

# Fault Codes

FAULT TRACING DIRECTIONS



## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2020, Mitel Networks Corporation

All rights reserved

# 1 DOMAIN 0 - MX-ONE COMPATIBLE ALARMS

## 1.1 FAULT CODE 10 - CONTROL SYSTEM DISTURBANCE COUNTER AT TOP

### 1.1.1 DESCRIPTION

Some, less serious, faults which occur in the control system are not serious enough for the alarm log to be informed immediately. On the other hand, the program execution could be seriously disturbed, if a large number of such less serious faults would occur within a certain time. The errors are logged in the LIM internal history log. Some of these errors might be repairable via a LIM restart, in this case the LIM disturbance counter is incremented.

The disturbance counter is incremented a different number of steps depending on how serious the fault is considered to be. The disturbance counter is decremented periodically. It is indicating zero if no faults have occurred.

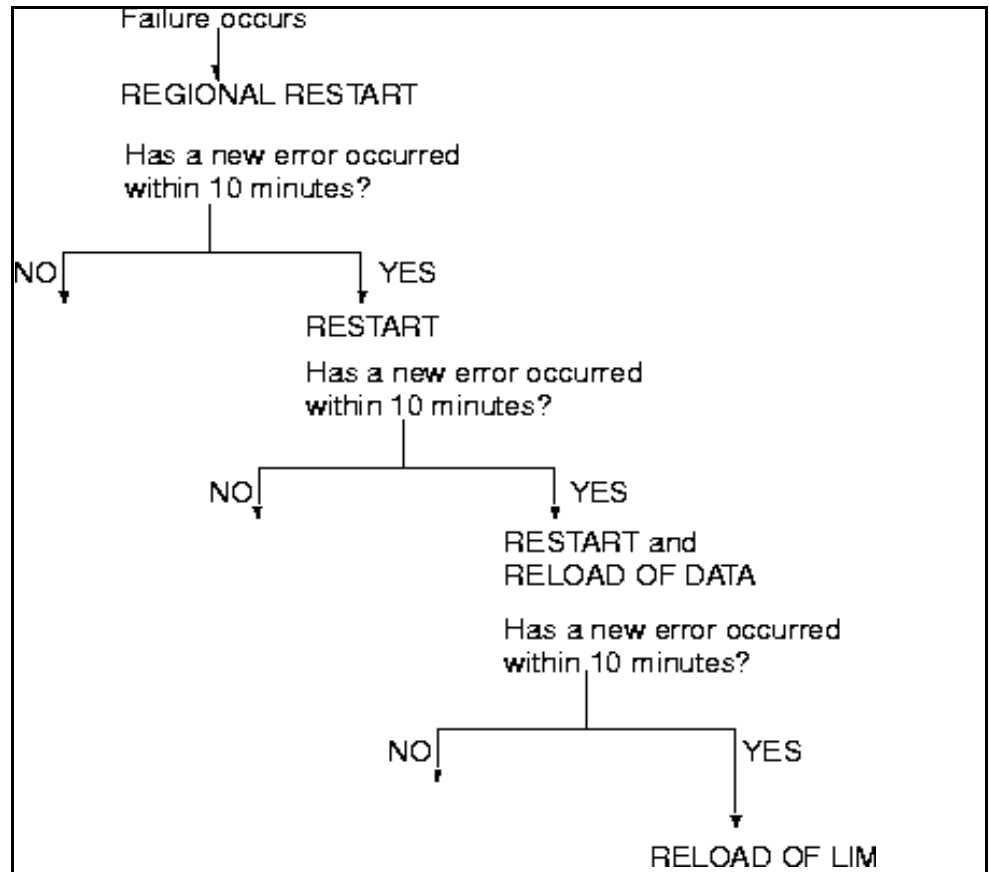
The alarm log is informed if the disturbance counter would reach its top level, i.e. a predefined max value.

If the disturbance counter reaches the top measures are taken via the Action Chart.

### 1.1.2 ACTION CHART

A process of decision and measures which decides the suitable measure for recovery when a fault occurs at a given system situation.

The LIM is supervised in a way which makes measures to be escalated if a new error occurs within 10 minutes.



## 1.1.3

## MEASURE

1. Has any alarm concerning reload/restart in the current LIM arrived at the alarm log?
2. Read out the information about the error by means of command *trace -print 0*. Save the information.
3. Key in the command *trace -clear 0* to acknowledge the information.

## 1.2

## FAULT CODE 11 - DEVICE BOARD IN WRONG POSITION

## 1.2.1

## DESCRIPTION OF FAULT CODE

Most of the approximately 30 device boards positions of a classic LIM can be used for all types of boards requiring up to 32 time slots.

If a device board is placed in a position where not all individuals can be reached, the board will be marked passive and the alarm log will be informed.

## 1.2.2

## MEASURES

1. Compare the indicated board position with the LIM configuration. Use the command *board\_list*.

2. Is the board in the wrong position?
3. NO: Consult an expert.
4. YES: Place the board in the correct position. With reference to device boards need of time slots.

## 1.3 FAULT CODE 12 - NO CONNECTION WITH DEVICE BOARDS IN ONE MAGAZINE

### 1.3.1 DESCRIPTION OF FAULT CODE

The device boards are regularly checked.

If no answer from any device board at all on multiple numbers:

- 0 - 255 it is assumed that DSU0 is faulty
- 256 - 511 it is assumed that DSU1 is faulty
- 512 - 767 it is assumed that DSU2 is faulty
- 768 - 1023 it is assumed that DSU3 is faulty.

#### ADD INFO 1

States the faulty magazine (DSU).

### 1.3.2 MEASURE

1. Check that the connected board edge cables are placed correctly.
2. Use the command *ls\_config\_test* to order a functional test of the DSU.
3. Is DSU board faulty?
4. NO: Use the command *restart -lim* to restart the Server.  
See operational directions for *ADMINISTRATOR USER'S GUIDE*.
5. YES: Replace the faulty DSU board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

## 1.4 FAULT CODE 13 - NO CONNECTION WITH DEVICE BOARDS IN LIM

### 1.4.1 DESCRIPTION OF FAULT CODE

The physical or virtual device boards are regularly checked.

If no physical or virtual device board at all answers during such a check, an alarm will be issued for faulty Media Gateway (faulty LIM).

### 1.4.2 MEASURES

1. Check that the connected board edge cables are placed correctly.

2. Restart the Media Gateway with the command *media\_gateway\_start*.

## 1.5 FAULT CODE 14 - ACTIVATION OF DEVICE BOARD HAS FAILED

### 1.5.1 DESCRIPTION OF FAULT CODE

Every board is regularly supervised by means of check questions. When the device processor has answered with the board identity and it has shown to be correct, a check is also made to see if the board is active and whether it is supposed to be so. If the board is passive while it should be active, an activation signal is issued. If the activation fails, a reset signal is sent and the alarm log is informed.

### 1.5.2 MEASURES

1. Use the command *board\_restart* to restart the device board.
2. Has the board been activated? Was the restart successful?
3. NO: Consult an expert.
4. YES: Turn to the main flow for verification.

## 1.6 FAULT CODE 15 - DEVICE BOARD FAULTY OR MISSING

### 1.6.1 DESCRIPTION OF FAULT CODE

All device boards are regularly checked in the LIM.

If a fault is detected, a fault marking will take place. No alarm will be generated, though, until detection and activation attempts of the same fault have taken place twice in a row, whereby the board is blocked.

If the answer from a board fails to occur, a reset signal is sent and the alarm log is informed.

### 1.6.2 MEASURES

1. Is the indicated board position expected to be equipped?
2. NO: Key the command *board\_config -remove* in order for the supposed faulty board to disappear from the LIMs board table.
3. YES: Restart with the command *board\_restart*.

## 1.7 FAULT CODE 23 - ROLLBACK OF LDAP DATA SUCCESSFUL

### 1.7.1 DESCRIPTION OF FAULT CODE

As a part of certain system initiated error recovery routines, the ldap data in all LIMs may be reloaded from a backup in order to reset the system to the last known state with data consistency. This means that all changes made since the latest dump occasion will be lost.

Examples of such recovery measures are data reload as a part of LIM reload and data reload when a command that alters exchange data fails to be completed.

**Note:** The fault code does not indicate any fault but is merely informative.

## 1.8 FAULT CODE 25 - SLIP ON PCM LINE

### 1.8.1 FAULT CODE DESCRIPTION

If the synchronization between the LIM and the GSM clock is faulty, (or between two LIMs) SLIP will occur on the PCM line and the supervision program is informed.

If a fault on the incoming clock sync. is detected by the GSM clock (alarm 88), consult this fault locating directions in the first place.

The slip can occur in one or several LIMs.

Reasons for faulty synchronization in a LIM could be:

- Faulty GJUL or faulty GJUG
- Faulty LIM clock
- Faulty transmission equipment
- Equipment is faulty or the sync is not configured accurately.

Reasons for faulty synchronization in several LIMs could be:

- Synchronization loop  
External sync. taken from a system that is receiving its sync. from this exchange.
- Disturbed external synchronization  
Disturbances on the external sync. will cause continuous re-synchronization in the whole system, giving SLIP faults.
- Disturbed synchronization in the master LIM  
Any faulty board on a 32 individual slot can disturb the LIM clock on the LSU board, thus affecting the LIM or the whole system.
- Disturbed synchronization in the master GSM  
Any faulty GJUG board can disturb the GS clock, GCU.
- Faulty clock bus  
Clock bus cable not connected to the GCU, will render in this alarm.

The system will receive one alarm per line.

The detailed print-out gives the board position, gsmult position and the first occurred ccc and group switch side.

If the system has not detected a slip indication for 30 minutes, the alarm will be cleared.

Clock Controlling LIM will be abbreviated to CCL in this document.

## 1.8.2

### MEASURE

1. Remove the external sync reception with command *trsp\_synchronization*, if any.
2. Any better?
3. YES: Check the incoming sync source and the TLU board with the master function.
4. NO: Problem solved by changing the master CCL?
5. YES: Check the LIM clock on the LSU and the sync source from the GJUL and TLU boards.
6. NO: Problem solved by changing the master GSM?
7. YES: Check the GCU board in the master GSM.  
Make a status read-out. See operational directions for *GROUP SWITCH*.
8. NO: The fault can be anywhere on the clock bus.  
See 1.40 Fault Code 88 - Group Switch Module Clock Alarm on page 28. Make a read-out and check that the CU control value is not on max or min. See operational directions for *GROUP SWITCH*.
9. Is the fault found and corrected?
10. NO: Consult an expert.
11. YES: Initiate external sync, with command *trsp\_synchronization*, if any.  
See operational directions for *GROUP SWITCH*.
12. Re-initiate the internal sync, with command *pcm\_synchronization*, if it was altered.  
See operational directions for *GROUP SWITCH*.

## 1.9

### FAULT CODE 29 - ALARM LOG ALMOST FULL

#### 1.9.1

#### FAULT CODE DESCRIPTION

The alarm system has a limited storage space for alarms. When there is a risk that the storage space will become full, an alarm is generated.

When the alarm log is full, the oldest alarm with the lowest alarm class will be overwritten unless incoming alarms have a lower alarm class, in which case they are not stored.

#### 1.9.2

#### MEASURE

Localize the fault with the aid of fault code references. Begin with the highest alarm class.



## 1.10 FAULT CODE 30 - INCREMENTATION ALARM FOR ALARM CLASS

### 1.10.1 FAULT CODE DESCRIPTION

If a specified number of system acknowledged alarms (defined in mdSystemConfig file) has arrived in alarm class 0, a new alarm is generated in alarm class 1. This is called incrementation alarm. The incrementation alarm is removed if the number of alarms in alarm class 0 becomes less than the specified number.

For related information see operational directions for *ALARM HANDLING*.

### 1.10.2 MEASURE

Localize the fault with the aid of fault code references. Begin with the highest alarm class.

## 1.11 FAULT CODE 31 - INCREMENTATION ALARM FOR ALARM CLASS 1

### 1.11.1 FAULT CODE DESCRIPTION

If a specified number of system acknowledged alarms (defined in mdSystemConfig file) has arrived in alarm class 1, a new alarm is generated in alarm class 2. This is called incrementation alarm. The incrementation alarm is removed if the number of alarms in alarm class 1 becomes less than the specified number.

For related information see operational directions for *ALARM HANDLING*.

### 1.11.2 MEASURE

Localize the fault with the aid of fault code references. Begin with the highest alarm class.

## 1.12 FAULT CODE 32 - INCREMENTATION ALARM FOR ALARM CLASS 2

### 1.12.1 FAULT CODE DESCRIPTION

If a specified number of system acknowledged alarms (defined in mdSystemConfig file) has arrived in alarm class 2, a new alarm is generated in alarm class 3. This is called incrementation alarm. The incrementation alarm is removed if the number of alarms in alarm class 2 becomes less than the specified number.

For related information see operational directions for *ALARM HANDLING*.

## 1.12.2

## MEASURE

Localize the fault with the aid of fault code references. Begin with the highest alarm class.

## 1.13

## FAULT CODE 33 - INCREMENTATION ALARM FOR ALARM CLASS 3

## 1.13.1

## FAULT CODE DESCRIPTION

If a specified number of system acknowledged alarms (defined in mdSystemConfig file) has arrived in alarm class 3, a new alarm is generated in alarm class 4. This is called incrementation alarm. The incrementation alarm is removed if the number of alarms in alarm class 3 becomes less than the specified number.

For related information see operational directions for *ALARM HANDLING*

## 1.13.2

## MEASURE

Localize the fault with the aid of fault code references. Begin with the highest alarm class.

## 1.14

## FAULT CODE 34 - LIM OUT OF ORDER

## 1.14.1

## FAULT CODE DESCRIPTION

The alarm is received when the LIM cannot be reached through signaling.

The fault might be due to network problems, faulty hardware in the LIM, or due to that the software in the LIM is being reloaded. The LIM is reloaded after a power failure or if a serious software fault has occurred in the LIM.

The LIM may also be out of reach due to a command ordered reload of the LIM.

If the LIM is being reloaded it will be operational in a couple of minutes and the alarms will be cleared. If the fault is of a more serious character manual measures can be needed.

**ADD INFO 1**

States if common functions exist in the LIM.

## 1.14.2

## MEASURE

1. Is the alarm older than 10 minutes?
2. NO: Wait 10 minutes before further action is taken.  
Wait to allow normal recovery to be ready.
3. YES: Use the Unix command *ping* towards the LIM.  
Try to contact the LIM over the network.
4. Either no network contact with the LIM or the use of *ping* is stopped.

5. Is it possible to login to the LIM with *ssh*?  
Does secure shell login work?
6. NO: Is it possible to login to the LIM at site?  
Try local login.
7. YES: Enter the command *status -system*.  
Check if the system is running any fault handling measures.
8. Enter the command *alarm* locally in the LIM o print (list) alarms in the alarm log.  
Handle related alarms, if there are any.

9. Read the files */var/log/messages* and */var/log/localmessages*.  
Look for logged records that are related to the fault.  
Consult an expert.
10. NO: Is the server rebooting or reloading?
11. YES: Wait for the server to complete the reboot and perform recovery.
12. NO: Is the server indicating any hardware fault?
13. NO: Replace faulty hardware and wait for system recovery?
14. NO: Consult an expert.

## 1.15

## FAULT CODE 35 - TRAFFIC HANDLING COMMON FUNCTION OUT OF ORDER

### 1.15.1

#### FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit not is accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which one version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

### 1.15.2

#### MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is located
2. YES: Go to the fault locating directions for *FAULT CODE 34*
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is located.
4. YES: Go to the fault locating directions for *FAULT CODE 50*.
5. NO: Has fault code 44 arrived in the alarm log for the program unit?
6. YES: Go to the fault locating directions for *FAULT CODE 44*.
7. NO: Has fault code 49 arrived in the alarm log for the program unit?
8. YES: Go to the fault locating directions for *FAULT CODE 49*.
9. NO: Has fault code 56 arrived in the alarm log for the program unit?
10. YES: Go to the fault locating directions for *FAULT CODE 56*.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult and expert.
14. YES: Are there any fault codes left in the alarm log?

## 1.16 FAULT CODE 36 - FAULT CORRECTING COMMON FUNCTION OUT OF ORDER

### 1.16.1 FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit is not accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which one version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

### 1.16.2 MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is located.
2. YES: Go to the fault locating directions for *FAULT CODE 34*.
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is located.
4. YES: Go to the fault locating directions for *FAULT CODE 50*.
5. NO: Has fault code 44 arrived in the alarm log for the program unit?
6. YES: Go to the fault locating directions for *FAULT CODE 44*.
7. NO: Has fault code 49 arrived in the alarm log for the program unit?
8. YES: Go to the fault locating directions for *FAULT CODE 49*.
9. NO: Has fault code 56 arrived in the alarm log for the program unit?
10. YES: Go to the fault locating directions for *FAULT CODE 56*.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult and expert.
14. YES: Are there any fault codes left in the alarm log?

## 1.17 FAULT CODE 37 - ORDINARY COMMON FUNCTION OUT OF ORDER

### 1.17.1 FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit is not accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which the version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

## 1.17.2

## MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is located.
2. YES: Go to 1.14 Fault Code 34 - LIM out of order on page 10.
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is located.
4. YES: Go to 1.24 Fault Code 50 - Restart of LIM has failed on page 17.
5. NO: Has fault code 44 arrived in the alarm log for the program unit?
6. YES: Go to 1.21 Fault Code 44 - Reload of program code has failed on page 16.
7. NO: Has fault code 49 arrived in the alarm log for the program unit?
8. YES: Go to 1.23 Fault Code 49 - Restart of program unit has failed on page 17.
9. NO: Has fault code 56 arrived in the alarm log for the program unit?
10. YES: Go to 1.29 Fault Code 56 - The system does not have an accessible backup on page 19.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult and expert.
14. YES: Are there any fault codes left in the alarm log?

## 1.18

## FAULT CODE 40 - EXCHANGE DATA RELOADED

## 1.18.1

## FAULT CODE DESCRIPTION

As a part of certain system initiated error recovery routines, the exchange data in all LIMs may be reloaded from the system backup in order to reset the system to the last known state with data consistency. This means that all changes made since the latest dump occasion will be lost. Examples of such recovery measures are data reload as a part of LIM reload and data reload when a command that alters exchange data fails to be completed.

**ADD INFO 1**

States which LIM that requested the data reload.

**ADD INFO 2**

States which program unit that requested the data reload.

**Note:** The program unit number is decimal, not hexadecimal.

## 1.18.2

## MEASURE

1. The fault code does not indicate any fault but is merely informative
2. Are there any other fault codes in the alarm log?

## 1.19 FAULT CODE 42 - RESTORATION OF EXCHANGE DATA HAS FAILED

### 1.19.1 FAULT CODE DESCRIPTION

An error occurred while restoring exchange data.

#### **ADD INFO 1**

States the error cause.

### 1.19.2 MEASURE

#### 1.19.2.1 *ADD INFO 1 = 9*

1. Is the value of ADD INFO 1 = 9?
2. NO: Continue to section ADD INFO 1 = 0, 1, 2, 3, 10.
3. YES: The program unit failed to respond within time limit.
4. Wait for restore of exchange data to occur or key the command *data\_restore*.
5. Does the fault still exist?
6. YES: Consult an expert and show the saved information to the expert.

#### 1.19.2.2 *ADD INFO 1 = 0, 1, 2, 3, 10, 11*

1. Is the value of ADD INFO 1 = 0, 1, 2, 3, 10?
2. YES: Exchange data configuration is missing/faulty. Data backup directory is missing/faulty. Data file is missing/faulty/does not match program code.
  - Install a safety copy.
  - Wait for restore of exchange data to occur or key the command *data\_restore*.
  - Does the fault still exist?
  - If YES, consult an expert.
3. NO: Is the value of ADD INFO 1 = 11?
4. YES: The job has been terminated by a job of higher priority. Wait for the new job to be completed and for restore of data to occur.
5. NO: Consult an expert.

## 1.20 FAULT CODE 43 - PROGRAM UNIT RELOADED AND RESTARTED

### 1.20.1 FAULT CODE DESCRIPTION

Information indicating that a program unit has been reloaded and restarted.

A reload of a program unit means that the existing program code in the memory is replaced with the program version stored on the external backup.

**Note:** The fault code does not indicate any fault but is merely informative.

1.20.2

MEASURE

-

1.21

## FAULT CODE 44 - RELOAD OF PROGRAM CODE HAS FAILED

1.21.1

### FAULT CODE DESCRIPTION

A system initiated reload of a program unit's program code has failed.

#### ADD INFO 1

States the error cause.

1.21.2

### MEASURE

1. Is the value of ADD INFO 1 = 3?
2. YES: A file handling error has occurred.  
Make sure that the program unit file is available in the file system.
3. NO: Is the value of ADD INFO 1 = 4,5?
4. YES: The program unit file is corrupted.  
Install safety copy.  
See operational directions for *ADMINISTRATOR USER'S GUIDE*.
5. NO: Consult an expert and show the saved information.

1.22

## FAULT CODE 45 - LIM RELOADED AND RESTARTED

1.22.1

### FAULT CODE DESCRIPTION

Information indicating that a LIM has been reloaded and restarted.

**Note:** The fault code does not indicate any fault but is merely informative.

1.22.2

### MEASURE

-



## 1.23 FAULT CODE 49 - RESTART OF PROGRAM UNIT HAS FAILED

### 1.23.1 FAULT CODE DESCRIPTION

The program unit is marked as faulty if a restart after reload is unsuccessful.

#### **ADD INFO 1**

Shows in which start phase the restart failed.

### 1.23.2 MEASURE

1. Attempt to restart the program unit by means of the command *restart -unit*.
2. Is the program unit restarted?
3. NO: Does alarm 39 - Checksum error or alarm 4 - parity error occur in alarm log?
4. YES: See the fault location instruction for respective fault codes.
5. NO: Consult an expert.

