechanism.

— Configure SNMP Master Agent



The SNMP Master Agent can be configured with engineId attribute. For further details, refer to [Configure SNMP Master Agent with engineId](#).