## 1.24 FAULT CODE 50 - RESTART OF LIM HAS FAILED

### 1.24.1 FAULT CODE DESCRIPTION

#### **ADD INFO 1**

Shows in which start phase the restart failed.

### 1.24.2 MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is loaded.
2. YES: Go to the fault locating directions for *FAULT CODE 34*.
3. NO: Has fault code 44 arrived in the alarm log?  
For the LIM where the common program is loaded.
4. YES: Go to the fault locating directions for *FAULT CODE 44*.
5. NO: Has fault 49 arrived in the alarm log for a program unit in the LIM?
6. YES: Go to the fault locating directions for *FAULT CODE 49*.
7. NO: Key the command *restart -lim* to restart the LIM.
8. Was the restart successful?
9. NO: Consult an expert.
10. Are there any fault codes left in the alarm log?

## 1.25 FAULT CODE 51 - DEVICE BOARD INDIVIDUAL MANUALLY BLOCKED

### 1.25.1 FAULT CODE DESCRIPTION

Individuals on the device board are blocked by means of command `block`. This takes place in the same way as for blocking of device boards (fault code 52).

**Note:** If this alarm is removed from the alarm log (with command `alarm`), the individual will remain manually blocked.

### 1.25.2 MEASURE

1. Is the individual expected to be blocked?
2. NO: Deblock the individual by means of command `deblock -equ`.
3. Key command `alarm` to print (list) alarms in the alarm log.  
More fault code exist in the alarm log?

## 1.26 FAULT CODE 52 - DEVICE BOARD MANUALLY BLOCKED

### 1.26.1 FAULT CODE DESCRIPTION

All individuals on a device board are blocked by means of the command `block -bpos`.

**Note:** If this alarm is cleared from the alarm log (with the command `alarm`), the device board will remain manually blocked.

### 1.26.2 MEASURE

1. Is the board expected to be blocked?
2. NO: Deblock the board by means of command `deblock -bpos`.
3. Any more fault codes exist in the alarm log?

## 1.27 FAULT CODE 53 - DEVICE BOARD POSITION ALREADY OCCUPIED

### 1.27.1 FAULT CODE DESCRIPTION

The physical board's board identity does not match the initiated board identity (board type) in the system for the designated location (board position).

Either the physical board is placed in the wrong position, or the initiation/configuration in the system is incorrect, and not matching the HW.

## 1.27.2

### MEASURE

1. Check the configuration using the command *board\_list*.
2. Is the board incorrectly placed?
3. NO: Call for an expert.
4. YES: Move the board to a correct position. (Alternatively, change the initiated board identity to match the physical board's identity, if the location is OK).

## 1.28

### FAULT CODE 54 - PROGRAM UNIT RESTARTED

#### 1.28.1

#### FAULT CODE DESCRIPTION

Information indicating that a program unit has been restarted.

#### 1.28.2

#### MEASURE

1. The fault code indicates no fault and is merely informative.
2. Are there any fault codes left in the alarm log?
3. NO: Return to the main flowchart.

## 1.29

### FAULT CODE 56 - THE SYSTEM DOES NOT HAVE AN ACCESSIBLE BACKUP

#### 1.29.1

#### FAULT CODE DESCRIPTION

This fault code is obtained when the system does not have any accessible backup.

#### 1.29.2

#### MEASURE

1. Enter the command *data\_backup*.  
Make a data backup.
2. Did the data backup fail or does fault code 56 remain in the alarm log?  
Wait for at least 2 minutes.
3. YES: Install a safety backup.  
See operational directions for *ADMINISTRATOR USER'S GUIDE* section *SAFETY BACKUP*.
4. Are there any fault codes left in the alarm log?  
Wait for at least 2 minutes.
5. Return to the main flowchart.

## 1.30 FAULT CODE 64 - RECOVERY MODE IS SET MANUAL

### 1.30.1 FAULT CODE DESCRIPTION

The alarm is obtained if the function for recovery mode is set to manual. This is done with the command `recoverymode`. Key the command `recoverymode -help` for more details.

### 1.30.2 MEASURE

1. Are maintenance going on in the system that requires manual recovery mode?
2. NO: Key the command `recoverymode -system` to activate system recovery mode.
3. Is the alarm cleared?
4. NO: Consult an expert.

## 1.31 FAULT CODE 65 - SYNCHRONIZATION FAULT IN LIM

### 1.31.1 FAULT CODE DESCRIPTION

**Note:** External synchronization source for a LIM, is for example a TLU board placed in the LIM. Internal synchronization source for a LIM is the own clock oscillator in the LSU-E.

The LIM clock (LSU-E) supervises the external clock synchronization in the back plane that is transmitted from the TLU board. The status is reported to the supervision program and an alarm is issued in the following cases:

- External clock rate is not present although it is expected.
- External clock rate is present although it is not expected.
- More than one external clock rate present.
- External clock rate is present but bad.
- External clock rate is beyond boundaries.

#### ADD INFO 1

- 0 Not Valid.
- 1 The LIM does not have any external synchronization source, although there is one specified.
- 2 The LIM has an external synchronization source, although there is no one specified.
- 3 The LIM has more than one external synchronization source, no external synchronization source is specified.
- 4 The LIM has more than one external synchronization source, only one is specified.

#### ADD INFO 2

- 0 Not Valid.

- 1 The frequency of the external synchronization source exists, but LIM clock cannot synchronize to it.
- 2 The difference of the external synchronization source and the synchronization source of LIM clock is not within the allowed limit.

### ADD INFO 3

- 0 Not Valid.
- 1 The LIM is receiving synchronization from the external synchronization source.

## 1.31.2

### MEASURE

External synchronization source for a LIM, is for example a TLU board placed in the LIM. Internal synchronization source for a LIM is the own clock oscillator in the LSU-E.

### 1.31.2.1

*Does FAULT CODE 65 indicate that the LIM has more than one external synchronization source?*

The difference between the external frequency and the LIM's own oscillator frequency is too large, therefore the LIM is unable to lock to the external frequency. One reason for this could be that the LIM's own oscillator is aging.

1. NO: Continue to the next section.
2. YES: The LIM's external synchronization source which were pointed out as faulty, must be investigated.
3. Define a new synchronization source for the LIM and do a resynchronization.  
Use the command *trsp\_synchronization*.
4. Does fault code 65 still occur for the LIM?
5. YES: The LIM's oscillator must be replaced, which means the LSU-E board must be replaced.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
6. Does fault code 65 still occur for the LIM?
7. NO: Check the previous synchronization source.
8. YES: Consult an expert.

### 1.31.2.2

*Does fault code 65 indicate that the LIM is receiving an external synchronization although there is no one expected?*

1. NO: Continue to the next section.
2. YES: A device board is giving synchronization to the back plane without this being expected.  
This device board can be broken and working incorrectly.
3. Do a resynchronization of the LIM.  
Use the command *trsp\_synchronization*.
4. Does fault code 65 still occur for the LIM?

5. YES: Consult an expert.

Test signal TESTFUNC can be used to read out which positions that give synchronization to the back plane. The signal is sent to LSU-E board. Use the command *message\_send*

### 1.31.2.3

*Does fault code 65 indicate that the LIM is not receiving an external synchronization although there is one expected?*

1. NO: Continue to the next section.
2. YES: LIM does not receive external synchronization.  
This can depend on, **see note**.
3. Do a resynchronization of the systems.  
See the command *trsp\_synchronization*.
4. Does fault code 65 still occur for the LIM?
5. YES: Replaced the expected device board with a new one.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
6. Is this the first time the device board has been replaced?
7. YES: Do a resynchronization of the systems again.
8. NO: Consult an expert.

**Note:** This can depend on:

The buffer circuit for transmission of the clock rate (FRSY signal) towards the back plane is faulty.

The board is not updated from the software.

On the back plane a pin is bent or a foil-connection is cut or short circuited.

The MUX circuits on the DSU board that receives the clock rate (FRSY signal) from respective device board position could be faulty.

The oscillator on the LSU-E board could be faulty.

### 1.31.2.4

*Does fault code 65 indicate that the external synchronization source exists and the LIM cannot synchronize to it?*

1. NO: Fault code 65 indicates that the external synchronization is not within the allowed limits.
2. YES: Is the back plane LBP14 or newer version?  
In an previous version, the synchronization from all device boards is received on the same wire.
3. NO: The external synchronization source is probably a mix between two device boards giving synchronization to the back plane.
4. YES: The difference between the external and the internal synchronization sources is very bad. This problem must be investigated further.  
This can depend on: The clock rate is not correctly recovered from the PCM line.
5. Consult an expert.

## 1.32 FAULT CODE 66 - TRAFFIC HANDLING COMMON FUNCTION FAULTY

### 1.32.1 FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit not is accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which one version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

### 1.32.2 MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is loaded.
2. YES: Go to the fault locating directions for *FAULT CODE 34*.
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is loaded
4. YES: Go to the fault locating directions for *FAULT CODE 50*.
5. NO: Has fault code 44 arrived in the alarm log?  
For the LIM where the common program is loaded
6. YES: Go to the fault locating directions for *FAULT CODE 44*.
7. NO: Has fault 49 arrived in the alarm log for a program unit in the LIM?
8. YES: Go to the fault locating directions for *FAULT CODE 49*.
9. NO: Has fault 56 arrived in the alarm log for a program unit in the LIM?
10. YES: Go to the fault locating directions for *FAULT CODE 56*.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult an expert.
14. Are there any fault codes left in the alarm log?

## 1.33 FAULT CODE 67 - FAULT CORRECTING COMMON FUNCTION FAULTY

### 1.33.1 FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit not is accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which one version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

### 1.33.2

#### MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is loaded.
2. YES: Go to the fault locating directions for *FAULT CODE 34*.
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is loaded
4. YES: Go to the fault locating directions for *FAULT CODE 50*.
5. NO: Has fault code 44 arrived in the alarm log?  
For the LIM where the common program is loaded
6. YES: Go to the fault locating directions for *FAULT CODE 44*.
7. NO: Has fault 49 arrived in the alarm log for a program unit in the LIM?
8. YES: Go to the fault locating directions for *FAULT CODE 49*.
9. NO: Has fault 56 arrived in the alarm log for a program unit in the LIM?
10. YES: Go to the fault locating directions for *FAULT CODE 56*.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult an expert.
14. Are there any fault codes left in the alarm log?

## 1.34

### FAULT CODE 68 - ORDINARY COMMON FUNCTION FAULTY

#### 1.34.1

##### FAULT CODE DESCRIPTION

A common program unit often occurs in a version with two editions in the system, one active and one passive as standby. The alarm is obtained when one version of the common program unit not is accessible any longer to the rest of the system.

This is due to that one version of the common program unit is faulty or that the LIM in which one version of the common program unit is located is faulty.

A combination of these causes can, of course, lead to the same fault state.

#### 1.34.2

##### MEASURE

1. Has fault code 34 arrived in the alarm log?  
For the LIM where the common program is loaded.
2. YES: Go to the fault locating directions for *FAULT CODE 34*.
3. NO: Has fault code 50 arrived in the alarm log?  
For the LIM where the common program is loaded



4. YES: Go to the fault locating directions for *FAULT CODE 50*.
5. NO: Has fault code 44 arrived in the alarm log?  
For the LIM where the common program is loaded
6. YES: Go to the fault locating directions for *FAULT CODE 44*.
7. NO: Has fault 49 arrived in the alarm log for a program unit in the LIM?
8. YES: Go to the fault locating directions for *FAULT CODE 49*.
9. NO: Has fault 56 arrived in the alarm log for a program unit in the LIM?
10. YES: Go to the fault locating directions for *FAULT CODE 56*.
11. NO: Start the system by the command *start --system*.
12. Was the alarm cleared?
13. NO: Consult an expert.
14. Are there any fault codes left in the alarm log?

## 1.35

## FAULT CODE 69 - COMMON FUNCTION IS LOADED IN MORE THAN TWO LIMS

### 1.35.1

#### FAULT CODE DESCRIPTION

A program unit can be of type Common function. This means that it is centrally located and can be used by all program units in all LIMs.

A common program unit may only occur in one version and two editions, one active and one passive, which are located in different LIMs.

An alarm is generated when a common function exists in more than two LIMs.

### 1.35.2

#### MEASURE

1. Check in which LIMs the common function unit is loaded. Use the command *pu\_info -unit*.
2. Determine which two versions of the program unit are to remain in the system. Use the command *status -comfunc*.
3. Remove excess program units from the system. Use the command *pu\_remove*. Do not remove the active common function.
4. Update the common function data in the system. Use the command *start --system*.
5. Are there any fault codes left in the alarm log?
6. Return to the main flow.

## 1.36

## FAULT CODE 70 - TOO MANY SIDE CHANGES IN THE GROUP SWITCH

## 1.36.1

## FAULT CODE DESCRIPTION

The number of side changes in the group switch, due to PCM-line alarm, has exceeded the limit 3/hour.

System blocking caused by the following types of fault can cause side changes:

- signal channel fault (T16)
- parity fault in the group switch
- AIS (Alarm indication signal which is issued when all bits in all time slots on the PCM-line are set to one)
- frame locating fault, result when three consecutive controls show incorrect information in the synchronization word.

## 1.36.2

## MEASURE

1. Check all PCM-lines in the system at the side that issued the alarm by keying command *pcm\_status*.
2. Key command *pcm\_status* for the PCM-lines that show any of the faults mentioned above.
3. Are faulty PCM-lines found on either side?
4. YES: Block the faulty PCM-lines on the faulty side by keying command *pcm\_order*.
5. Key command *pcm\_order* to clear the control memory.  
Key command *pcm\_status* to clear the alarm.
6. Unblock the restarted PCM-lines with command *pcm\_order*.
7. Key command *pcm\_status* for each PCM-line to get relevant alarm situation.
8. Does the PCM-line show any of the above alarms?
9. YES: Key command *pcm\_status* for those PCM-lines that show the alarms.
10. Any PCM-line still faulty?
11. YES: Key command *pcm\_status* for the faulty GSM side to which the PCM-line is tied.
12. If any of the PCM-lines (GJU-L) are faulty, change the GJU-G board and/or the GSMs own time switch boards.  
See the operational directions for *GROUP SWITCH*.
13. Key command *pcm\_config* for relevant GSM.
14. Check PCM-line using command *pcm\_status*.
15. Is the PCM-line faulty?
16. YES: Consult an expert.
17. NO: if necessary, define a new active side using command *pcm\_config*.

## 1.37 FAULT CODE 73 - LIM RESTARTED

### 1.37.1 FAULT CODE DESCRIPTION

Information stating that a LIM has been restarted.

#### **ADD INFO 1**

Show the cause is included in the alarm.

### 1.37.2 MEASURE

1. The fault code indicates no fault; it is only of an informing character.
2. Are there still fault codes in the alarm log?
3. Return to the main flow.

## 1.38 FAULT CODE 81 - LIM MANUALLY BLOCKED

### 1.38.1 FAULT CODE DESCRIPTION

All individuals on all device boards in a LIM are blocked for traffic by means of command block.

The alarm is only a means of information and if the right LIM is blocked, no actions need to be performed.

Deblocking is performed with the command `deblock`.

### 1.38.2 MEASURE

1. Is the LIM expected to be blocked?
2. NO: Deblock the LIM by means of command `deblock -lim`.
3. Are there more alarms in the alarm log?

## 1.39 FAULT CODE 82 - HIGH BIT FAULT RATE ON PCM-LINK

### 1.39.1 FAULT CODE DESCRIPTION

Running at a higher bit fault rate on the group switch PCM-line than the defined alarm level, so the alarm log is informed. This is an observation alarm. Action shall, however, be taken in the case of data transmission and in the case of a high bit fault rate on the link.

### 1.39.2 MEASURE

1. Enter the command `pcm_status` to print the status of the PCM-line(s) indicated.
2. Are there other alarms for the indicated PCM-line(s)?

3. YES: Check the Fault locating directions for those alarms, if any.
4. NO: Check if there is any external transmission equipment that has a too high bit fault rate, or change the PCM-line.

## 1.40

## FAULT CODE 88 - GROUP SWITCH MODULE CLOCK ALARM

### 1.40.1

#### FAULT CODE DESCRIPTION

The GCU2 supervises functions on the board and the communication between the GCU2 boards. If any fault is detected, the GCU2 will issue an Internal Clock Alarm (ICA), causing fault code 88. The alarm does not necessarily imply, that non-synchronization between group switch modules exist.

Only one alarm is raised, with information about all the GJUG boards that reports clock alarm and/or clock order incomplete.

When a group switch is put into service, the most probable fault is a faulty cable, bent pins in the front device or in the back plane.

During operation the most probable fault is a faulty GCU2 board. If only alarm 88 is raised it could be the GCU2 bus cable that is faulty or not connected properly. If reported incomplete together with an 1:11 alarm, it is most likely a clock controlling PCM line that is faulty. Correct the 1:11 alarm first. If clock alarm and/or together with an 1:13 alarm, there is most likely a faulty GCU2 board in the GSM indicated by the 1:13 alarm.

The alarm will be given at re-synchronization initiated by command or by a fault. The alarm is automatically cleared in this situation. The clock alarm or the clock order incomplete, or both has been clear for a line. That is, the alarm has first been raised, then cleared again 10 seconds later.

If there are no other group switch alarms, the fault is most likely not affecting the traffic.

**Note:** When removing a clock bus cable, there will be no synchronization between the GSMs, causing parity fault, slip and lost signals in the group switch. This will disturb the traffic.

### 1.40.2

#### MEASURE

1. Read status on all GCU2 boards.  
See operational directions for *GROUP SWITCH*.
2. Display = E5 or E9? or Printout, ERR= 64-77?
3. YES: Change the faulty board.  
See operational directions for *GROUP SWITCH*.  
If changing the board does not solve the problem, continue to either of the flows in the following sections.
4. NO: Continue to either of the flows in the following sections.
5. Is the Group switch duplicated?

#### 1.40.2.1

##### *Single Group Switch*

1. Key the command *pcm\_order* to block all GSMs except the master GSM.  
See operational directions for *GROUP SWITCH*.
2. End all GSMs except the master GSM, key the command *pcm\_config*.
3. Check all pins and cables on the clock bus.  
If just one alarm is given, start with the alarming board.
4. Any fault found?
5. NO: Replace all GCU2 boards one at a time and check with *pcm\_status* after each replacement.  
If several fault code 88 are given, start with the GCU2 in the master GSM.
6. Wait until the system is steady.
7. Key command *pcm\_order* to clear the control memory.  
See operational directions for *GROUP SWITCH*.
8. Key the command *pcm\_config* to initiate the GSMs.
9. Key command *pcm\_order* to test all GSMs.  
See operational directions for *GROUP SWITCH*.
10. Key the command *pcm\_order* to unblock the GSMs.

#### 1.40.2.2

##### *Duplicated Group Switch*

1. Change side in group switch if a board is to be replaced on active side, with command *pcm\_config*.
2. Check all pins and cables on the clock bus.  
If just one alarm is given, start with the alarming board.
3. Any fault found?

4. If NO, replace all GCU2 boards one at a time and check with *pcm\_order* after each replacement.  
If several fault code 88 are given, start with the GCU2 in the master GSM.
5. Wait until the PCM lines are OK.  
Check with command *pcm\_order*.
6. Key command *pcm\_order* to clear the control memory.  
See operational directions for *GROUP SWITCH*.
7. Key the command *pcm\_order* to test all GSMs on the passive side.  
See operational directions for *GROUP SWITCH*.

## 1.41 FAULT CODE 93 - BACKUP OF EXCHANGE DATA HAS FAILED

### 1.41.1 FAULT CODE DESCRIPTION

Dump of exchange data to backup has failed. The fault code is issued per LIM.

#### **ADD INFO 1**

States the error cause.

### 1.41.2 MEASURE

1. Is fault 42 present in the alarm log?
2. YES: handle fault 42.
3. Is ADD INFO 1 = 6?
4. YES: One or several program units need restart or reload.
5. Is fault code 44 present in the alarm log?
6. YES: handle fault 44.
7. Check the status of the program units. Key the command *status -lim y -unit all* where y = LIM number reported in alarm.
8. Are all program units OK?
9. YES: Order backup of exchange data again.
10. Faulty start phase 1.3 and/or reload data?
11. YES: Restore exchange data. Key the command *data\_restore*.
12. Faulty start or restart phase 1.0, 1.5 or 2.0?
13. YES: Restart the faulty program units.
14. Are all program units OK?
15. YES: Consult an expert.
16. NO: Order backup of exchange data again.

### 1.41.2.1

#### ADD INFO 1 = 0

1. Is ADD INFO 1 = 0? Exchange data is inconsistent.
2. NO: Continue to ADD INFO 1 = 11.
3. YES: Check the market data status. Key the command *mxone\_maintenance* (and select the market option, which will show the currently valid market).
4. Is market data consistent?
5. NO: set market data/run necessary start phases.
6. Is market data consistent? If NO, consult an expert.
7. YES: Order backup of exchange data again.
8. Restore exchange data. Key the command *data\_restore*.
9. Was the restore successful?
10. NO: Consult fault code 42.
11. YES: Order backup of exchange data again.

### 1.41.2.2

#### ADD INFO 1 = 11

1. Is ADD INFO 1 = 11? The job has been terminated by a job of higher priority.
2. YES: Wait for the new job to complete. Order backup of exchange data again.
3. NO: Order backup of exchange data again.
4. Was the backup successful?
5. NO: Consult an expert.

## 1.42

## FAULT CODE 97 - INTERNAL ERROR ON LSU BOARD

### 1.42.1

#### FAULT CODE DESCRIPTION

When LSU-E discovers a hardware fault it informs LSSUP, the LIM-switch supervision program.

##### **Additional text**

States the type of LSU-E fault.

### 1.42.2

#### MEASURE

1. Is the added info "no contact"?  
Network error or a faulty LSU-E circuit board.
2. Check the network and the cabling. If both are OK change the LSU-E board.
3. YES: possible errors are
  - "no contact with LIM Clock Unit (LCU)",
  - "error on LIM Clock Unit (LCU)", "PROM fault",
  - "RAM fault", or "cm fault".

If the fault remains change the LIM Clock Unit (LCU) board

A manual test can be performed with the command  
*ls\_config\_test -lim*.

## 1.43 FAULT CODE 98 - SIGNALING ERROR IN THE LIM SWITCH

### 1.43.1 FAULT CODE DESCRIPTION

When LSU discovers a signal error it informs the supervision program of the LIM switch.

#### **ADD INFO 1**

States where the signaling error is encountered.

#### **ADD INFO 2**

States the type of signaling error.

### 1.43.2 MEASURE

1. Is a DSU pointed out to be faulty?
2. YES: Block the relevant DSU board with the command *ls\_config\_block -dsu -lim*.
3. Change the relevant DSU board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Unblock the relevant DSU board with the command *ls\_config\_deblock*.
5. Continue with blocking of LIM and change of LSU board in the main flow.

## 1.44 FAULT CODE 100 - INTERNAL ERROR ON DSU BOARD

### 1.44.1 FAULT CODE DESCRIPTION

When the DSU discovers a hardware fault it reports it to the supervision program of the LIM switch, LSSUP.

#### **Additional text**

First: States faulty magazine (DSU board).

Second: States the type of magazine (DSU) fault.

### 1.44.2 MEASURE

1. Block the relevant DSU board with the command *ls\_config\_block*.
2. Check that the connected board edge cables are correctly placed.
3. Is the DSU board OK?
4. YES: Unblock relevant DSU board with the command *ls\_config\_deblock*, if it is blocked.



5. NO: Change the relevant DSU board.  
Test the new DSU board with the command *block\_list*.  
Is the DSU board OK?
6. NO: Change the relevant DSU board again, according to above.
7. YES: Unblock relevant DSU board with the command *ls\_config\_deblock*, if it is blocked.

## 1.45 FAULT CODE 101 - FAULTY CLOCK PROCESSOR

### 1.45.1 FAULT CODE DESCRIPTION

When a problem occurs with the LSU clock processor, it will be detected by the main processor on the LSU. The LSU board will inform LSSUP, the LIM switch supervision program, through the normal routine supervision.

**Additional text**

States the type of clock processor fault.

### 1.45.2 MEASURE

1. Use the command *board\_restart* for the LSU-E board.  
Was it a temporary fault?
2. Does the fault remain?
3. YES: Block the LIM and change the LSU-E board. Use the command *block*.

## 1.46 FAULT CODE 102 - POWER FAILURE DETECTED BY DSU

### 1.46.1 FAULT CODE DESCRIPTION

When a voltage disappear from a magazine, it will be detected by the DSU board in the relevant magazine. The DSU board will send a signal to the LSU-E board which forwards it to LSSUP, the LIM switch supervision program.

**Additional text**

First: States DSU board.

Second: States missing voltage.

### 1.46.2 MEASURE

1. Find out in which magazine the power has failed.
2. Check relevant voltage on the power unit with a voltage meter.
3. Power missing?
4. NO: Block the relevant DSU board with command *ls\_config\_block*.
5. Change the relevant DSU board.

Test the new DSU board with command *block\_list*. Check if device boards can be reached.

Is the DSU board OK?

6. NO: Change the relevant DSU board again according to above.
7. YES: Unblock the relevant DSU board with command *ls\_config\_deblock*.
8. Continue with blocking of LIM and change of relevant power unit.

## 1.47 FAULT CODE 103 - THE DSU BOARD IS BLOCKED BY COMMAND

### 1.47.1 FAULT CODE DESCRIPTION

When an LSU-E board is blocked by the command *ls\_config\_block*, the LSSUP program sends an alarm to the alarm log.

**Additional text**

States DSU board.

### 1.47.2 MEASURE

Unblock the relevant DSU board with the command *ls\_config\_deblock*.

## 1.48 FAULT CODE 104 - POWER FAILURE DETECTED BY LSU

### 1.48.1 FAULT CODE DESCRIPTION

When the 5 volt voltage disappears from a DSU it will be detected by the LSU-E board which forwards it to LSSUP, the LIM switch supervision program. This fault might also occur if the DSU cable is removed.

**Additional text**

States DSU board.

### 1.48.2 MEASURE

1. Check with the voltage meter if +5V is missing in the relevant magazine.
2. Is +5V missing?
3. YES: Change relevant power unit. Check the new power unit.
4. NO: Block the relevant DSU board with command *ls\_config\_block*.
5. Change the relevant DSU board.  
Test the new DSU board.  
Is the DSU board OK?
6. NO: Change the relevant DSU board again according to above.
7. YES: Unblock the relevant DSU board with command *ls\_config\_deblock*.

## 1.49 FAULT CODE 112 - INCONSISTENCY BETWEEN LOCAL BACKUP AND LIM MEMORY

### 1.49.1 FAULT CODE DESCRIPTION

When the 5 volt voltage disappears from a DSU it will be detected by the LSU-E board which forwards it to LSSUP, the LIM switch supervision program. This fault might also occur if the DSU cable is removed.

#### **ADD INFO 1**

States DSU board.

### 1.49.2 MEASURE

#### 1.49.2.1 *ADDINFO 1 = 1*

1. Is the value of ADD INFO 1 = 1?
2. NO: Continue to ADD INFO 1 = 2.
3. YES: program unit or units added by maintenance operator since last exchange data backup.  
The added program units have been removed from the LIM by the system.
4. Shall the previously added program units be added again?
5. YES: add the previously added program units once more. Use the command *pu\_add -unit*.

#### 1.49.2.2 *ADDINFO 1 = 2*

1. Is value of ADD INFO 1 = 2?
2. NO: Continue to ADD INFO 1 = 3.
3. YES: program unit or units removed by maintenance operator since last exchange data backup.  
The program will be loaded again.
4. Shall the program units be removed?
5. YES: Remove the previously removed program units once more to avoid data inconsistency.

#### 1.49.2.3 *ADDINFO 1 = 3*

1. Is the value of ADD INFO 1 = 3?
2. NO: Consult an expert.
3. YES: program unit or units have been loaded with different program code since last exchange data backup (likely due to an upgrade).  
The program units will be reloaded.

4. Is fault code 42 or 44 present in the alarm log?
5. YES: handle fault code 42 or 44 or both.
6. Shall the new program code be loaded again?
7. YES: Consult the applicable upgrade procedure.
8. NO: Consult an expert.

## 1.50 FAULT CODE 114 - DEVICE BOARD HAS BEEN ACTIVATED

### 1.50.1 FAULT CODE DESCRIPTION

All device board in LIM are regularly supervised in routine test. If a device board does not answer on the regularly check, after a second attempt, an attempt to activate this board is done. If the activating of this board was successful, sends fault code as an information alarm.

### 1.50.2 MEASURE

-

## 1.51 FAULT CODE 117 - HARDWARE ID DOES NOT MATCH LICENSE FILE

### 1.51.1 FAULT CODE DESCRIPTION

This fault code is given when the licence server detects that the ID of the hardware does not match with the license file. This can be caused by moving a license file to another hardware, installing an incorrect license file or replacing the hardware holding the hardware ID.

It is not possible to seize or release new licenses as long as this alarm condition exists.

### 1.51.2 MEASURE

1. Does the hardware ID match with the license file?  
Check the use of the correct license file with the command *license\_status* and command *license\_print*.
2. Has the license file provided the wrong hardware ID?
3. YES: Request a new license file from Mitel.
4. Is the license file lic.dat at the location /etc/opt/eri\_sn/?
5. NO: make sure that the correct license file is at the location etc/opt/eri\_sn/lic.dat.
6. Use the command *license\_reread* to request that the server reads the license file again.
7. Consult an expert.

## 1.52 FAULT CODE 118 - LICENSE SERVER OUT OF ORDER: INTERNAL ERROR OR INCONSISTENCY

### 1.52.1 FAULT CODE DESCRIPTION

This fault code is given in the following occasions:

- No license file was found
- Error decrypting or parsing the license file
- Inconsistency in the license server data
- Internal error in the license server.

It is not possible to seize or release new licenses as long as the alarm condition exists.

### 1.52.2 MEASURE

1. Do you use the correct license file, or was it altered e.g. during a FTP transfer?  
Check the use of the correct license file with the command *license\_status* and command *license\_print* (it makes the encrypted license file readable).
2. Is the license file *lic.dat* modified or garbled?
3. YES: Request a new license file from Mitel.
4. Is the correct license file *lic.dat* at the location */etc/opt/eri\_sn/*?
5. NO: Make sure that the correct license file is at the location */etc/opt/eri\_sn/lic.dat*.
6. Use the command *license\_reread* to request that the license server reads the license file again.
7. Do a data restore on the exchange data.
8. Is the license server working again?
9. NO: Consult an expert.

## 1.53 FAULT CODE 120 - LESS THAN SEVEN DAYS OF TRIAL PERIOD LEFT

### 1.53.1 FAULT CODE DESCRIPTION

The fault code is given when the licence server detects that there is seven days or less left of the trial period for a licence file and the number of allocated licences exceeds the number of allowed licences.

### 1.53.2 MEASURE

1. Key the command *license\_status* to find out which licence object is over-allocated.
2. Is the over-allocated licence object to be used after the end of the trial period?

3. YES: place a new order on the order desk to increase the number of licences for the licence object.
4. NO: Release the extra licences by terminating the applications using these licences.

Consult operational directions for relevant application.

## 1.54 FAULT CODE 121 - LICENSE SERVER BLOCKED: OVER LICENSE LIMIT

### 1.54.1 FAULT CODE DESCRIPTION

The fault code is given when:

- The license server detects that the number of allocated licenses exceeds the number of allowed licenses.
- The license server detects that the current license file is older than (sequence number in file) than the previously used license file.

### 1.54.2 MEASURE

1. Is one of the license objects over-allocated (and what is the sequence number of the license file)?  
Use the command *license\_status* to find out which license object is over-allocated, and to read the sequence number of the license file.
2. YES: Consult fault locating directions for *FAULT CODE 120*.
3. NO: Consult an expert.

## 1.55 FAULT CODE 122 - LICENSE COUNTERS OUT OF SYNCHRONIZATION

### 1.55.1 FAULT CODE DESCRIPTION

The Licence usage counting is distributed functionality. In some cases (like reload data manipulation) these counters get out of synchronisation. If this happens an automatic synchronisation process is started to correct this fault. During this process any licence requests are denied with the error indication: *licence server is temporarily blocked*.

### 1.55.2 MEASURE

1. Wait 5 - 10 minutes; The automatic synchronisation process was started by LISH to correct the problem. Clear the alarm with the command *alarm -e --alarm-code 122* after 5 - 10 minutes and retry the configuration changing commands.
2. Was the errors situation automatically corrected?
3. NO: Wait another 30 minutes for automatic correction.
4. Was the error situation automatically corrected?

5. NO: Consult an expert.

## 1.56 FAULT CODE 259 - FAULTY FTU BOARD

### 1.56.1 FAULT CODE DESCRIPTION

The function for time supervision of the FTU board (watchdog) indicates that this board is faulty.

The FTU board sets up a direct connection between predetermined extensions and the public exchange as a result of power failure or processor fault.

### 1.56.2 MEASURE

1. Change the FTU board.  
See the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.
2. Wait 5 minutes, then check if the alarm has reoccurred. Check also if trunk line alarms have been received. They are due to broken connections through this board.
3. Did the alarm recur?
4. NO: Consult an expert.
5. Return to the main flow.

## 1.57 FAULT CODE 260 - FAULT ON LINE TO INTERWORKING PBX OR PUBLIC EXCHANGE

### 1.57.1 FAULT CODE DESCRIPTION

The alarm is generated in the following situation:

- The voltage on the line is not in accordance with the table values.
- No current in idle state is detected.
- No seizure acknowledgment has been received.
- A number of consecutive proceed-to-send signals have failed to appear.
- No clearing acknowledgment has been received.

#### **ADD INFO 1**

Individual pointer to TRS data individual.

#### **ADD INFO 2**

Description of the type of line fault for external lines.

### 1.57.2 MEASURE

1. Was the alarm generated by an outgoing external line using E&M-signaling?

2. YES: Continue to section Alarm generated by an out going external line.
3. NO: Is the line that was indicated as faulty included in a route which has been assigned the category for voltage in idle state? (Check with the *RODAP* command.)
4. YES: Continue to section Check of correct voltage.
5. NO: Change the line board.  
See the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*
6. Make a call on the line.
7. Did the fault reappear?
8. YES: The fault is probably to be found on the line or in the public exchange or interworking PBX.
9. For corrective measures, contact the person responsible for external line operation.

#### 1.57.2.1

#### *Alarm generated by an outgoing external line.*

1. Is the line disturbance-marked? Enter the command *block\_list*.
2. NO: Deblock the line concerned. Enter the command *deblock*.
  - Make a new call on the line then clear the connection.
  - Did the alarm recur?
  - YES: Change the line board after blocking.
  - See the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.
  - Make a new call and clear the connection.
  - Did the alarm recur?
  - Check the cables from the board to MDF. Contact the person responsible for external line operation for checking of the line and the interworking PBX.
  - Probably cause of fault: Break on the line, or the interworking PBX has ceased to send seizure acknowledgement or clearing acknowledgement signals. Return to the main flow.
3. YES: Deblock the line concerned. Enter the command *deblock*
4. Make a new call on the line.
5. Has the line been disturbance-marked again? Enter the command *block\_list*
6. YES: Has a too short supervision time been set for the proceed-to-send signal?
7. YES: increase the supervision time for the proceed-to-send signal.  
Go back to step 4.
8. NO: should the interworking PBX always send a proceed-to-send signal before the sending of digits starts?
9. NO: Change the route data for the line so that no proceed-to-send signal is to be expected.



10. YES: Contact the person responsible for external line operation for checking of the interworking PBX and the line.  
Return to the main flow.

## 1.57.2.2

*Check of correct voltage*

1. Have all lines on the board been marked as faulty?
2. NO: enter the command *block* to block the board. Continue to the next step.
3. YES: Check if the voltage (24 V - 48 V) from the public exchange or interworking PBX is applied to the cable pair concerned in the MDF.
4. Was the correct voltage applied?
5. NO: for corrective measures, contact the person responsible for external line operation.
6. YES: Replace the line board.
7. Does the fault remain?
8. YES: Consult an expert.

## 1.58

**FAULT CODE 261 - NO CONNECTION WITH OPERATOR CONSOLE**

## 1.58.1

**FAULT CODE DESCRIPTION**

The MX-ONE Service Node Operator Work Station does not react when pressing buttons.

**ADD INFO 1**

Individual pointer to OPS data individual.

## 1.58.2

**MEASURE**

1. Does the alarm log contain other fault codes?
2. NO: Is the Operator Workstation powered on?
3. NO: Power on the Operator Workstation. Check connections to LAN and Operator Workstation. Activate the Operator Workstation program. Check Event Viewer log file for more details related to fault.
4. YES: Is the OMD (media device) connected to the LAN?
5. NO: Connect the OMD to the LAN.
6. YES: Is there connection between the Media Gateway and the LAN? Is the Media Gateway working?  
All operator traffic requires multi-party resources in the Media Gateway.
7. NO: Connect the Media Gateway.
8. YES: was the Media Gateway replaced?
9. NO: Replace the Media Gateway.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE*.

## 1.59 FAULT CODE 264 - FAULTY MF SENDER

### 1.59.1 FAULT CODE DESCRIPTION

A multi frequency sender fault is detected when performing periodic routine testing of MF receivers and senders. (Only supported with MFUs).

### 1.59.2 MEASURE

1. Does the indicated position correspond to an MFU board?
2. YES: Replace the MFU board, or consider changing to MGU.  
See the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*
3. NO: Consult an expert.  
Return to the main flow.

## 1.60 FAULT CODE 265 - FAULTY MF RECEIVER

### 1.60.1 FAULT CODE DESCRIPTION

A multi frequency receiver fault is detected when performing periodic routine testing of MF receivers and senders. (Only supported with MFUs).

### 1.60.2 MEASURE

1. Does the indicated position correspond to an MFU board?
2. YES: Replace the MFU board, or consider changing to MGU.  
See the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*
3. NO: Consult an expert.  
Return to the main flow.

## 1.61 FAULT CODE 268 - DIGITAL TRUNK OUT OF ORDER, AIS SIGNAL RECEIVED

### 1.61.1 FAULT CODE DESCRIPTION

The digital trunk resources of the Media Gateway (2 Bit) have discovered an error in that it has received less than 2 zeros (= basically all ones) per the last 250 micro seconds, and therefore registers a fault. All initiated individuals on the virtual or physical board have been automatically blocked. If more than 3 zeros per 250 micro seconds are received, the alarm will be cancelled.

The digital trunk resources of the Media Gateway (1.5 Bit) have discovered an error in that it has received unframed all 1"s in 5 frames. All initiated individuals on the virtual

or physical board will be automatically blocked. The alarm will be cancelled when the frame synchronization is obtained in succession for 150 ms.

Also called Alarm Indication Signal (AIS) alarm.

### 1.61.2

#### MEASURE

1. Restart the virtual trunk board by entering the command *board\_restart*.
2. Has the alarm returned?
3. YES: Replace the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: probably a fault on the line in interworking/public exchange. Inform instance responsible for the line.

## 1.62

### FAULT CODE 269 - DIGITAL TRUNK, LOSS OF FRAME SYNCHRONIZATION WORD

#### 1.62.1

##### FAULT CODE DESCRIPTION

The digital trunk resources of the Media Gateway (2 Bit) have discovered an error in that PCM receiving circuit has received more than 3 faulty frame synchronization words in succession. All initiated units on the board have been blocked. An alarm indication has been sent to the interworking equipment.

The alarm will be cancelled if more than 2 correct frame synchronization words are obtained in succession.

The digital trunk resources of the Media Gateway (1.5 Bit) have discovered that the out of frame, loss of signal or alarm indication signal persists for 2.5 s. All initiated individuals on the virtual board will be blocked. An alarm indication has been sent to the interworking equipment.

The alarm will be cancelled if frame synchronization are obtained in succession for 15 seconds.

#### 1.62.2

##### MEASURE

1. Change the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
2. Has the alarm returned?
3. YES: probably a fault on the line or interworking exchange/public exchange. Inform the instance responsible for the line.

## 1.63 FAULT CODE 270 - DIGITAL TRUNK, BIT ERROR IN FRAME SYNCHRONIZATION WORD

### 1.63.1 FAULT CODE DESCRIPTION

The digital trunk resources of the Media Gateway have discovered an error, that the PCM receiving circuit has received more than circa 900 checksum errors within one minute. This will generate fault code 269, and an attempt to find new synchronization. If alarm 269 remains for a period of at least 100 milliseconds, alarm 270 will be generated. All initiated lines on the virtual board will be blocked. An alarm indication has been sent to the interworking equipment. The alarm is acknowledged by the system if the frame synchronization error has ceased. (See fault locating directions for *FAULT CODE 269*.)

### 1.63.2 MEASURE

1. Restart the virtual trunk board by entering the command *board\_restart*.
2. Has the alarm returned?
3. YES: Replace the Media Gateway or the TLU board in MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: probably a fault on the line or in interworking exchange/public exchange. Inform the instance responsible for the line.
6. Return to the main flow.

## 1.64 FAULT CODE 271 - DIGITAL TRUNK, RECEIVED ALARM FROM REMOTE END

### 1.64.1 FAULT CODE DESCRIPTION

An alarm indication in time slots 0 and 16 is obtained when the interworking equipment detects a fault synchronization error, alarm indication signal, bit error (time slot 0) and multiframe synchronization error (time slot 16). All individuals on the virtual board will be blocked automatically. The alarm will be erased on removal of the alarm indication in time slots T0 and T16.

For digital trunk resources (1.5 Bit), the alarm indicates a remotely detected loss of synchronization (Yellow, ITU-T) and loss of signal frames in DMI mode (Remote Multiframe Alarm). All individuals on the virtual board will be blocked automatically. The alarm will be erased on removal of the alarm indication for 150 ms (Yellow, ITU-T) and for 1 s (Remote Multiframe Alarm).

#### ADD INFO 2

- 0 Synchronization error in time slot 0.
- 1 Multiframe synchronization error in time slot 16.

- 2 Yellow alarm (ITU-T).
- 3 Remote multiframe alarm.

## 1.64.2

## MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway type is located over the fan unit.
2. YES: Change to an other virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. NO: Replace the Trunk Line Unit.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: Consult an expert.

## 1.65

## FAULT CODE 272 - DIGITAL TRUNK, LOSS OF MULTI-FRAME SYNCHRONIZATION

## 1.65.1

## FAULT CODE DESCRIPTION

The digital trunk resources of the Media Gateway have discovered an error in the multi-frame synchronization word. The Media Gateway sends an alarm indication towards the interworking equipment. If the error ceases, the system will acknowledge. All initiated individuals on the virtual board will be blocked automatically. The alarm will be erased when the digital trunk resources (2 Bit) detect more than two successive multiframe synchronization words.

For digital trunk resources (1.5 Bit), the alarm will be erased when the Media Gateway detects successive multiframe synchronization words for 15 sec.

## 1.65.2

## MEASURE

Inform instance responsible for the line.

## 1.66

## FAULT CODE 274 - DIGITAL TRUNK, CLOCK MALFUNCTION (SLIP)

## 1.66.1

## FAULT CODE DESCRIPTION

The synchronization error (slip) occurs when the clock rates on sides A and B differ. An alarm is generated in the LIM or interworking exchange or public exchange if the number of slips exceeds 10 in 70 days, for the master link and 10 per hour for non master links. All initiated individuals on the virtual board will automatically be blocked.

## 1.66.2

## MEASURE

1. Replace the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
2. Has the alarm returned?
3. YES: probably a fault on the line or in the interworking exchange/public exchange. Inform the instance responsible for the line.

## 1.67

## FAULT CODE 275 - STATISTIC SUPERVISION, TOO SHORT SEIZURE OF TRUNK

### 1.67.1

### FAULT CODE DESCRIPTION

The time a trunk is seized is measured for each line, and if it falls below the time set in the DIST parameter, then the call is registered as a disturbance.

The statistical supervisory function uses two parameters: DIST which is defined for external lines, and DISL which is defined for routes. The disturbance level is the value that a line is allowed to reach before an alarm is generated. This alarm is generated by the MX-ONE Service Node SW, that is, the Media Gateway is not involved in generating the alarm.

#### ADD INFO 1

States pointer to data individual.

### 1.67.2

### MEASURE

1. Are the DIST and DISL values reasonable? Key the command *ROCAP* to check.
2. NO: Key the command *ROCAC* to set new *DIST* and *DISL* values.
  - Key the command *alarm* to erase (reset) alarms in the alarm log.
  - Wait and see if the alarm recurs.
  - Key command *alarm* to print (list) alarms in the alarm log.
  - Did the alarm recur?
  - YES: Key the command *board\_restart* to restart the virtual trunk board.
  - Wait and see if the alarm recurs.
  - Key command *alarm* to print (list) alarms in the alarm log.
  - Did the alarm recur?
3. YES: Replace the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

4. Wait and see if the alarm recurs.  
Key command *alarm* to print (list) alarms in the alarm log.
5. Did the alarm recur?
6. YES: probable cause: Fault on the line or in the interworking PBX/public exchange.
7. Inform the person responsible for external line operation.
8. If necessary, block the line.

## 1.68 FAULT CODE 276 - NO CONNECTION WITH PAGING EQUIPMENT

### 1.68.1 FAULT CODE DESCRIPTION

Expected answer signal fails to arrive or blocking information is received from the paging equipment.

#### **ADD INFO 1**

States paging channel.

### 1.68.2 MEASURE

1. Has the paging equipment lost its power feeding?
2. YES: verify the reason and take the necessary actions.
3. NO: verify the connection between the PBX and the paging equipment.
4. Does the fault remain?
5. YES: verify that exchange data in parameter VAR agree with the functions of the peripheral paging equipment.  
See parameter description for *MML COMMANDS*.
6. Do the data agree?
7. NO: alter values in parameter VAR.
8. YES: Replace the TLU-board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
9. Does the original fault remain?
10. YES: Fault in peripheral paging equipment.
11. Call a specialist.



## 1.69 FAULT CODE 277 - SUPERVISION VALUE EXCEEDED FOR PAGING EQUIPMENT

### 1.69.1 FAULT CODE DESCRIPTION

For each paging calls the time until transmission of the call to the paging equipment is measured. An average of these times is calculated per paging sector for each 15 minute period. If the average queue time for any paging sector exceeds a preset limit value set via command the alarm will be issued.

The alarm indicates that, due to incorrect dimensioning or blocking of paging equipment, the PBX is unable to transmit paging calls with the required degree of efficiency.

#### **ADD INFO 1**

States paging area.

#### **ADD INFO 2**

States mean waiting time.

#### **ADD INFO 3**

Defined value.

### 1.69.2 MEASURE

1. Has any fault occurred earlier?
2. YES: take no action if the fault is temporary.
3. NO: Use the command *PAEDP* and the command *block\_list* to verify whether the channels to the relevant paging sector are blocked.
4. Key the command *deblock*, if necessary, to deblock the channels. Use test connections to verify that the channels can be used.
5. Are the channels fully available?
6. NO: Fault in paging equipment. See also the fault locating directions for *FAULT CODE 276*.
7. YES: verify whether it is possible to initiate more channels to the paging sector, possibly by removing channels from another paging sector.
8. Is it possible to increase the number of channels?
9. YES: increase the number of channels for the paging sector. See operational directions for *PAGING*.
10. Can a higher alarm limit be tolerated?
11. YES: Key the command *global\_traffic\_data -c* to increase the alarm limit.
12. NO: verify whether the number of paging receivers with the given paging sector can be reduced or whether the paging equipment should be expanded or more equipment be procured.

## 1.70 FAULT CODE 280 - DIGITAL TRUNK, UNAUTHORIZED CHARGING PULSE

### 1.70.1 FAULT CODE DESCRIPTION

The fault code is used in digital external lines and indicates whether a faulty digital pattern for the charging pulse has been received. the fault is probably in the public exchange.

### 1.70.2 MEASURE

1. Inform the instance responsible for the line.
2. Block the line if necessary.

## 1.71 FAULT CODE 281 - QUALITY ERROR IN INTERFACE TO ICS COMPUTER

### 1.71.1 FAULT CODE DESCRIPTION

An information system can be in the form of an interception computer, a voice mail system or a text message system.

The interface between the MX-ONE Service Node and the information system is supervised with respect to status (see fault locating directions for *FAULT CODE 282*), quality (see fault locating directions for *FAULT CODE 281*) and character processing (see fault locating directions for *FAULT CODE 298*).

Quality checking means checking the reasonableness of each signal received by the MX-ONE Service Node from the information system. A signal is considered reasonable when all its characters are of the expected type, i.e. letters or digits.

An alarm is generated when a consecutive number of signals are identified as erroneous. The alarm is acknowledged when a consecutive number of correct signals have been received.

Quality checking is always performed continuously for each information system.

A prerequisite for alarm handling is that manuals for the information system concerned are available.

### 1.71.2 MEASURE

1. Check that the information system is not in an abnormal state which results in sending of unverifiable signals.  
Consult the manuals of the information system and/or activate test functions (if available).
2. Does the information system function properly?
3. NO: eliminate the fault and make sure that the user configuration is correct.  
See the manual of the information system.

4. Does the cable that interconnects the MX-ONE Service Node and the information system pass any point that may cause interference?
5. YES: Correct the cabling.

6. To check whether the alarm is still activated, key the command *ICUPI* for updating of the information system concerned.

A prerequisite for this is that a number of extensions have unrecorded messages in the information system and that the traffic through the MX-ONE Service Node is low.

7. Does the alarm remain?
8. YES: Consult an expert.
9. Return to the main flow.

## 1.72

## FAULT CODE 282 - STATUS ERROR IN INTERFACE TO ICS COMPUTER

### 1.72.1

#### FAULT CODE DESCRIPTION

An information system can be in the form of an interception computer, a voice mail system or a text message system.

The interface between the MX-ONE Service Node and the information system is supervised with respect to status (see fault locating directions for *FAULT CODE 282*), quality (see fault locating directions for *FAULT CODE 281*) and character processing (see fault locating directions for *FAULT CODE 298*).

Status checking means supervision of circuit 108 in the V.24 interface and heartbeat check to information system (if applicable). An alarm is generated when circuit 108 is OFF. An alarm is also generated if there is no response to the heartbeat check.

The status checking is continuous for each information system because the connection between the MX-ONE Service Node and the information system is to be permanent.

A prerequisite for alarm handling is that manuals for the information system concerned are available.

### 1.72.2

#### MEASURE

1. Use an interface tester to check that the information system sets circuit 108 to ON.  
Consult the manuals of the information system and/or activate test functions (if any).
2. Does the information system set circuit 108 to ON?
3. NO: Correct the fault in the information system. See the manual of the information system.
  - Does the alarm remain?
  - YES: Consult an expert.
  - NO: Command *ICUPI* should be keyed for updating of the information system concerned. A prerequisite for this is that the traffic through the MX-ONE Service Node is low.
  - Return to the main flow.
4. YES: Check the cable between the MX-ONE Service Node and the information system for breaks or loose contacts.

5. Is the cable intact?
6. NO: Repair or change the cable.
  - Does the alarm remain?
  - YES: Consult an expert.
  - NO: Command *ICUPI* should be keyed for updating of the information system concerned. A prerequisite for this is that the traffic through the MX-ONE Service Node is low.
  - Return to the main flow.
7. If YES: Does the information system signaling format perform a heart-beat check? Consult Operation and maintenance manuals.
8. NO: Consult an expert.
9. YES: The information system is at fault. Correct information system or consult an expert.  
 Consult the manuals of the information system and/or activate test functions (if any).  
 Return to the main flow.

## 1.73 FAULT CODE 283 - CONGESTION VALUE FOR KEYCODE RECEIVER REACHED

### 1.73.1 FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device
- a temporary high traffic flow
- the PBX is underdimensioned.

The following data can be read in the printout from the MX-ONE SN for this fault code:

#### **UNIT**

States the program unit that administers the function tone code receiver.

#### **ADD INFO 1**

States recorded congestion value in o/oo.

#### **ADD INFO 2**

States internal device record.

#### **ADD INFO 3**

States defined congestion value in o/oo.

## 1.73.2

## MEASURE

Key the command *block\_list* to verify that the device is blocked.

## 1.73.2.1

*Device is blocked*

1. Key the command *deblock* to deblock the device and key command *alarm* to erase (reset) alarms in the alarm log.
2. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
3. Alarm has returned?
4. YES: Replace the TMU-board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
5. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
6. Alarm has returned?
7. YES: Consult an expert.

## 1.73.2.2

*Device is not blocked*

1. Traffic measurement in progress at device?
2. NO: Key the command *TRKRI* to initiate traffic measurement and wait for measurement result.
3. YES: Key the command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the MX-ONE SN to determine how the alarm should be dealt with, that is:
  - No action
  - The MX-ONE Classic needs to be redimensioned.  
Add more TMU boards.

## 1.74

## FAULT CODE 284 - CONGESTION VALUE FOR TONE RECEIVER REACHED

## 1.74.1

## FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device

- a temporary high traffic flow
- the PBX is underdimensioned.

The following data are provided in the printout supplied by the MX-ONE SN for this fault code:

**UNIT**

States the program unit that administers the tone receiver function.

**ADD INFO 1**

States recorded congestion value in o/oo.

**ADD INFO 2**

States internal device record.

**ADD INFO 3**

States defined congestion value in o/oo.

## 1.74.2

### MEASURE

Key the command *block\_list* to verify that the device is blocked.

#### 1.74.2.1

##### *Device is blocked*

1. Key the command *deblock* to deblock the device and key the command *alarm* to erase (reset) relevant alarm.
2. After 15 minutes key command *alarm* to print (list) alarms in the alarm log to verify that the alarm has not returned.
3. Alarm has returned?
4. YES: Replace the TMU-board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
5. After 15 minutes key command *alarm* to print (list) alarms in the alarm log to verify that the alarm has not returned.
6. Alarm has returned?
7. YES: Consult an expert.

#### 1.74.2.2

##### *Device is not blocked*

1. Traffic measurement in progress at device?
2. NO: Key the command *TRTRI* to initiate traffic measurement and wait for measurement result.
3. YES: Key the command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the MX-ONE SN to determine how the alarm shall be dealt with, that is:
  - No action
  - The MX-ONE MX-ONE Classic needs to be redimensioned  
Add more TMU boards.

## 1.75

## FAULT CODE 285 - CONGESTION VALUE FOR CS (MFC) REACHED

## 1.75.1

## FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device
- a temporary high traffic flow
- the PBX is underdimensioned.

The printout from the PBX contains the following data for this fault code:

**UNIT**

States the program unit that administers the MFC-sender function

**ADD INFO 1**

States recorded congestion value in o/oo.

**ADD INFO 2**

States internal device record.

**ADD INFO 3**

States defined congestion value in o/oo.

## 1.75.2

## MEASURE

1. Key command *block\_list* to verify that the device is blocked.
2. NO: Traffic measurement in progress at device?
  - NO: Key command *TRCSI* to initiate traffic measurement and wait for measurement result.
  - YES: Key command *TRREP* to verify traffic measurement data.  
 Contact person responsible for the PBX to determine how the alarm shall be dealt with, that is:
    - No action.
    - PBX needs to be redimensioned.
  - Return to the main flow.
3. YES: Key command *deblock* to deblock the device and key command *alarm* to erase (reset) alarms in the alarm log.
4. After 15 minutes key command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
5. Alarm has returned?
6. YES: Replace MSU-board.



See operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.

7. After 15 minutes key command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
8. Alarm has returned?
9. YES: Consult an expert.  
Return to the main flow.

## 1.76 FAULT CODE 286 - CONGESTION VALUE FOR CR (MFC) REACHED

### 1.76.1 FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device
- a temporary high traffic flow
- the PBX is underdimensioned.

The following data are provided in the printout supplied by the PBX for this fault code.

#### UNIT

States the program unit that administers the MFC-sender function

#### ADD INFO 1

States recorded congestion value in o/oo.

#### ADD INFO 2

States internal device record.

#### ADD INFO 3

States defined congestion value in o/oo.

### 1.76.2 MEASURE

1. Key command *block\_list* to verify that the device is blocked.
2. NO: traffic measurement in progress at device?
  - NO: Key command *TRCRI* to initiate traffic measurement and wait for measurement result
  - YES: Key command *TRREP* to verify traffic measurement data
  - Contact person responsible for the PBX to determine how the alarm shall be dealt with, that is:
    - No action
    - PBX needs to be redimensioned

3. YES: Key command *deblock* to deblock the device and key command *alarm* to erase (reset) alarms in the alarm log.
4. After 15 minutes key command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
5. Alarm has returned?
6. YES: Replace MSU-board.  
See operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.
7. After 15 minutes key command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
8. Alarm has returned?
9. YES: Consult an expert.

## 1.77

## FAULT CODE 287 - CONGESTION SUPERVISION VALUE REACHED FOR PCM-LINE

### 1.77.1

#### FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit 1/100.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to:

- A faulty device
- A temporary high traffic flow
- The PBX is underdimensioned.

An unsuccessful seizure attempt means that no free time slot has been obtained.

The following data can be read in the printout from PBX for this fault code:

#### UNIT

The program unit that administers the function PCM-line

#### ADD INFO 1

Recorded congestion value in o/oo.

#### ADD INFO 2

Internal device record.

#### ADD INFO 3

Defined congestion value in o/oo.

### 1.77.2

#### MEASURE

Key the command *block\_list* to verify that the device is blocked.

### 1.77.2.1

#### *Device is blocked*

1. Key the command *deblock* to deblock the device and key the command alarm to erase (reset) relevant alarm.
2. After 15 minutes key command *alarm* to print (list) alarms in the alarm log to verify that the alarm has not returned.
3. Alarm has returned?
4. YES: Replace GJU-board.  
See operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.
5. After 15 minutes key command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
6. Alarm has returned?
7. YES: Consult an expert.  
Return to the main flow.

### 1.77.2.2

#### *Device is not blocked*

1. Traffic measurement in progress?
2. NO: Key command *TRPLI* to initiate traffic measurement and wait for measurement result.
3. YES: Key command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the MX-ONE SN to determine how the alarm shall be dealt with, that is:
  - No action
  - PBX needs to be redimensioned
5. Return to the main flow.

## 1.78

## FAULT CODE 288 - CONGESTION VALUE FOR CONFERENCE REACHED

### 1.78.1

#### FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device
- a temporary high traffic flow
- the MX-ONE Service Node is underdimensioned.

The printout from the MX-ONE Service Node contains the following data for this fault code:

**UNIT**

The program unit that administers the conference function

**ADD INFO 1**

Recorded congestion value in o/oo.

**ADD INFO 2**

Internal device record.

**ADD INFO 3**

Defined congestion value in o/oo.

## 1.78.2

### MEASURE

Key the command *block\_list* to verify that the device is blocked.

#### 1.78.2.1

##### *Device is blocked*

1. Key the command *deblock* to deblock the device and key the command *alarm* to erase (reset) relevant alarm.
2. After 15 minutes key command *alarm* to print (list) alarms in the alarm log to verify that the alarm has not returned.
3. Alarm has returned?
4. YES: after 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned
5. Alarm has returned?
6. YES: Consult an expert.  
Return to the main flow.

#### 1.78.2.2

##### *Device is not blocked*

1. Is traffic measurement in progress at device?
2. NO: Key the command *TRCOI* to initiate traffic measurement and wait for measurement result.
3. YES: Key the command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the MX-ONE Service Node to determine how the alarm shall be dealt with, that is:
  - No action
  - The MX-ONE Service Node needs to be redimensioned
5. Return to the main flow.

## 1.79 FAULT CODE 289 - CONGESTION VALUE FOR COMMON BELL REACHED

### 1.79.1 FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo (per thousandth).

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of seizure attempts that do not reach the common bell group for each even quarter.

Provided that the used congestion value is relevant the alarm can be caused by

- a temporary high traffic flow
- an underdimensioned common bell group (number of group members, queue length) in relation to the number of calls.

The printout from the PBX contains the following data for this fault code:

#### **UNIT**

The program unit that administers the common bell function

#### **ADD INFO 1**

Recorded congestion value in o/oo.

#### **ADD INFO 2**

Internal supervision record.

#### **ADD INFO 3**

Defined congestion value in o/oo.

### 1.79.2 MEASURE

1. Is traffic measurement in progress at the device?
2. NO: Key the command *TRCBI* to initiate traffic measurement and wait for the measurement result.
3. YES: Key the command *TRREP* to verify the traffic measurement data.
4. Contact the person responsible for the PBX to determine how the alarm shall be handled, that is:
  - The Common bell group needs to be redimensioned.
5. Return to the main flow

## 1.80 FAULT CODE 290 - CONGESTION VALUE FOR ROUTE REACHED

### 1.80.1 FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty line in the route
- a temporary high traffic flow
- an underdimensioned route.

The printout from the system contains the following data for this fault code:

**UNIT**

The program unit that administers the route function

**ADD INFO 1**

Recorded congestion value in o/oo.

**ADD INFO 2**

The route number subjected to congestion monitoring.

**ADD INFO 3**

Defined congestion value in o/oo.

## 1.80.2

### MEASURE

1. Key the command *ROEDP* to verify which external lines belong to the route.
2. Key the command *block\_list* to find blocked line (if any) in route.

### 1.80.2.1

#### *Device is blocked*

1. Key the command *deblock* to deblock the line and key command *alarm* to erase (reset) relevant alarms in the alarm log.
2. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that the alarm has not returned.
3. Has the alarm returned?
4. YES: Replace the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
5. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that the alarm has not returned.
6. Has the alarm returned?
7. YES: Consult an expert.
8. Return to the main flow.

### 1.80.2.2

#### *Device is not blocked*

1. Is traffic measurement in progress at device?
2. NO: Key the command *TRROI* to initiate traffic measurement and wait for measurement result.
3. YES: Key the command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the PBX to determine how the alarm shall be dealt with, that is:
  - No action
  - Route needs to be redimensioned
  - The set congestion value shall be altered with command *TRRSI*.
5. Return to the main flow.

## 1.81

## FAULT CODE 292 - TRAFFIC RECORDING DATA DUMP COULD NOT BE EXECUTED

### 1.81.1

#### FAULT CODE DESCRIPTION

This fault code is obtained when the system has attempted to dump traffic recording data and failed for any one of the reasons detailed on the flow diagram. The temporary memory contents have not been erased at this point, and another attempt will be made to dump the data onto the system storage device on the next data storage operation cycle.

The following information is given in the printout from the exchange for this fault code:

#### **ADD INFO 1**

States the reason for the fault.

## 1.81.2

## MEASURE

1. Does the fault printout show any of the following values for ADD INFO 1?
  - 1 User interrupt. Current *TRREP* operation is conflicting with the dump attempt.
  - 11 File system record congestion.
  - 25 Working directory is being changed. Unable to access system file table.
  - 28 Directory for file cannot be extended or no free space remaining on the device to contain the file. Copy (optionally) old traffic recording data results files to another storage medium and delete.

Traffic recording data dump will be retried on the next data storage operation.  
Return to the main flow.

2. NO: Does ADD INFO 1 = any of the following?
  - 2 Failure to create file. File does not exist and the file status is not set to create, or a component of path prefix does not exist.
  - 3 I/O unit is blocked.
  - 4 Signal interrupt during system write.
  - 5 I/O error.
  - 6 Request is outside of the capabilities of the device.
  - 7 User unknown.
  - 8 No contact with stated node.
  - 9 File descriptor not valid.
  - 13 Access to file denied.
  - 14 Path points outside of addressing space.
  - 17 File exists. Not created.
  - 20 File path not valid.
  - 23 System file table full. Maximum number of files already open.
  - 27 Attempt made to write file exceeding the maximum file size
  - 31 LIM communication fault or lost signal.
  - 32 Buffer congestion.

YES: Consult an expert.

3. NO: Undefined error. Consult an expert.
4. Does the fault printout show any of the following values for ADD INFO 1?
  - 1 User interrupt. Current *TRREP* operation is conflicting with the dump attempt.
  - 11 File system record congestion.
  - 25 Working directory is being changed. Unable to access system file table.
  - 28 Directory for file cannot be extended or no free space remaining on the device to contain the file. Copy (optionally) old traffic recording data results files to another storage medium and delete.
5. NO: Does ADD INFO 1 = any of the following?
  - 2 Failure to create file. File does not exist and the file status is not set to create, or a component of path prefix does not exist.
  - 3 I/O unit is blocked.
  - 4 Signal interrupt during system write.



- 5 I/O error.
- 6 Request is outside of the capabilities of the device.
- 7 User unknown.
- 8 No contact with stated node.
- 9 File descriptor not valid
- 13 Access to file denied.
- 14 Path points outside of addressing space.
- 17 File exists. Not created.
- 20 File path not valid.
- 23 System file table full. Maximum number of files already open.
- 27 Attempt made to write file exceeding the maximum file size.
- 31 LIM communication fault or lost signal.
- 32 Buffer congestion.

YES: Consult an expert.

- 6. NO: Undefined error. Consult an expert.

## 1.82 FAULT CODE 293 - TRAFFIC RECORDING INTERNAL MEMORY DATA ERASED, MEMORY FULL

### 1.82.1 FAULT CODE DESCRIPTION

This fault code is obtained when the system has failed to dump traffic recording data due to any of the reasons given on the flow diagram. Data in the internal memory was lost due to memory space overwritten by new traffic recording data.

The following information is given in the printout from the exchange for this fault code:

#### **ADD INFO 1**

States the reason for the fault.

### 1.82.2 MEASURE

1. Does fault printout show any of the following values for ADD INFO 1?
  - 1 User interrupt. Current *TRREP* operation is conflicting with the dump attempt.
  - 11 File system record congestion.
  - 25 Working directory is being changed. Unable to access system file table.
  - 28 Directory for file cannot be extended or no free space remaining on the device to contain the file. Copy (optionally) old traffic recording data results files to another storage medium and delete.
2. YES: Return to main flow.
3. NO: Does ADD INFO 1 = any of the following?
  - 2 Failure to create file. File does not exist and the file status is not set to create, or a component of path prefix does not exist.
  - 3 I/O unit is blocked.

- 4 Signal interrupt during system write.
  - 5 I/O error.
  - 6 Request is outside of the capabilities of the device.
  - 7 User unknown.
  - 8 No contact with stated node.
  - 9 File descriptor not valid
  - 13 Access to file denied.
  - 14 Path points outside of addressing space.
  - 17 File exists. Not created.
  - 20 File path not valid.
  - 23 System file table full. Maximum number of files already open.
  - 27 Attempt made to write file exceeding the maximum file size
  - 31 LIM communication fault or lost signal.
  - 32 Buffer congestion.
- 4. YES: Consult an expert.
  - 5. NO: Undefined error. Consult an expert.

## 1.83

## FAULT CODE 294 - TRAFFIC RECORDING INTERNAL MEMORY DATA ERASED, MIDNIGHT DUMP

### 1.83.1

#### FAULT CODE DESCRIPTION

This fault code is obtained when the system has failed to dump traffic recording data on the day's last storage operation for any one of the reasons given on the flow diagram. Internal memory contents will be overwritten by the new days data.

The following information is given in the printout from the exchange for this fault code:

#### **ADD INFO 1**

States the reason for the fault.

### 1.83.2

#### MEASURE

- 1. Does fault printout show any of the following values for ADD INFO 1?
  - 1 User interrupt. Current *TRREP* operation is conflicting with the dump attempt.
  - 11 File system record congestion.
  - 25 Working directory is being changed. Unable to access system file table.
  - 28 Directory for file cannot be extended or no free space remaining on the device to contain the file. Copy (optionally) old traffic recording data results files to another storage medium and delete.
- 2. YES: Return to main flow.
- 3. NO: Does ADD INFO 1 = any of the following?
  - 2 Failure to create file. File does not exist and the file status is not set to create, or a component of path prefix does not exist.

- 3 I/O unit is blocked.
  - 4 Signal interrupt during system write.
  - 5 I/O error.
  - 6 Request is outside of the capabilities of the device.
  - 7 User unknown.
  - 8 No contact with stated node.
  - 9 File descriptor not valid
  - 13 Access to file denied.
  - 14 Path points outside of addressing space.
  - 17 File exists. Not created.
  - 20 File path not valid.
  - 23 System file table full. Maximum number of files already open.
  - 27 Attempt made to write file exceeding the maximum file size
  - 31 LIM communication fault or lost signal.
  - 32 Buffer congestion.
- 4. YES: Consult an expert.
  - 5. NO: Undefined error. Consult an expert.

## 1.84

## FAULT CODE 295 - CALENDAR TIME ACTIVATION REQUEST DENIED

### 1.84.1

### FAULT CODE DESCRIPTION

This fault code is obtained when an unsuccessful request from the traffic recording function for a system (calender) time indication is made. A prerequisite for the traffic recording function to work in an MX-ONE Service Node is that it receives continuous calender time updating. This updating is provided by the operating system.

The traffic recording requests to get continuous updates of the system (calender) time, that shall take place once per minute from the operating system, with the help of a "program signal", that contains date and time information.

The following data can be read in the printout from the MX-ONE Service Node for this fault code:

#### ADD INFO 2

- 0 No individual free.
- 1 (Not used)
- 2 Incorrect ordering signal.
- 3 (Not used)
- 4 Request initiated already

### 1.84.2

### MEASURE

- 1. Key the command *date* to check system time and date.

System time is set when the Linux OS is started.

2. Congestion in calendar time handling program, or a coding error in requesting program.

ADDINFO 2 = 0 / 2 / 4.

3. Consult an expert.

## 1.85

## FAULT CODE 296 - CONGESTION VALUE FOR KEYCODE SENDER REACHED

### 1.85.1

### FAULT CODE DESCRIPTION

This fault code is obtained when the volume of unsuccessful seizure attempts, congestion, relative to the total volume, reaches or exceeds a predetermined congestion value. The congestion value is stated in unit o/oo.

Calculation of the real congestion value is made based on the total number of seizure attempts and the total number of unsuccessful seizure attempts for each even quarter.

Provided that the used congestion value is relevant the alarm can be due to

- a faulty device
- the PBX is underdimensioned
- a temporary high traffic flow.

The printout from the MX-ONE SN contains the following data for this fault code:

#### UNIT

The program unit that administers the tone code-sender function

#### ADD INFO 1

Recorded congestion value in o/oo.

#### ADD INFO 2

Internal device record.

#### ADD INFO 3

Defined congestion value in o/oo.

### 1.85.2

### MEASURE

Is the device blocked? Key the command *block\_list* to verify.

#### 1.85.2.1

#### *Device is blocked*

1. Key the command *deblock* to deblock the device and command alarm to erase (reset) relevant alarms in the alarm log.
2. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
3. Alarm has returned?
4. YES: Replace the TMU-board.

See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

5. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log and verify that alarm has not returned.
6. Alarm has returned?
7. YES: Consult an expert. Return to the main flow.

#### 1.85.2.2

*Device is not blocked*

1. Traffic measurement in progress at device?
2. NO: Key the command *TRKSI* to initiate traffic measurement and wait for measurement result.
3. YES: Key the command *TRREP* to verify traffic measurement data.
4. Contact the person responsible for the MX-ONE Service Node to determine how the alarm should be dealt with, that is,:
  - No action
  - MX-ONE Service Node needs to be redimensioned.
5. Return to the main flow.

## 1.86

## FAULT CODE 297 - LOSS OF POWER (-60 V)

### 1.86.1

### FAULT CODE DESCRIPTION

Disturbance in the -60 V feed to the C-wire.

### 1.86.2

### MEASURE

1. Key command *block* to block the TLU board.
2. Check if power is fed through the cable to the board.
3. Is there any power?
4. YES: Change the board.  
See operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.
5. Key command *board\_restart* to restart the new board
6. NO: Change the voltage converter.
7. Key command *deblock* to deblock the board.
8. Key command *alarm* to erase (reset) the alarm state for the line.
9. Await the possible reappearance of the alarm.
10. Did the alarm reappear?
11. YES: Start again from the beginning of this flow.

## 1.87

## FAULT CODE 298 - CHARACTER ERROR IN THE INTERFACE TO INFORMATION COMPUTER SYSTEM

## 1.87.1

## FAULT CODE DESCRIPTION

An information system may be in the form of an interception computer, a voice mail system or a text message system.

The interface between the MX-ONE Service Node and the information system is supervised with respect to status (see fault locating directions for *FAULT CODE 282*), quality (see fault locating directions for *FAULT CODE 281*), and character processing (see fault locating directions for *FAULT CODE 298*).

Character checking means that all characters used in the signals sent from the information system to the MX-ONE Service Node are checked as follows:

- Parity  
A command is entered to select checking on odd parity, checking on even parity, or no checking. Characters with erroneous parity are “reset”, which means that the signal in which the character is contained is interpreted as incorrect.
- Character overlay  
This means that the MX-ONE Service Node does not have time to attend to a character before the next one arrives. The reason for this may be too high data transmission speed in the interface between the MX-ONE Service Node and the information system.
- Incorrect data transmission speed  
Data is transmitted to the MX-ONE Service Node at a speed other than that for which the MX-ONE Service Node is programmed. The reason for this may be that the speed value set in the MX-ONE Service Node and in the information system do not tally.

An alarm is generated when a consecutive number of characters are identified as erroneous in one or more of the above mentioned situations. The alarm is acknowledged after a consecutive number of correct characters have been received. Character checking is selectable by command for each information system.

A prerequisite for alarm handling is that manuals for the information system concerned are available.

## 1.87.2

## MEASURE

1. Should character checking be activated?
2. NO: ignore the alarm and cancel the character checking function.  
See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*.  
Return to the main flow.
3. YES: Has parity checking been initiated (odd or even)?  
See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*.
4. NO: Continue to step 9.
5. Check that the parities set in the MX-ONE Service Node and in the information system agree.

See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*.

6. Do the parities agree?

7. YES: Continue to step 9.

8. NO: See to it that the parities agree.

See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*.

9. Check that the data transmission speeds set in the MX-ONE Service Node and in the information system agree.

10. Do the data transmission speeds agree?

11. NO: Continue to step 13.

12. YES: See to it that the data transmission speeds agree.

See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*

13. Check that the data transmission speed between the MX-ONE Service Node and the information system is not too high.

See interworking description for the information system concerned.

14. Is the data transmission speed too high?

15. NO: Continue to step 17.

16. YES: See to it that the data transmission speed is lowered.

See the command description for *MML COMMAMDS, INFORMATION SYSTEMS*

17. Check whether the alarm is still activated by keying the command ICUPI to request updating from the information system concerned.  
A prerequisite for this check is that a number of extensions have unreproduced messages in the information system and that the traffic through the MX-ONE Service Node is low.
18. Does the alarm remain?
19. YES: Consult an expert.  
Return to the main flow.

## 1.88 FAULT CODE 299 - DIGITAL TRUNK, WRONG PATTERN RECEIVED IN IDLE STATE

### 1.88.1 FAULT CODE DESCRIPTION

Wrong bit pattern has been received in idle state. The fault remains until release guard is received.

#### **ADD INFO 1**

Pointer to the interface.

### 1.88.2 MEASURE

Inform the instance responsible for the line.

## 1.89 FAULT CODE 300 - DIGITAL TRUNK, SEIZURE ACKNOWLEDGEMENT NOT RECEIVED

### 1.89.1 FAULT CODE DESCRIPTION

Seize acknowledgement has not been received within the stipulated time or bit b in the signal scheme = 0 before the end of selection signal has been received. The fault remains until a seize acknowledgement is received or when a release guard is received.

### 1.89.2 MEASURE

Inform the instance responsible for the line. Return to the main flow.

## 1.90 FAULT CODE 301 - DIGITAL TRUNK, WRONG BIT PATTERN RECEIVED AFTER DISCONNECTION

### 1.90.1 FAULT CODE DESCRIPTION

A wrong bit pattern has been received after disconnection. The fault remains until a proper disconnection signal (release guard) is received.



## 1.90.2

### MEASURE

Inform the instance responsible for the line. Return to the main flow.

## 1.91

### FAULT CODE 302- DIGITAL TRUNK, WRONG BIT PATTERN RECEIVED IN REGISTRATION STATE

#### 1.91.1

##### FAULT CODE DESCRIPTION

Bit b in the signal scheme = 1 in 1 - 2 seconds after seize acknowledgement has been sent and before end of selection has been sent. The fault remains until clear forward is received.

#### 1.91.2

##### MEASURE

Inform the instance responsible for the line. Return to the main flow.

## 1.92

### FAULT CODE 303- ISDN DATA LINK ALARM

#### 1.92.1

##### FAULT CODE DESCRIPTION

The TLU-board has discovered an error on the data link layer and has informed layer 3. Layer 3 has analyzed the type of error and according to type some action is performed.

Possible actions are, request link restart, send alarm and block board. Assumption is that cause for alarm will expire after a while. The alarm will be acknowledged when the TLU-board receives information from the other side that the data link layer is in right state. Layer 3 will be informed by primitive that the data link is established again.

##### ADD INFO 1

Pointer to the interface.

##### ADD INFO 2

- 0 G fault, Unsuccessful data link establishment.
- 1 H fault, No DL (Data Link) -RELEASE acknowledgement.
- 2 Maximum retransmit count exceeded.
- 3 J fault, Invalid received sequence number.
- 4 K fault, Frame reject response.
- 5 A fault, Not expected supervisory response.
- 6 B, C, D, E fault, Not expected UA (Unnumbered Acknowledgement or DM (Disconnected Mode) response.
- 7 F fault, SABME (Set Asynchronous Balanced Mode Extended) from peer received.
- 8 Q fault, Blocking received.
- 9 R fault, DM (Disconnected Mode) response received.
- 10 I fault, No response on RR (Receiver Ready) or RNR (Receiver Not Ready).
- 11 O fault, Received information field > N201 (260 Octets)

- 12 L fault, Undefined control field.
- 13 N fault, Received frame with incorrect length.
- 14 M fault
- 15 P fault, N2X4, Maximum number of retransmission of RNR frames exceeded.
- 18 TEI Removal received.
- 26 TEI Removal received.

## 1.92.2

## MEASURE

1. Another alarm connected to this interface exists in the alarm log?
2. YES: Consult fault location direction for that fault code.
3. NO: inform the instance responsible for the line. Return to the main flow.

## 1.93

## FAULT CODE 305- BLOCKED TRUNK LINE BY A MANUAL SWITCH ON THE BOARD

## 1.93.1

## FAULT CODE DESCRIPTION

The alarm is generated in the following situation:

- The manual blocking switch on the hardware has been pressed.

**ADD INFO 1**

Faulty TRS-individual pointer.

## 1.93.2

## MEASURE

1. Is the blocking lamp on the board lighting?
2. NO: Replace the board and press the manual switch on the new board.
3. Is the blocking-lamp on the board lighting?
4. NO: Consult an expert.
5. YES: Unblock the line (if that is desired) by pressing the switch on the board.

## 1.94

## FAULT CODE 306- INCOMING CALL, THE LINE PULSES ARE NOT IN RANGE

## 1.94.1

## FAULT CODE DESCRIPTION

The alarm is generated in the following situations:

- The seizure pulse has been received with a length out of range XX times. The faulty signal counter for incoming traffic has reached the limit. (XX = limit of the faulty signal counter, APS-parameter MAXFAULTYSIGINC).

- The terminal seizure ("Weichenbelegungs") pulse has been received with a length out of range XX times. The faulty signal counter for incoming traffic has reached the limit. (XX = limit of the faulty signal counter, APS-parameter MAXFAULTYSIGINC).

#### ADD INFO 1

Faulty TRS-individual-pointer.

### 1.94.2

#### MEASURE

1. Reset the faulty signal counter by clearing the alarm with the *alarm* command.
2. Initiate some incoming calls and measure the seizure pulse length.
3. Correct the pulse length in the cooperating exchange.
4. Are the pulse lengths in range?  
Pulse lengths (ms):
  - normal seizure (not UIC): 50 - 80
  - "Weichenbelegungs": 120 - 160
  - seizure UIC: 70 - 130.
5. NO: Correct the pulse length in the cooperating exchange again.
6. YES: Check the test values in the own exchange.
7. Are the test values according to the range values?
8. YES: Consult an expert.
9. NO: set the correct test-values in the own exchange.  
Pulse lengths (ms):
  - normal seizure (not UIC): 50 - 80
  - "Weichenbelegungs": 120 - 160
  - seizure UIC: 70 - 130.

## 1.95

### FAULT CODE 307- OUTGOING CALL, THE LINE PULSES ARE NOT IN RANGE

### 1.95.1

#### FAULT CODE DESCRIPTION

The alarm is generated in the following situations:

- The seizure acknowledgment pulse has been received with a length out of range XX times. The faulty signal counter for outgoing traffic has reached the limit. (XX = limit of the faulty signal counter, APS-parameter MAXFAULTYSIGOUT).
- The forward clear acknowledgment pulse has been received with a length out of range XX times. The faulty signal counter for outgoing traffic has reached the limit. (XX = limit of the faulty signal counter, APS-parameter MAXFAULTYSIGOUT).

#### ADD INFO 1

Faulty TRS-individual-pointer.

## 1.95.2

## MEASURE

1. Reset the faulty signal counter by clearing the alarm with the *alarm* command.
2. Initiate some outgoing calls and measure the seizure acknowledgement and forward clearing acknowledgement pulse.
3. Correct the pulse length in the cooperating exchange.
4. Are the pulse lengths in range?  
Pulse lengths (ms):
  - normal seizure (not UIC): 50 - 80
  - "Weichenbelegungs": 120 - 160
  - seizure UIC: 70 - 130
5. NO: Correct the pulse length in the cooperating exchange again.
6. YES: Check the test values in the own exchange.
7. Are the test values according to the range values?
8. YES: Consult an expert.
9. NO: Set the correct test-values in the own exchange.  
Pulse lengths (ms):
  - normal seizure (not UIC): 50 - 80
  - "Weichenbelegungs": 120 - 160
  - seizure UIC: 70 - 130

## 1.96

## FAULT CODE 308- ANALOGUE TRUNK, UNAUTHORIZED CHARGING PULSE

## 1.96.1

## FAULT CODE DESCRIPTION

The fault code is used in analogue external lines and indicates whether a faulty analogue pattern for the charging pulse has been received. The fault is probably in the public exchange.

## 1.96.2

## MEASURE

1. Inform the instance responsible for the line.
2. Block the line if necessary.

## 1.97

## FAULT CODE 309- ISDN DATA LINK ALARM, BIT ERROR IN STREAM (CRC-4)

## 1.97.1

## FAULT CODE DESCRIPTION

The TLU-board has discovered a bit error on the data link layer and has informed layer 3. The alarm is discovered when the TLU-board has reached the threshold level for CRC-4 (Cyclic Redundance Check) errors. The alarm can be divided into three error rates which is indicated in addinfo 2.

#### ADD INFO 1

Pointer to the interface.

#### ADD INFO 2

- 0 Bit error rate > 1 / second. (Errored second ES).
- 1 Bit error rate >  $1 \cdot 10^{-3}$  / second. (Severed Errored Second SES).
- 2 Bit error rate >  $1 \cdot 10^{-6}$  / minute. (Degraded Minutes DM).

**Note:** If no additional information is present in the alarm printout for ADDINFO2, the error level has not been determined.

The alarm ceases when the TLU-board has received correct CRC-4 multi frames.

1.97.2

#### MEASURE

1. Another alarm connected to this interface exists in the alarm log?
  2. YES: Consult fault location direction for that alarm.
  3. NO: inform instance responsible for the line.
- Return to the main flow.

1.98

## FAULT CODE 310- ISDN EXCESSIVE BIPOLAR VIOLATION

1.98.1

#### FAULT CODE DESCRIPTION

The alarm indicates that the accumulative bipolar violation counter has exceeded the threshold level on the TLU-board (1.5 Bit). The alarm will be erased on the accumulative bipolar violation counter being less than the threshold level.

#### ADD INFO 1

Pointer to TLU data individual.

1.98.2

#### MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway is located over the fan unit.
2. YES: Change to an other available virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. NO: Change the TLU-board.  
Consult the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: Clear the fault counters.  
Consult the operational directions for *ROUTE DATA, RO*.
6. Has the alarm returned?

7. YES: probably the line is faulty in an interworking exchange, or public exchange.  
Inform the instance responsible for the line.  
Return to the main flow.

## 1.99 FAULT CODE 311- ISDN FAILED SIGNAL STATE

### 1.99.1 FAULT CODE DESCRIPTION

The alarm indicates that the accumulative missed framing bits or CRC-6 have exceeded the threshold level for 10 consecutive seconds on the TLU-board (1.5 Bit). All initiated individuals on the board will be blocked automatically. The alarm will be erased on the accumulative missed framing bits being less than the threshold level.

#### ADD INFO 1

Pointer to TLU data individual.

### 1.99.2 MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway is located over the fan unit.
2. YES: Change to an other available virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. NO: Change the TLU-board.  
Consult the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: Key command alarm to erase (reset) alarms in the alarm log.
6. Has the alarm returned?
7. YES: probably the line is faulty in an interworking exchange, or public exchange.  
Inform the instance responsible for the line.  
Return to the main flow.

## 1.100 FAULT CODE 312- ISDN DIGITAL TRUNK, LOSS OF SIGNAL

### 1.100.1 FAULT CODE DESCRIPTION

The trunk line unit raises the alarm on detected loss of signal for 400 msec. The alarm will be erased on detection of framed signal for 4 seconds.

#### ADD INFO 1

Individual pointer of (virtual) device board.

## 1.100.2

### MEASURE

1. Check that the trunk cables are properly connected and the cooperating/public exchange working.
2. Are connections and cooperating exchange OK?
3. NO: fix the connections or wait for the cooperating exchange to be working.  
If there are free trunk ports, try another port.
4. Has the alarm returned?
5. YES: Replace the Media Gateway or the TLU board in the MX-ONE Classic.  
See operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
6. Has the alarm returned?
7. YES: probably the line is faulty on interworking exchange/public exchange.  
Inform the instance responsible for the trunk line.  
Return to the main flow.

## 1.101

### FAULT CODE 313- ISDN EXCESSIVE OUT OF FRAME

#### 1.101.1

#### FAULT CODE DESCRIPTION

The alarm indicates that the accumulative out of frame counter has exceeded 17 for 24 hours on the TLU-board (1.5 Bit). The alarm will be erased on the accumulative out of frame counter being less than 9.

#### **ADDINFO1**

Pointer to TLU data individual

#### 1.101.2

### MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway is located over the fan unit.
2. NO: Change to an other available virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. YES: Change the TLU board.  
Consult the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: probably the line is faulty on an interworking exchange, or public exchange.  
Inform the instance responsible for the line.  
Return to the main flow.

## 1.102 FAULT CODE 314- ISDN BIT ERROR RATE

### 1.102.1 FAULT CODE DESCRIPTION

The alarm indicates that the accumulative bit error counter has exceeded the threshold level on the TLU-board (1.5 Bit). The alarm will be erased on the accumulative bit error counter being less than the threshold level.

#### **ADD INFO 1**

Pointer to TLU data individual.

### 1.102.2 MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway is located over the fan unit.
2. NO: Change to an other available virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. YES: Change the TLU board.  
Consult the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
4. Has the alarm returned?
5. YES: probably the line is faulty on an interworking exchange, or public exchange.  
Inform the instance responsible for the line.  
Return to the main flow.

## 1.103 FAULT CODE 317- ISDN ERRORED SECONDS

### 1.103.1 FAULT CODE DESCRIPTION

The alarm indicates that the accumulative errored second counter has exceeded the threshold level on the TLU-board (1.5 Bit). The alarm will be erased on the accumulative errored second counter being less than the threshold level.

#### **ADD INFO 1**

Pointer to TLU data individual.

### 1.103.2 MEASURE

1. Is the Media Gateway of the single unit server type?  
This Media Gateway is located over the fan unit.
2. NO: Change to an other available virtual board for the ISDN trunk.  
See operational directions for *ROUTE DATA, RO*.
3. YES: Change the TLU board.



Consult the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

4. Has the alarm returned?
5. YES: probably the line is faulty on an interworking exchange, or public exchange.  
Inform the instance responsible for the line.  
Return to the main flow.

## 1.104

## FAULT CODE 319- STATIC SEMIPERMANENT CONNECTION DISTURBANCE

### 1.104.1

### FAULT CODE DESCRIPTION

This fault code indicates that a static semipermanent connection has encountered disturbances due to LIM isolation, blockings, and so on.

The following information is given in the printout from the exchange for this fault code:

#### **ADD INFO 1**

Failed connection's record pointer in the program unit SSM.

### 1.104.2

### MEASURE

1. Enter the command *SEMIP:LIM=x*; where x is the LIM number of EQU reported in the alarm.
2. Check if the static semipermanent connection is in the database?
3. NO: Consult an expert.
4. YES: Has the system, LIM or program unit SSM restarted within the past 5 minutes?
5. YES: Is the restart successfully completed?  
YES: Consult an expert.
6. NO: Wait 2 minutes.
7. Is the alarm reset?
8. NO: Is external line or CAS extension involved?
9. NO: Continue to section Possible board fault.
10. YES: Is it a line fault?
11. YES: Repair the line fault.
12. NO: Is it an equipment fault?
13. NO: Continue to section Possible board fault.
14. YES: Repair the equipment.
15. Wait 2 minutes
16. Is the alarm reset
17. NO: Consult an expert.

## 1.104.2.1

*Possible board fault*

1. Is it a board fault?
2. YES: Repair the board.
3. Wait for 2 minutes.
4. Is the alarm reset?
5. NO: Consult an expert.

## 1.105

## FAULT CODE 320- TELEPHONY CALLS THROTTLED

## 1.105.1

## FAULT CODE DESCRIPTION

The MX-ONE Service Node has rejected calls due to an almost overloaded CPU (for example, caused by high call rate, or by some heavy application executing on the same processor).

**ADD INFO 1**

Server processor status.

- 0 Less than Yellow level of signaling response time delay. No rejection of calls.
- 1 Yellow to Red level of signaling response time delay. New internal calls are rejected.
- 2 More than Red level of signaling response time delay. All new calls are rejected.

Where Yellow and Red are signaling response time delay levels. The alarm is sent when a call has been rejected (since level Yellow or Red is valid). Indirectly the signaling response time delay indicates the level of CPU load.

**ADD INFO 2**

Average number of new calls the last 10 seconds.

**Note:** It is possible to change the alarm triggering for High call rate.

## 1.105.2

## MEASURE

Check for any of the following alarms:

- Fault code 1:1 High CPU load
- Fault code 1:31 Too much memory paging
- Fault code 1:32 Slow event response

If any of these alarms are found, they should be solved first. The fault condition triggering those alarms is most likely also the cause of this alarm.

The alarm indicates that an investigation of traffic load in this system should be performed. A reduction of the number of extensions or external lines, move of certain applications, or a more powerful server processor might prevent this alarm in the future.

The number of calls/second which can be handled by a MX-ONE Service Node depends on the selected processor of the server.

## 1.106 FAULT CODE 321- IP ADDRESS BLOCKED

### 1.106.1 FAULT CODE DESCRIPTION

The MX-ONE Service Node has received a failed registration/authentication from a specific IP address exceeding the configured level (number of attempts). The address will be blocked for a configured number of seconds, see the *ip\_telephony.conf* file.

### 1.106.2 MEASURE

1. The source of this blocking can be an encroachment/trespassing attempt or a mis-configured device. More information on this failure can be found in the system log of the concerned server.
2. If wanted, the detection limits can be adjusted in the *ip\_telephony.conf* file.

## 1.107 FAULT CODE 324- FAULTY TMU BOARD

### 1.107.1 FAULT CODE DESCRIPTION

Faulty tone receiver, tone sender or multiparty equipment has been detected when performing periodic routine test of the TMU board, or the TMU board has been placed on an invalid board position.

#### **ADD INFO 1**

Faulty function on the TMU board, or if the TMU board has been placed on an invalid board position.

### 1.107.2 MEASURE

1. Was it a faulty tone receiver, tone sender, or multiparty equipment (ADD INFO 1 = 1, 2)?
2. YES: Change the TMU-board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
3. NO: Change to a valid board position.
4. Does the multiparty equipment function properly?
5. NO: consult an expert. Return to the main flow.

## 1.108 FAULT CODE 330- NO SIGNALING LINK ACTIVE WITHIN SIGNALING LINK SET (SS7)

### 1.108.1 FAULT CODE DESCRIPTION

The alarm will be generated if none of the signaling links owned by a signaling link set is in service, that is, in state active. (For SS7/TL81 trunk).

The following data can be read in the printout from the exchange for this fault code:

**ADD INFO 1**

States the individual pointer to the TRS data individual, that is, the signaling link set.

**ADD INFO 2**

States the signaling link set number.

**ADD INFO 3**

States the cause for becoming out of service [B0 - B3]:

- 0 Reception of consecutive LSSUs.
- 1 Intolerably high signal unit error rate.
- 2 Alignment unsuccessful.
- 3 Excessive delay of acknowledgments.
- 4 Two out of three unreasonable backward sequence numbers or FIBs.
- 5 Layer 1 failure.
- 6 Time out T6 (remote congestion).
- 7 Board activation.
- 8 Excessive pause between consecutive signal units.

**Note:** If this information is not present, the cause is not determined. The Information in [B4 - B7] is for expert use.

## 1.108.2

## MEASURE

1. Key the command *MTSSP* to get the status of the signaling links within the signaling link set. Use the information specified by ADD INFO 2 for the command entry.
2. NO: consult an expert. Return to the main flow.
3. Is there any alarm indicating a fault on the concerned board? Key command alarm to print (list) alarms in the alarm log.
4. YES: Consult the fault locating directions for this fault code.
5. NO: Is any of the links in state ACTIVE?
6. NO: Is any of the links in state STARTING?
7. NO: Key the command *MTSDC* to start a signaling link.
8. Key the command *MTSSP* to get the status of the signaling links within the signaling link set.
9. Is any of the links in state STARTING?
10. NO: Consult an expert.

## 1.109 **FAULT CODE 332- EXCESSIVE DELAY OF ACKNOWLEDGEMENT MESSAGE**

### 1.109.1 **FAULT CODE DESCRIPTION**

In the case a signaling message is sent to the cooperating exchange and an acknowledgment message is expected, a time supervision will be started. The alarm will be generated when the time supervision elapses. The message will be repeated until it is acknowledged or the alarm is cleared.

#### **ADD INFO 1**

Shows whether the message is for a board or a trunk individual.

#### **ADD INFO 2**

States the pointer of the board or trunk individual.

#### **ADD INFO 3**

States the code of the sent message.

### 1.109.2 **MEASURE**

1. Has any fault occurred in concerned LIM on concerned link set which can be the cause for this alarm? Key command *alarm* to print (list) alarms in the alarm log.
2. YES: Consult the fault locating directions for this fault code.
3. NO: Check faults in the cooperating exchange.
4. Is there any fault in the cooperating exchange?
5. YES: Consult the fault locating directions for the actual alarm in the cooperating exchange.
6. NO: Start a signal trace on the unit shown in the alarm log.
7. Analyze the signal trace. If it is of too high dignity, consult an expert.

## 1.110 **FAULT CODE 333 - DIGITAL TRUNK GROUP, EXCESSIVE NUMBER OF BLOCKED LINES**

### 1.110.1 **FAULT CODE DESCRIPTION**

This alarm is set when a predefined number of lines within one blocking group are manually blocked.

#### **ADD INFO 1**

States the blocking group number.

#### **ADD INFO 2**

States the calculated threshold value of blocked lines.

### 1.110.2 **MEASURE**

1. Check the blocked lines with the command *block\_list*.
2. Check with command *ROEDP* to which route the line or lines belong.

3. Check with command *RODAP* which lines there are in the affected blocking group.
4. Deblock the lines with the command *deblock*.

## 1.111

### FAULT CODE 334 - DIGITAL TRANSMISSION SYSTEM FAULTY

#### 1.111.1

#### FAULT CODE DESCRIPTION

The alarm will be generated when the hardware detects a fault on the digital transmission.

##### **ADD INFO 1**

States the pointer of the board individual.

#### 1.111.2

#### MEASURE

1. Has any fault occurred in concerned LIM for concerned board which can be the cause for this alarm? Key command *alarm* to print (list) alarms in the alarm log.
2. YES: Consult the fault locating directions for this fault code.
3. NO: Check faults on the line and in the cooperating exchange.
4. Is there any fault on the line or in the cooperating exchange?
5. YES: Consult the instance responsible for the line or the cooperating exchange.
6. NO: Is there any hardware fault?
7. YES: Change the hardware.

Consult the operational directions for *CONFIGURATION OF HARDWARE, REPLACEMENT*.

8. NO: Consult an expert.

## 1.112

### FAULT CODE 336 - LOST DATA FROM/TO INFORMATION COMPUTER SYSTEM

#### 1.112.1

#### FAULT CODE DESCRIPTION

An information computer system may be in the form of an interception computer, a voice mail system or other text message system.

The interface between the MX-ONE Service Node and the information computer system is supervised with respect to status (fault code 282), quality (fault code 281) and character processing (fault code 298). Data is sent to and from the information system in the form of messages. The messages are supervised to determine whether or not they reach their destination (fault code 336).

##### **ADD INFO 1**

Direction and type of lost data.

- 0 A message was not sent from the MX-ONE Service Node to the information computer system because the buffer in the MX-ONE Service Node was full.
- 1 A network message waiting message was not processed by the MX-ONE Service Node due to network congestion.
- 2 A network message waiting message was not processed by the MX-ONE Service Node due to RM record congestion.

#### **ADD INFO 2**

Information system identity. (Only used for ADDINFO1 = 1 or 2.)

### 1.112.2

#### MEASURE

#### 1.112.2.1

##### *ADD INFO 1 = 0*

1. Is ADD INFO 1 = 0?
2. NO: Continue to ADD INFO 1 = 1.
3. YES: Is the information computer system on line?
4. NO: Restore the information computer system to operational status.
5. YES: Can the baud rate between the MX-ONE Service Node and the information computer system be increased?
  - YES: increase the baud rate. See the command description for *MML COMMANDS, INFORMATION SYSTEMS*. Continue to the next step in the flow.
  - NO: Consult an expert.
6. Acknowledge fault code 336.  
See the command description for *alarm function*.
7. Does fault code 336 come back?
8. YES: Consult an expert.
9. Return to the main flow.

#### 1.112.2.2

##### *ADD INFO 1 = 1*

1. Is ADD INFO 1 = 1?
2. NO: Consult an expert.
3. YES: Are there any alarms indicating problems with the ISDN network?
4. NO: Consult an expert.
5. YES: Resolve any problems with the ISDN network.  
Consult fault locating directions for appropriate alarm.
6. Acknowledge fault code 336.
7. Initiate an information computer update.  
See the command description for *MML COMMANDS, INFORMATION SYSTEMS*

8. Does fault code 336 come back?  
See the command description for *alarm*.
9. YES: Consult an expert.
10. Return to the main flow.

## 1.113

### FAULT CODE 337 - DIGITAL TRUNK, CALL SETUP MESSAGE RECEIVED FOR UNASSIGNED CIRCUIT

#### 1.113.1

##### FAULT CODE DESCRIPTION

The alarm will be generated if a call set-up message is received identifying a circuit which is not assigned to any time slot within the concerned signaling link set.

##### **ADD INFO 1**

states the circuit identification code.

##### **ADD INFO 2**

states the signaling link set number.

#### 1.113.2

##### MEASURE

1. Consult maintenance personnel for information about the configuration of the exchange.
2. Must the circuit be initiated?
3. YES: initiate the circuit.

## 1.114

### FAULT CODE 339 - QUALITY ERROR IN ANCD COMMUNICATION

#### 1.114.1

##### FAULT CODE DESCRIPTION

An error has been detected in the ANCD information flow between nodes.

The interface between the PBX and the information system is supervised with respect to status (see fault locating directions for *FAULT CODE 282*), quality (see fault locating directions for *FAULT CODE 281*) and character processing (see fault locating directions for *FAULT CODE 298*).

Alarm 339 detects if the signal number is faulty, the checksum is not OK or the signal length is wrong.

##### **ADD INFO 1**

Type of fault:

- 0 Faulty signal length.
- 1 Faulty checksum.
- 2 Faulty order.



## 1.114.2

### MEASURE

1. Does the alarm 281, 282, 298 exist?
2. YES: See respective fault codes.
3. NO: The quality on the channel is not good, check the transmission equipment (that is the LAN connection).
4. Does the alarm remain?
5. YES: Consult an expert.  
Return to the main flow.

## 1.115

### FAULT CODE 345 - INFORMATION COMPUTER, FAULTY COMMUNICATION CHANNEL

#### 1.115.1

#### FAULT CODE DESCRIPTION

The fault code is obtained when the General Information Computer Interface is unable to communicate with the external application using the Ethernet port due to

- faulty network connection between the exchange and the external application
- faulty external application.

#### 1.115.2

#### MEASURE

1. Is the cable connection and external application bad?
2. YES: Correct cable and/or external application.
3. Key command *alarm* to print (list) alarms in the alarm log.  
Has the alarm been erased?
4. NO: Check the Ethernet port and Ethernet board.  
See fault locating instructions for *MiVOICE MX-ONE FAULT LOCATION*
5. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log.
6. Has the alarm returned?
7. YES: Consult an expert.  
Return to the main flow.

## 1.116

### FAULT CODE 346 - INFORMATION COMPUTER OUTPUT BUFFER OVERFLOW

#### 1.116.1

#### FAULT CODE DESCRIPTION

The fault code is obtained when the output buffer for the connected information computer system is full.

## 1.116.2

## MEASURE

1. Is there any bad cable connection and/or faulty external application?
2. YES: Correct cable connection and/or external application.
3. Key command alarm to print (list) alarms in the alarm log.  
Has the alarm been erased?
4. NO: Check the Ethernet port and Ethernet board.  
See fault locating instructions for *MIVOICE MX-ONE T FAULT LOCATION*
5. After 15 minutes key command alarm to print (list) alarms in the alarm log.
6. Has the alarm returned?
7. YES: Consult an expert.  
Return to the main flow.

## 1.117

## FAULT CODE 347 - SYNCHRONIZATION FAULT FOR DECT FIXED PART

## 1.117.1

## FAULT CODE DESCRIPTION

Synchronization between all ELU31 boards in the system is handled by a Dect synchronization RING structure. The RING consists of separate electrical interfaces.

Only one ELU31 board (RING MEMBER) in each subrack can be connected directly to the RING, the other ELU31 boards (BUS SLAVES) in the subrack receive synchronization signals and FRAME COUNTER values through a bus connection in the back-plane.

The synchronization alarm is generated in the following situations:

- broken RING cable
- unplugged RING cable
- broken or unplugged BUS cable
- individual board failure
- faulty RING receiver
- faulty RING transmitter
- faulty BUS receiver
- faulty BUS transmitter
- configuration fault.

**ADD INFO 1**

Pointer to faulty individual.

**ADD INFO 2**

Description of the type of fault

- 0 Loss of communication on RING interface
- 1 Loss of synchronization on RING interface
- 2 Loss of synchronization on BUS interface

- 3 Loss of synchronization on BUS interface
- 4 Unplugged RING cable transmitter side
- 5 Unplugged RING cable receiver side
- 6 Unplugged BUS cable, transmitter- and/or receiver side
- 12 Faulty operation of Automatic Cable Delay Measurement (ACDM)

## 1.117.2

### MEASURE

First check that all ELU31 boards have latest FW. And that all ring boards are of the same type.

- ELU31/3 and ELU31/4 'index\_3\_mode'
- ELU31/4 'index\_4\_mode'

To verify mode on ELU31/4 boards key command *dect\_cfp -p -v -s ring*.

For each alarm there is a count value indicating how often the alarm has been reported. Use command 'alarm -p -f detail'.

1. Does the fault printout show value 0 for ADD INFO 2?
2. YES: Go to section ADD INFO 2 = 0.
3. NO: Does the fault printout show value 1 for ADD INFO 2?
4. YES: Go to section ADD INFO 2 = 1.
5. NO: Does the fault printout show value 2 for ADD INFO 2?
6. YES: Go to section ADD INFO 2 = 2.
7. NO: Does the fault printout show value 3 for ADD INFO 2?
8. YES: Go to section ADD INFO 2 = 3.
9. NO: Does the fault printout show value 4 for ADD INFO 2?
10. YES: Go to section ADD INFO 2 = 4.
11. NO: Does the fault printout show value 5 for ADD INFO 2?
12. YES: Go to section ADD INFO 2 = 5.
13. NO: Does the fault printout show value 6 for ADD INFO 2?
14. YES: Go to section ADD INFO 2 = 6.
15. NO: Does the fault printout show value 12 for ADD INFO 2?
16. YES: Go to section ADD INFO 2 = 12.
17. NO: Is additional text 'Receiving PCM synchronization is bad'?
18. YES: Go to section PCM synchronization faulty.
19. NO: Undefined error. Consult an expert.

## 1.117.2.1

*ADD INFO 2 = 0*

Loss of communication on Dect synchronization RING interface.

There is a checksum control on the communication, bit error(s) in that control can cause this alarm. The cable could be too long or not be shielded and other equipment can cause disturbance.

1. Attend to all 347 'unplugged TX/RX cable' if any.
2. Check the ring structure, with t. ex. *dect\_cfp -p -s ring*.
3. Verify the cabling for the RING. Cable is not cut, no glitch in cross connection points. Cable is too long? Verify the cable length and dimension to specification in Installation Instruction.
4. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
5. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
6. NO: Return to the main flow.
7. YES: Key command *diagnostic\_print -unit CTLP -lim x -request 'clock quality snap view, verbose'*, check jitter on the pcm clock and/or jitter on the ACDM measurement.  
Are the values stable?
8. YES: Continue to section ELU31 board.
9. NO: Replace the board reporting the fault  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
10. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.  
Does the fault remain?
11. NO: Return to the main flow.
12. YES: Replace the board that is before the board that is reporting the fault. Use command *dect\_cfp -p -s ring* to find previous board in the ring.
13. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log. Wait one minute. Does the fault remain?
14. NO: Return to the main flow.
15. YES: this could be a problem with the MGU board in the previous boards subrack.  
Consult an expert.

## 1.117.2.2

*ADD INFO 2 = 1*

Loss of Dect synchronization on Dect synchronization RING interface.

1. Attend to all 347 'unplugged TX/RX cable' if any.

2. Check the ring structure with *dect\_cfp -p -s ring*.
3. Verify the cabling for the RING. Cable is not cut, no glitch in cross connection points. Cable is too long? Verify the cable length and dimension to specification in Installation Instruction.
4. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute
5. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
6. NO: Return to the main flow.
7. YES: Key command *diagnostic\_print -unit CTLP -lim x -request 'clock quality snap view, verbose'*, check jitter on the pcm clock and/or jitter on the ACDM measurement. Are the values stable?
8. YES: Continue to section ELU31 board.
9. NO: Replace the board reporting the fault  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
10. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.  
Does the fault remain?
11. NO: Return to the main flow.
12. YES: Replace the board that is before the board that is reporting the fault. Use command *dect\_cfp -p -s ring* to find previous board in the ring.
13. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.  
Does the fault remain?
14. NO: Return to the main flow.
15. YES: this could be a problem with the MGU board in the previous boards subrack. Please consult an expert.

### 1.117.2.3

#### ADD INFO 2 = 2

Loss of communication on BUS interface.

1. Is the ELU31 board placed in subrack with BUS INTERFACE integrated in the backplane?
2. NO: verify the cabling for the BUS interface.
3. YES: Is the bus cable connected to the ELU31 board?  
NO: Continue to section ELU31 board.  
YES: Remove the bus cable.
4. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.

Wait one minute

5. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
6. NO: Return to the main flow.
7. YES: Continue to section ELU31 board.

#### 1.117.2.4

#### ADD INFO 2 = 3

Loss of synchronization on BUS interface.

1. Is the ELU31 board placed in a subrack with BUS INTERFACE integrated in the backplane?
2. NO: verify the cabling for the BUS interface.
3. YES: Is the bus cable connected to the ELU31 board?  
NO: Continue to section ELU31 board.  
YES: Remove the bus cable.
4. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
5. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
6. NO: Return to the main flow.
7. YES: Continue to section ELU31 board.

#### 1.117.2.5

#### ADD INFO 2 = 4

Unplugged Dect synchronization RING cable on transmitter side, TX.

1. Verify if the plug for the RING cable is connected to the outgoing side (transmitter side).
2. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
3. Key the command *alarm* to print (list) alarms in the alarm log and verify the result  
Does the fault remain?
4. NO: Return to the main flow.
5. YES: Continue to section ELU31 board.

#### 1.117.2.6

#### ADD INFO 2 = 5

Unplugged Dect synchronization RING cable on the receiver side, RX.

1. Verify if the plug for the RING cable is connected to the incoming side (receiver side).

2. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
3. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
4. NO: Return to the main flow.
5. YES: Continue to section ELU31 board.

#### 1.117.2.7

#### ADD INFO 2 = 6

Unplugged BUS cable, transmitter-, or receiver side, or both transmitter- and receiver sides.

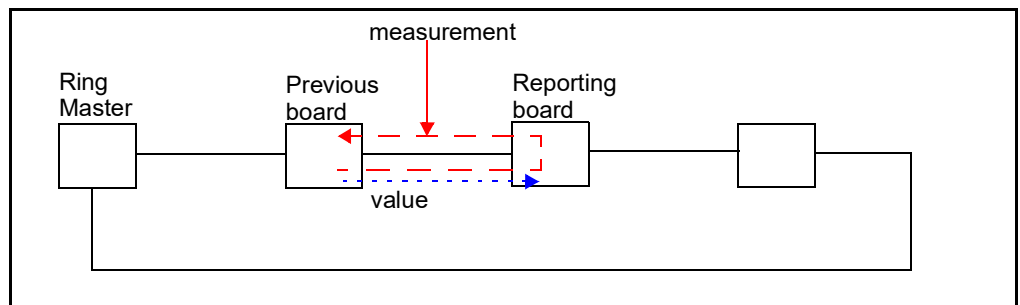
1. Verify if the plugs for the BUS cables are connected to the incoming and outgoing side (transmitter- and receiver side).
2. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
3. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
4. NO: Return to the main flow.
5. YES: Continue to section ELU31 board.

#### 1.117.2.8

#### ADD INFO 2 = 12

The Automatic Cable Delay Measurement is faulty.

Measurement is made by previous board and communicated down wards.



1. Attend to all 347 'Loss of communication on the Dect synchronization ring' if any.
2. Check the ring structure with *'dect\_cfp -p -s ring'*.
3. Verify the cabling for the RING. Cable is not cut, no glitch in cross connection points. Cable is too long? Verify the cable length and dimension to specification in Installation Instruction.
4. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.

5. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
6. NO: Return to the main flow.
7. YES: Key command *diagnostic\_print -unit CTLP -lim 'previous board lim' -request 'clock quality history view'*  
  
key the command *diagnostic\_print -unit CTLP -lim 'include reporting lim and previous boards lim' -request 'clock quality snap view, verbose'* to check the ACDM values where minimum and maximum are not equal.  
  
Are the pcm clock jitter stable and ACDM min=max?
8. YES: Continue to section ELU31 board.
9. NO: Replace the board previous to the reporting board.  
  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
10. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
  
Wait one minute.
11. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
12. NO: Return to the main flow.
13. YES: Replace the board that is reporting the fault.
14. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
  
Wait one minute.  
  
Does the fault remain?
15. NO: Return to the main flow.
16. YES: this could be a problem with the MGU board in the previous boards subrack. Please consult an expert.

### 1.117.2.9

#### *PCM synchronization faulty*

1. Check the ring structure with 'dect\_cfp -p -s ring'.
2. Verify the cabling for the RING. Cable is not cut, no glitch in cross connection points. Cable is too long? Verify the cable length and dimension to specification in Installation Instruction.
3. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
  
Wait one minute.
4. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
5. NO: Return to the main flow.
6. YES: Key command *diagnostic\_print -unit CTLP -lim all -request 'clock quality history view' or multiple 'clock quality snapshot'*. Are the values stable? Or are the values high?



7. NO: Continue to section ELU31 board.
8. YES: Continue to check the values for the previous boards until a board with stable/low values are found.
9. This could be a problem with the MGU board or incoming synchronization in the subrack with stable values. Please consult an expert.

#### 1.117.2.10

#### *ELU31 board*

1. Block the faulty ELU31 board that gives the alarm.  
Key the command *block -bpos*.
2. Is there any traffic on the ELU31 board?  
Check the result of the blocking command.
3. YES: Do the previous step again.
4. NO: Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.
5. Restart the faulty ELU31 board that gives the alarm. Key the command *board\_restart*.
6. Unblock the ELU31 board.  
Key the command *deblock*.
7. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
8. YES: verify the configuration of the DECT system. That only one board per subrack is a ring board. That all boards has synchronization role. That all delay values are reasonable, see installation instruction to find typical delay across a copper cable.
9. Does the fault remain?
10. YES: Are BUS slaves placed in subrack with BUS INTERFACE integrated in the backplane?  
NO: Continue to the next step.  
YES: Are bus cables connected to the ELU31 boards that are BUS slaves?  
NO: Continue to the next step.  
YES: Remove the bus cables.
11. Key the command *alarm -e --alarm-code 347* to erase (reset) fault code 347 in the alarm log.  
Wait one minute.
12. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
13. YES: Replace the faulty ELU31 board that gives the alarm.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
14. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?

15. YES: Are there more than one board on the same bus that give alarm?
16. YES: The fault may be in the RING MEMBER board. Try to replace the RING MEMBER board.
17. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
18. YES: Change the ring cables and bus cables (if they exist).
19. Key the command *alarm* to print (list) alarms in the alarm log and verify the result.  
Does the fault remain?
20. YES: Consult an expert.  
Return to the main flow.

## 1.118

## FAULT CODE 348 - SYNCHRONIZATION DISTURBANCE FOR DECT FIXED PART

### 1.118.1

### FAULT CODE DESCRIPTION

The alarm indicates that a disturbance is detected on the synchronization between two ELU31 boards. The disturbance may be caused by a mismatch between the received and the local Frame Counter Value (controlled by the Device Processor) or that a synchronization reload has occurred the board.

This can occur during maintenance and/or when changing synchronization source.

- New ring master, no measure.
- New external synchronisation source, no measure.
- Initiating board, no measure.
- Manual restart of board, no measure.

When the alarm keep appearing spontaneously it is an indication on that synchronization is either not stable or not present at all and this will cause disturbance for the dect users.

#### ADD INFO 1

Pointer to disturbance marked individual.

#### ADD INFO 2

Correction of Delay Compensation or Frame Counter when:

- Faulty MGU board.
- Synchronization distortion caused by bad or disturbed cable. Very noisy environment requires shielded cables.
- Faulty board.
- Too long synchronization cable or too thin wires.
- Other media for DECT synchronization than copper is not approved.
- Repeaters in the DECT synchronization ring are not approved.

**Note:** This may lead to that the base stations are restarted.

## 1.118.2

## MEASURE

For each alarm there is a count value indicating how often the alarm has been reported. Use command 'alarm -p -f detail'.

1. Mismatch in Frame Counter value or reload of synchronization counter has occurred.
2. Does the alarm occur frequently?
3. NO: take note of the alarm and observe the alarm log. If the alarm does not occur again, there has only been an accidental disturbance that has been fixed by the system.
4. YES: Check that all media gateways, with ELU31 boards, has correct synchronization source, key command *trsp\_synchronization*. Consider the faulty configuration case described in installation description. This alarm is typical for that faulty configuration.
5. Check the built in diagnostic in CTLP. Key command *diagnostic\_print -unit CTLP -lim x -request xxx*  
  
Check the accumulated delay at ring master, should not exceed 2000 nano seconds, consult installation instruction for action to take  
  
Check the clock quality data for the whole ring, history and snap view. Has jitter high values or unstable values?
6. NO: Continue next step.
7. YES: Replace the board previous to the board reporting high/unstable values
8. Clear the history and min/max values with *diagnostic\_print -unit CTLP -lim all -request xxx*.
9. Wait up to 30 minutes, check the clock quality data, history and snapview. Are there still high/unstable values?
10. NO: Continue next step.
11. YES: Replace the board with the high/unstable values.
12. Erase fault code 348 with the command *alarm -e --alarm-code 348*.
13. Key command alarm to print (list) alarms in the alarm log to check if the alarm returns.
14. Does the fault remain?
15. YES: Check all synchronization cables connected to the disturbance marked board. Replace them if necessary. Check if other media than copper wires are used for the DECT synchronization ring.
16. Does the fault remain?
17. YES: Restart the MGU board in the LIM where the ELU31 board is located that transmits the synchronization signals to disturbance marked board. Check if other media than copper wires are used for the DECT synchronization ring.  
  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
18. Does the fault remain?
19. YES: Restart the MGU board in the LIM where the fault occurs.  
  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

20. Does the fault remain?
21. YES: Consult an expert. Include *diagnostic\_print* data in the ticket.
22. Return to the main flow.

## 1.119 FAULT CODE 349 - FAULTY RFP FOR DECT FIXED PART

### 1.119.1 FAULT CODE DESCRIPTION

The alarm indicates faulty Radio Fixed Part (RFP). This alarm is generated in the following situations:

- The RFP is initiated but physically not connected. - The RFP is marked as faulty.

#### **ADD INFO 1**

Pointer to faulty individual.

#### **ADD INFO 2**

Description of the type of fault.

- 2 RFP initiated but not connected.
- 4 RFP faulty.

#### **ADD INFO 3**

Faulty RPN (Radio Fixed Part Number)

### 1.119.2 MEASURE

For each alarm there is a count value indicating how often the alarm has been reported. Use command 'alarm -p -f detail'.

1. Does the fault printout show value 2 for ADD INFO 2?
2. YES: Go to section ADD INFO 2 = 2.
3. NO: Does the fault printout show value 4 for ADD INFO 2?
4. YES: Go to section ADD INFO2 = 4.
5. NO: Undefined error, consult an expert.

#### 1.119.2.1 *ADD INFO 2 = 2*

The RFP is initiated, but no connection between the ELU31 board and the RFP.

1. Check the connection between the ELU31 board and RFP. Also, check if the RFP is connected to correct port on the ELU31 board.
2. Also visually check that the RFP indicates power ON.

3. Does the fault remain?  
Key the command *alarm to print (list) alarms in the alarm log*.
4. YES: Replace the RFP.  
See operational directions for *CORDLESS EXTENSION*.
5. Does the fault remain?  
Key the command *alarm to print (list) alarms in the alarm log*.
6. YES: Consult an expert.  
Return to the main flow.

#### 1.119.2.2

#### ADD INFO 2 = 4

The RFP is reported as faulty.

1. Restart the RFP with the command *CXRFI*.  
See operational directions for *CORDLESS EXTENSION*.
2. Has the fault returned?  
Key the command *alarm to print (list) alarms in the alarm log*.
3. YES: Replace the RFP.  
See operational directions for *CORDLESS EXTENSION*.
4. Has the fault returned?  
Key the command *alarm* to print (list) alarms in the alarm log.
5. YES: Consult an expert.  
Return to the main flow.

## 1.120

## FAULT CODE 350 - CSTA, FAULTY COMMUNICATION CHANNEL

### 1.120.1

### FAULT CODE DESCRIPTION

The fault code is obtained when CSTA cannot communicate with an external application using this Ethernet port due to:

- faulty network connection between the exchange and the external application
- faulty external application.

The following information is given in the printout from the exchange for this fault code:

#### ADD INFO 1

Individual pointer to link group individual.

### 1.120.2

### MEASURE

1. Is cable and/or external application faulty?
2. YES: Correct cable and/or external application.

3. Has the alarm been erased?
4. NO: Check the Ethernet port and Ethernet board.  
See fault locating instructions for *MIVOICE MX-ONE FAULT LOCATION*.
5. After 15 minutes key the command *alarm* to print (list) alarms in the alarm log.
6. Has the alarm returned?
7. YES: Does printout for the command *CSTLP* indicate that the link is faulty?
8. YES: Consult an expert.  
Return to the main flow.

## 1.121 FAULT CODE 358 - SMS, FAULTY COMMUNICATION CHANNEL

### 1.121.1 FAULT CODE DESCRIPTION

The fault code is obtained when there is a problem with the communication to external SMS equipment. There are two types of fault.

- Service node is SMS server, *sms\_server\_initiate*. External equipment sends SMS to the service node.
- Service node is SMS client, *sms\_client\_initiate*. Extension sends SMS to external equipment. When this alarm is raised will this service node stop sending SMS to this IP address.

The alarm is cleared when a heart beat or SMS message is received by the service node SMS server. The heart beat is expected every minute.

### 1.121.2 MEASURE

#### 1.121.2.1 *Report from service node SMS server*

The service node expect that a heart beat message is received once per minute. If no such message or other messages has been received from the external equipment is this alarm raised. It will be cleared at the first heart beat or SMS message received from the external equipment.

1. Check what IP address the service node SMS server have.
2. Check the external equipment.  
Does the external equipment send SMS to the IP address of the service node SMS server?  
YES: Continue.  
NO: Change the IP address in the external equipment.
3. Check the external equipment.  
Does LEDs or other indicators show any problem?  
YES: Look in the manual for external equipment how to handle the indicated fault.

NO: Continue.

4. Log on to the server that has reported the fault and key ping xx.xx.xx.xx, the address of external equipment.

Does the external equipment answer on *ping*?

YES: Continue.

NO: Check cables and IP network.

5. Log on to the external equipment or equivalent tool to send a test SMS to service node.

Can the external equipment send SMS to the service node and the extension has received it?

YES: End.

NO: Check the IP address used in external equipment for addressing the service node. Check the IP address in service node for addressing the external equipment.

6. Remove the service node SMS server with command *sms\_server\_end* and initiate it again with command *sms\_server\_initiate*. Wait up to 5 minutes.

7. Alarm still active?

YES: Consult an expert.

NO: End.

#### 1.121.2.2

#### *Reported from service node SMS client*

When extension sends SMS to the service node it will setup a connection to the external equipment. If this failed is an alarm raised. When this alarm is raised will this service node stop sending SMS to this IP address.

The alarm is cleared when a heart beat or SMS message is received by the service node SMS server. The heart beat is expected every minute.

1. Check that the fault reporting service node SMS client data is configured correctly, Key *sms\_client\_print*.

Is the client IP address correct?

YES: Continue.

NO: Remove faulty client data and initiate the IP address of the external equipment.

2. Log on to the server that has reported the fault and key ping xx.xx.xx.xx, the address of external equipment.

Does the external equipment answer on *ping*?

YES: Continue.

NO: Check cables and IP network.

3. Log on to the external equipment or equivalent tool to send a test SMS to service node.

Can the external equipment send SMS to the service node and the extension has received it?

YES: Continue.

NO: Continue at 1.121.2.1 Report from service node SMS server on page 102.

4. Send a SMS from an extension in the service node that reported the fault.
5. Could the extension send a SMS and it was received by the intended extension?  
YES: End.  
NO: Check the IP network. This service node have problem to connect to the external equipment.
6. Check the count indicator on the alarm, use alarm -p -f detail.  
Are count more then 1?  
YES: This indicates an intermittent fault. Probably caused by IP network congestion.  
NO: Continue.
7. Remove the service node SMS client with command *sms\_client\_end -lim* to remove only faulty client and initiate it again with command *sms\_client\_initiate -lim*.
8. Send a SMS from an extension in the service node that reported the fault.
9. Could the extension send a SMS and it was received by the intended extension?  
YES: End.  
NO: Consult an expert.

## 1.122

## FAULT CODE 359 - ROUTING SERVER, FAULTY IP CONNECTION TO SATELLITE

### 1.122.1

### FAULT CODE DESCRIPTION

The fault code is obtained when the Routing Server has found a faulty IP connection towards a satellite. A Faulty IP connection is discovered when the routine check is performed in Routing Server towards a satellite.

#### ADD INFO 1

- 0 The first initiated IP connection is faulty.
- 1 The second initiated IP connection is faulty.

#### ADD INFO 2

Digits 1 - 4 in the destination code to satellite.

#### ADD INFO 3

Digits 5 - 8 in the destination code to satellite.

#### ADD INFO 4

Digits 9 - 10 in the destination code to satellite.

### 1.122.2

### MEASURE

Consult an expert.



## 1.123 FAULT CODE 360 - ROUTING SERVER, PNR TABLE HAS BEEN SPLIT

### 1.123.1 FAULT CODE DESCRIPTION

The fault code is obtained when the PNR table is split. If the length of the entry in the satellite is shorter than the length of the entry in the Routing Server, the PNR table in the satellite will be split until it matches the length of the entry in the Routing Server.

No additional information is supplied.

### 1.123.2 MEASURE

This is just an indication alarm, no measures are to be taken.

The system administrator should verify the changed data in the PNR table, and perform a system dump. Key command *alarm* to erase (reset) the alarm.

## 1.124 FAULT CODE 362 - DEVICE BOARD IS AT ALARM LEVEL 2

### 1.124.1 FAULT CODE DESCRIPTION

An alarm is generated by the MX-ONE system for the ELU34 analog extension board due to traffic through the board, when the temperature and power dissipation values on the board fall in the range of alarm level 2 defined for this board type.

The alarm is reset by the system when the board alarm level changes from alarm level 2 to any other defined alarm level.

If the board is at alarm level 2, no new traffic is allowed for the board. The board blocks all the new outgoing calls from the extensions initiated on the board and system software blocks the new incoming calls to the connected extensions.

The ongoing traffic is not affected by transition of alarm levels.

### 1.124.2 MEASURE

1. Key the command *call\_trace -bpos* to check the number of calls through the board.
2. Is there an alarm even though there is only low traffic through the board?
3. YES: Consult an expert.
4. NO: Wait for some time to allow the clearance of few ongoing calls through that board.
5. Enter the command *alarm* to print (list) alarms in the alarm log.  
Has the alarm been acknowledged by the system?
6. YES: Return to the main flow.
7. NO: Are the fans in the fan unit functioning correctly?
8. YES: Consult an expert.
9. NO: Repair or replace any faulty fan equipment.

10. Does the alarm remain?
11. YES: Is the room temperature too high?
12. NO: Consult an expert.

13. YES: adjust the cooling equipment to achieve an acceptable room temperature.  
The cooling equipment can be out of order or can have too low capacity.
14. Does the alarm remain?
15. YES: Consult an expert.

## 1.125

## FAULT CODE 363 - IP DEVICE BOARD, MAJOR FAULT

### 1.125.1

### FAULT CODE DESCRIPTION

The alarm indicates that a major fault has been generated in the IP device board. All devices are automatically blocked for new calls.

The following information is given in the printout from the exchange for this fault code:

#### ADD INFO 1

Individual pointer to device board.

#### ADD INFO 2

Description of the type of alarm:

- 1 Faulty connection  
A disconnection of Ethernet Layer 2 is detected. Most likely the physical cable is missing or faulty.
- 3 Network overflow  
The IP device board is receiving more packets from the IP network than it is able to process.
- 5 Faulty DSP
- 7 Network configuration error  
The IP device board tried to set up the ethernet interface but did not succeed.
- 8 SysCom messages lost  
The IP device board detects that messages from or to the System Software through the system communication interface, the backplane, are lost. This can be due to high load.
- 9 SysCom backplane error  
The IP device board detects a Layer 1 error on the system communication interface, the backplane.
- 10 Configuration parameter invalid  
The configuration parameters fetched from the EEPROM device are invalid.
- 11 EEPROM error  
The IP device board detects a hardware read/write error while accessing the EEPROM device.
- 12 IP device board cannot reach default gateway xxx  
No RTP media via this MGU/IPLU board can be used, i.e. gateway traffic does not work. However it will be possible to use RTP resources for inter-gateway media.

### 1.125.2

### MEASURE

#### 1.125.2.1

#### *Faulty connection (ADD INFO2 = 1)*

1. Check the physical line connection to the IP device board.  
See LED2 on the board front.

2. Does the physical connection exist and work properly?
3. YES: Replace the physical line connection to the IP device board.  
Does the fault remain? Enter the command *alarm* to print (list) alarms in the alarm log.  
YES: Continue to the next step, if NO return to main flow.
4. NO: enter the command *board\_restart* to re-activate the board.  
All ongoing calls will be cleared.
5. Does the fault remain?  
Enter the command *alarm* to print (list) alarms in the alarm log.
6. YES: Replace the IP device board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
7. Enter the command *alarm* to print (list) alarms in the alarm log.  
Does the fault remain?
8. YES: Check the line connection with a protocol analyzer in order to test the layer-2 connection.
9. Is the layer-2 connection OK?
10. YES: Does the fault remain?  
Enter the command *alarm* to print (list) alarms in the alarm log.
11. YES: Consult an expert.
12. Return to the main flow.

### 1.125.2.2

#### *Network overflow (ADD INFO2 = 3)*

1. Enter the command *alarm* to erase (reset) alarms in the alarm log.
2. Enter the command *board\_restart -bpos*.
3. Does the fault remain?
4. YES: Replace the board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS* section *Replacing IPLU*.
5. Does the fault remain?
6. YES: Consult an expert.

### 1.125.2.3

#### *Faulty DSP (ADD INFO2 = 5)*

1. Enter the command *board\_restart -bpos*.
2. Does the fault remain?
3. YES: Replace the board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS* section *Replacing IPLU*.
4. Does the fault remain?
5. YES: Consult an expert.

### 1.125.2.4

#### *Network configuration error (ADD INFO 2 = 7)*

1. Check the IP address, net mask and gateway parameter supplied to the command *media\_gateway\_interface*.
2. Are they all correct?
3. NO: enter the command *media\_gateway\_interface* again.  
Use correct IP network values.
4. Enter the command *alarm* to print (list) alarms in the alarm log.  
Does the fault remain?
5. Enter the command *board\_restart -bpos*.
6. Does the fault remain?  
Enter the command *alarm* to print (list) alarms in the alarm log.
7. YES: Consult an expert.
8. Return to the main flow.

### 1.125.2.5

#### *SysCom messages lost (ADD INFO2 = 8)*

1. Enter the command *alarm* to erase (reset) alarms in the alarm log.
2. Enter the command *board\_restart -bpos*.
3. Does the fault remain?

4. YES: Replace the board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS* section *Replacing IPLU*.
5. Does the fault remain?
6. YES: Consult an expert.

## 1.125.2.6

*SysCom backplane error (ADDINFO2 = 9)*

1. Enter the command *alarm* erase (reset) alarms in the alarm log.
2. Enter the command *board\_restart -bpos*.
3. Does the fault remain?
4. YES: Replace the board.  
See operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS* section *Replacing IPLU*.
5. Does the fault remain?
6. YES: Consult an expert.

## 1.125.2.7

*Configuration parameter invalid (ADDINFO2 = 10)*

1. Check the IP address, net mask and gateway parameter supplied to the command *media\_gateway\_interface*.
2. Are they all correct?
3. NO: enter the command *media\_gateway\_interface* again.  
Use correct IP network values.
4. Does the fault remain?  
Enter the command *alarm* to print (list) alarms in the alarm log.
5. YES: enter the command *board\_restart -bpos*.
6. Enter the command *alarm* to print (list) alarms in the alarm log.  
Does the fault remain?
7. YES: Consult an expert.  
Return to the main flow.

## 1.125.2.8

*EEPROM error (ADDINFO2 = 11)*

1. There is a serious problem writing to or reading from the onboard EEPROM device.
2. Restart the board with command *board\_restart*.
3. Does the fault remain?  
Enter the command *alarm* to print (list) alarms in the alarm log.
4. YES: Replace the board.
5. Enter the command *alarm* to print (list) alarms in the alarm log

Does the fault remain?

6. YES: Consult an expert.  
Return to the main flow.

## 1.126

## FAULT CODE 364 - IP DEVICE BOARD, MINOR FAULT

### 1.126.1

### FAULT CODE DESCRIPTION

The alarm indicates that a minor fault has been generated in the IP device board. No traffic is blocked. Further actions must be taken if the speech quality is not acceptable. The following information is given in the printout from the exchange for this fault code:

#### ADD INFO 1

Individual pointer to device board.

#### ADD INFO 2

Description of the type of alarm:

- 0 Unacceptable quality of service  
The number of lost packets exceeds the threshold (2% of lost packets).
- 2 Jitter buffer overflow  
RTP packets are dropped from the jitter buffer. This happens when the decoder has deleted a frame due to buffer overflow. Buffer overflow occurs when the expected playout delay is exceeded.
- 4 Network delay  
The round trip delay divided by 2 between two endpoints exceeds the threshold (100 ms of maximum delay).
- 6 Playout delay  
The internal processing time to play out a packet received from IP exceeds 10 ms. The codec size and the fixed TDM delay inside the Media Stream Processor have to be considered. (The fixed TDM delay is the delay the Media Stream Processor needs to access one sample from the TDM bus.)

### 1.126.2

### MEASURE

#### 1.126.2.1

*Common measures for ADDINFO2 = 0, 2 or 4*

1. Analyze the network.  
The problem most likely lies in the network.
2. Enter the command *alarm* to erase (reset) alarms in the alarm log.
3. Does the fault remain?
4. YES: enter the command *block -bpos*.
5. Enter the command *board\_restart -bpos*.
6. Does the fault remain?
7. YES: Consult an expert.  
A better network is needed.

## 1.126.2.2

*Playout delay (ADDINFO2 = 6)*

1. Enter the command *alarm* to erase (reset) alarms in the alarm log.
2. Enter the command *block -bpos*.
3. Enter the command *board\_restart -bpos*.
4. Does the fault remain?
5. YES: Consult an expert.

## 1.127

## FAULT CODE 365 - DEVICE FAULT

## 1.127.1

## FAULT CODE DESCRIPTION

The alarm indicates a detected device fault. See Additional information for detailed description.

**ADD INFO 1**

Type of fault.

- 1 Ring lead on ELU34 individual grounded.

**Note:** Permanent board damage may occur.

## 1.127.2

## MEASURE

Disconnect and check the connected cable immediately. This situation may cause permanent board damage

This event will set the Linefault bit in the blocking information, see command *block\_list*.

If the ELU34 has reported this event several times the instrument bit in the blocking information will also be set, see command *block\_list*. If this stage is reached the ALARM and blocking will not clear itself. Both blocking and ALARM must be cleared manually, see commands *alarm* and *block/deblock*.

## 1.128

## FAULT CODE 366 - INCONSISTENCY BETWEEN DEFINED ITYPE AND ACTIVE TERMINAL

## 1.128.1

## FAULT CODE DESCRIPTION

The alarm indicates a detected inconsistency between initiated and plugged-in terminal types for the ELU33 digital extension board. See additional information for detailed description.

Additional information gives the directory number of the extension and the ITYPE of the newly connected terminal. See Digital Key System Telephone parameter description for ITYPE values.

**ADD INFO 1**

Directory Number where r = XXX, Connected ITYPE = yy.



1.128.2

MEASURE

If the terminal is the correct model that shall be used, the extension data must be removed and re-initiated with the correct instrument type (ITYPE). If the terminal is not the correct one, but the extension data is correct, replace the terminal. The alarm must be manually cleared when the extension is re-initiated with the correct ITYPE.

## 2 DOMAIN 1 - SES

### 2.1 FAULT CODE 1:1 - HIGH CPU LOAD

#### 2.1.1 DESCRIPTION OF FAULT CODE

This alarm is indicating that the CPU, processor is constantly working so that the idle process is not reached. Normally this is an indication that there are applications working in an abnormal way in the processor, or that there are too many applications running on the processor.

#### 2.1.2 MEASURE

1. Log in (as root) to the system. Key the command *alarm* to print (list) alarms in the alarm log.
2. Is the alarm still present?
3. NO: Continue to step 6.
4. YES: Are there any processes that are orphans?
5. YES: Continue to step 9.
6. NO: Key the linux command **top** to list processes that are running.
7. Is the idle process running at all?
8. NO: monitor the **top** command to see if some processes are sporadically using too much CPU power.  
Is any process using CPU power intermittently?  
NO: It seems the processor running the application is too weak. A reconfiguration to minimize the number of active applications are recommended. However, a restart of the processor might remedy the problem. Keep a printout of **ps -ax** for further reference. Make a reboot at a convenient time and compare printouts. An investigation of the applications running on the system is recommended together with an applications expert to determine what changes to the configuration that can be made.  
YES: Continue to step 9.
9. YES: What programs are consuming most processor time? If a process is consuming the major part of the available processor power check what system function it is providing.
10. Is the application a telephony application?
11. YES: Reload/restart the application with the command *restart*. If the fault is recurring make a core dump with the linux command **core\_dump** for diagnostic use prior to the restart.  
Continue to step 13.
12. NO: Is the application a system function (daemon)?
13. YES: Restart the function as root by typing */etc/init.d/function\_name restart*.  
Continue to step 17.

14. NO: Is the process started from a shell and not running any necessary process?
15. NO: Restart the processor when convenient, after keeping a printout of **ps -ax**. Compare the printout with a new **ps -ax** printout in the just restarted CPU. Check if the offending process is present but working ok, in this case check if any other differences are noted. If the problem is persistent report the problem to the vendor of the problematic application.
16. YES: Key the linux command **kill -9 xxx** to end the rouge process xxx.
17. Key the command **top** to list the processes that are running. Make sure that the load condition has ended, that is, the idle process is running.
18. Is the alarm 1:1 denoted to severity level 1?
19. Consult an expert.

## 2.2 FAULT CODE 1:2 - ALARM BLOCK, AL, COULD NOT READ CONFIGURATION FILE

### 2.2.1 DESCRIPTION OF FAULT CODE

The alarm log program unit AL has three different configuration files:

- /opt/eri\_sn/etc/alarm\_severity.conf
- /opt/eri\_sn/etc/alarm\_text.conf
- /opt/eri\_sn/etc/alarm\_log.conf

This alarm is a result of that AL failed to read one or several of these files. Possible cause can be:

- a file does not exist
- a file does not exist
- the file content is garbled
- the file has been edited and a syntax error was introduced

### 2.2.2 MEASURE

1. Key the command **alarm** to print (list) alarms in the alarm log and analyze the information.
  2. Can you find the problem in the information listed?
  3. YES: Correct the problem
  4. NO: Make sure the correct files (as supplied by Mitel) are present at the correct path.
  5. Key the command **alarm** to erase (reset) alarms in the alarm log.
  6. Key the command **alarm\_cfg** to read the configuration files again
  7. Key the command **alarm** to print (list) alarms in the alarm log and check if the problem still exist
- Does the alarm still exist?

8. YES: Key the command alarm to print (list) alarms in the alarm log and analyze the information.
9. Has the information changed since step 1?
10. YES: Start again from the beginning.
11. NO: Consult an expert

## 2.3 FAULT CODE 1:3 - CONFIGURATION OF DMDR DATA-BASE ACCESS IS INVALID

### 2.3.1 DESCRIPTION OF FAULT CODE

-

### 2.3.2 MEASURE

1. Print data - use the command *callinfo\_status\_print -output all* to print current data.
2. Change data - use the command *callinfo\_output\_set* to correct the setup.

## 2.4 FAULT CODE 1:4 - WRITE TO SMDR DATABASE FAILED

### 2.4.1 DESCRIPTION OF FAULT CODE

When trying to write to the output unit it was not possible to send any data to the unit.

### 2.4.2 MEASURE

1. Use the command *alarm -p --format full*. The “Additional text” field, will explain the problem in greater detail.

The reason can be:

- The database does not exist.
- Directory does not exist.
- User has no access rights.
- The output (V24/printer/TCP) can not write data to the device. That is, there could be a buffer full, device off-line, cable problems, application/driver not running and so on.
- The target computer exists but is changed or reconfigured.
- The target computer does not exist.

2. Use the linux commands *ping* and *traceroute*.

With these commands it is possible to examine the network configuration, and to determine if the network path to the host is working.

## 2.5 FAULT CODE 1:5 - CONNECT TO SMDR DATABASE FAILED

### 2.5.1 DESCRIPTION OF FAULT CODE

Failure to connect to the output is generally due to media or cable problems. (DNS is not used to find the target machine as DNS look up in a real time applications affects performance.)

### 2.5.2 MEASURE

1. Use the command *alarm -p --format full*. The “Additional text” field, will explain the problem in greater detail.  
The reason can be:
  - Directory does not exist.
  - User has no access rights.
  - IP address/Hostname or port is faulty.
2. Print the configuration. Use the command *callinfo\_status\_print -output all* to print current data. Check that the server data is valid.
3. Use the linux commands *ping* and *traceroute*.  
With these commands it is possible to examine the network configuration, and to determine if the network path to the host is working.

## 2.6 FAULT CODE 1:6 - SPEECH QUALITY VALUE AT RED LEVEL

### 2.6.1 DESCRIPTION OF FAULT CODE

The quality of service alarm function has detected that a number of calls has had a bad speech quality. The cause of this are probably due to the configuration of the devices involved in the calls. The data that was used to trigger the alarm can be found in the call logging output data, if call logging was enabled and was storing the Quality of Service, QoS data.

### 2.6.2 MEASURE

1. Use the command *callinfo\_limit\_print* to see the current status of the supervision function and the specified alarm levels used.
2. If possible analyse the call logging data at the time of the alarm. Look for call records where the *a2bSimpleR\_value* or *b2aSimpleR\_value* are less than the bad limit.
3. These faulty samples should the be examined to determinate if the RTCP addresses used in these calls can be affiliated with a certain path in the network or some common equipment or bottle necks. Try to investigate if the path in the network has the necessary bandwidth to cope with the RTCP traffic currently allocated to it.

- Use external “sniffers” to examine the load in the network.
- Examine logs in routers and gateways if possible.
- Use external measurement tools to do analysis of traffic paths.
- Examine the use of Diffserv Code Point values in the network. See the file */etc/system\_conf.xml*, for values used in the telephony application. The network might not use diffserv to prioritize between real time applications, in this case, please consider to enable diffserv if possible.

## 2.7 FAULT CODE 1:7 - SPEECH QUALITY VALUE AT YELLOW LEVEL

### 2.7.1 DESCRIPTION OF FAULT CODE

The quality of service alarm function has detected that a number of calls has had a poor speech quality. The cause of this are probably due to the configuration of the devices involved in the calls. The data that was used to trigger the alarm can be found in the call logging output data, if call logging was enabled and was storing the Quality of Service, QoS data.

### 2.7.2 MEASURE

1. Use the command *callinfo\_limit\_print* to see the current status of the supervision function and the specified alarm levels used.
2. If possible analyse the call logging data at the time of the alarm. Look for call records where the *a2bSimpleR\_value* or *b2aSimpleR\_value* are less than the warning limit.
3. These faulty samples should be examined to determinate if the RTCP addresses used in these calls can be affiliated with a certain path in the network or some common equipment or bottle necks.

Try to investigate if the path in the network has the necessary bandwidth to cope with the RTCP traffic currently allocated to it.

- Use external “sniffers” to examine the load in the network.
- Examine logs in routers and gateways if possible.
- Use external measurement tools to do analyses of traffic paths.
- Examine the use of Diffserv Code Point values in the network. See the file */etc/system\_conf.xml*, for values used in the telephony application. The network might not use diffserv to prioritize between real time applications, in this case, please consider to enable diffserv if possible.

## 2.8 FAULT CODE 1:8 - CALL INFORMATION OUTPUT QUEUE ALMOST FULL

### 2.8.1 DESCRIPTION OF FAULT CODE

Output to SQL database, V24 (serial line) and TCP/IP is done asynchronously. This means that when a call information record is produced, it is put in an output FIFO queue. Queued records from the output FIFO queue is then written out as fast as the flow control allows.

This alarm indicates that the output FIFO queue is almost full. No information has yet been lost, but the safety margin is too small. (If the queue gets totally full you will get alarm Alarm 1:4 Failed while writing to call information output.)

### 2.8.2 MEASURE

The current number of queued records in the output FIFO queues can be examined with the command *callinfo\_status\_print*.

Possible reasons for this alarm are:

- The throughput of the media (V24, ethernet, database) is too low to cope with the call rate of the exchange.  
If this is the case, consider using a faster media, or splitting the output to several parallel media.
- Due to an external disturbance (like LAN hick-up) the throughput of the media (V24, ethernet, database) was temporarily lowered or stopped.  
If this is the case, consider what can be done to avoid future disturbances.
- The network connectivity is broken, and the information records are being queued up.  
If this is the case, fix the network.

## 2.9 FAULT CODE 1:9 - SAFETY BACKUP PASSED

### 2.9.1 DESCRIPTION OF FAULT CODE

This fault code does not indicate any fault. It just tells that a safety backup has been performed to satisfaction.

Safety backups are performed as periodic background jobs. The only way to indicate that the job has been performed is through the event log, and thus as a fault code. For further information about the safety backup, see operational directions for *ADMINISTRATOR USER'S GUIDE* section SAFETY BACKUP.

### 2.9.2 MEASURE

No measure is needed.

The fault code is normally disabled. It can be enabled by modifying the file *eri\_sn\_safety\_backup*.

## 2.10 FAULT CODE 1:10 - SAFETY BACKUP FAILED

### 2.10.1 DESCRIPTION OF FAULT CODE

When a safety backup is performed, preselected directories and files are copied to an external data store, for example, a tape in a tape station. The alarm indicates that the system could not access this device in a satisfactory way.

### 2.10.2 MEASURE

The settings for the safety backup can be found in the file `/etc/opt/eri_sn/safety_backup.conf`. Arguments that can be set are, for example, the path to where the backup device is mounted, and the directories or files that are to be stored, and if the tape is to be rewound or not. For more informations, see operational directions for *ADMINISTRATOR USER'S GUIDE*.

To avoid this alarm, make sure that the configuration file is in sync with the device that you are using, that is, that the content of the file is correct.

## 2.11 FAULT CODE 1:11 - FAULTY PCM LINE

### 2.11.1 DESCRIPTION OF FAULT CODE

The GJUL board has received information about a fault on the PCM line, which means that the system has found a fault in the transmission equipment, or discovered that the cable is disconnected at either LIM or group switch side.

Different alarm types can cause this alarm:

- AIS, Alarm Indication Signal, is issued if 1 only exists in all bits on all of the time slots of the PCM link.
- Frame Locking Fault, is issued when three consecutive frames shows incorrect information in the synchronization word.
- Signal Channel Fault (T16).
- Signal Loss in GJUL, the signal is lost when the outgoing signal buffer is full and a further signal arrives. In other words the last signal to arrive will be lost.

To get more specific information on what the alarm has generated, key command `pcm_status`.

### 2.11.2 MEASURE

1. Key command `pcm_status`, to check the status of the indicated PCM link.
2. Connect the cable, correct the faulty transmission equipment or replace faulty equipment.
3. Wait until the supervision check is completed and the alarm is cleared.  
This can take some time.



## 2.12 FAULT CODE 1:12 - FAULTY GJUG BOARD

### 2.12.1 DESCRIPTION OF FAULT CODE

All links connected to this board are discovered to be faulty. The Media for up to 4 LIMs can be affected. Detail description of the fault informs which PCM lines that are affected. This can have bin inpackt on traffic depending on configuration.

While replacing the GJUG board, a cable is not connected this will result in a new 1:11 alarm.

### 2.12.2 MEASURE

1. Check the detailed information of the alarm, to see which LIMs that are affected.
2. Change the faulty hardware.
3. Wait until the supervision check is completed and the alarm is cleared.  
This can take some time.
4. Check that no new alarms are raised.

## 2.13 FAULT CODE 1:13 - FAULTY GSM

### 2.13.1 DESCRIPTION OF FAULT CODE

All PCM links in a group switch module (GSM) are reported faulty.

At power failure or faulty GCU2 board, check if the displays on the GCU2 and the GSU boards reports any errors. For more information, see the operational directions for *GROUP SWITCH*.

A detailed description of the fault, will show which PCM links that are affected.

This will have big impact on traffic depending on configuration. There can be disturbances on the synchronization, which can cause disturbance on other LIMs not connected to this GSM and generate more alarms.

This can cause parity errors in the group switch. Use pcm\_order to clear the control memory.

**Note:** Clearing of the control memory causes disturbance on the traffic.

### 2.13.2 MEASURE

1. Is the power on?
2. NO: Check the GCU board and power supply.
3. YES: Check status of the indicated GSM.
4. Does the GCU2 board indicate fault?
5. Handle the faults indicated by the GCU2 board.
6. If the faulty GSM is the master GSM, check that the spare master GSM (if one exists) has taken over the responsibility.
7. Replace the faulty equipment.

8. Wait until the supervision check is completed and the alarm is cleared.  
This can take some time.
9. Check that no new alarm is raised.

## 2.14

## FAULT CODE 1:14 - GROUP SWITCH HAS BEEN ORDERED TO RESYNCHRONIZE TOO MANY TIMES

### 2.14.1

#### DESCRIPTION OF FAULT CODE

This alarm is raised when the system has given the group switch a synchronization order 3 times during 1 hour.

If the GCU2 board, in the master or spare master GSM, indicate that the GSM is using interim clock for synchronization use `pcm_synchronization` to resynchronize the group switch.

The system can not order resynchronization automatically as long as this alarm is valid. Which means that when the system has noticed a fault and wanted to resynchronize the group switch, it was not allowed. It is strongly recommended to manually order the group switch to resynchronize.

Things that can result in a resynchronization is, for example, "Faulty PCM link" or "Device board faulty or missing".

If the system has been stable, that is the system has not detected any reason for a resynchronization, during one hour the alarm will be cleared.

### 2.14.2

#### MEASURE

1. Check that the master and reserve GSM is not using the interlim clock for synchronization.
2. Key command `pcm_synchronization` to order a resynchronization of the group switch.
3. Check what has caused the resynchronization. Check and repair other alarms.  
This can take some time.
4. When all alarms are cleared.  
Key command `alarm` to erase (reset) alarms in the alarm log. This will remove the stop of further system ordered resynchronizations.

## 2.15

## FAULT CODE 1:15 - GSM IS MANUALLY BLOCKED

### 2.15.1

#### DESCRIPTION OF FAULT CODE

This alarm is raised when the GSM has been blocked manually, with command `pcm_order`.

The alarm will be cleared when the GSM is deblocked.

Manually blocked will hide new incoming alarms for the manually blocked device.

## 2.15.2

### MEASURE

Key command *pcm\_order* to deblock the GSM, which will clear the alarm.

## 2.16

### FAULT CODE 1:16 - GJUG MULTIPLE IS MANUALLY BLOCKED

#### 2.16.1

##### DESCRIPTION OF FAULT CODE

This alarm is raised when the GJUG multiple has been blocked manually, with command *pcm\_order*.

The alarm will be cleared when the GJUG multiple is deblocked.

Manually blocked will hide new incoming alarms for the manually blocked device.

#### 2.16.2

##### MEASURE

Key command *pcm\_order* to deblock the GJUG multiple, which will clear the alarm.

## 2.17

### FAULT CODE 1:17 - GROUP SWITCH SIDE IS MANUALLY BLOCKED

#### 2.17.1

##### DESCRIPTION OF FAULT CODE

This alarm is raised when a group switch side has been blocked manually, with command *pcm\_order*.

The alarm will be cleared when the group switch side is deblocked.

Manually blocked will hide new incoming alarms for the manually blocked device.

#### 2.17.2

##### MEASURE

Key command *pcm\_order* to deblock the group switch side, which will clear the alarm.

## 2.18

### FAULT CODE 1:18 - CLOCK CONTROLLING LINE HANDLING

#### 2.18.1

##### DESCRIPTION OF FAULT CODE

This alarm is for information only, it will be received once and if it is cleared it will not recur until a new fault occurs.

A PCM line has been removed with command *pcm\_config*. That line was a clock controlling line.

The group switch wants to have 3 clock controlling LIMs.

## 2.18.2

## MEASURE

1. Check the synchronization order.
2. Give a new synchronization order, if it is needed.

## 2.19

## FAULT CODE 1:19 - FAULTY TIME SWITCH IN GROUP SWITCH

## 2.19.1

## DESCRIPTION OF FAULT CODE

Supervision of a PCM line can detect that it is not possible to signal over its own time switch board, even if the line is otherwise ok.

The alarm is cleared, when the first line succeeds to signal over the time switch.

## 2.19.2

## MEASURE

1. Check display and led on the time switch board.
2. Check cable.
3. Change the time switch board.

## 2.20

## FAULT CODE 1:21 - BACKUP OF LDAP DATA HAS FAILED

## 2.20.1

## DESCRIPTION OF FAULT CODE

Dump of ldap data to backup has failed. The fault code is issued per LIM. This fault is more severe if it happens in the ldap master LIM (normally LIM1).

That is because the ldap backup version in the ldap master is used at restore of ldap data.

## 2.20.2

## MEASURE

1. Do a `data_backup`. Wait for the *data\_backup* to complete. Is the alarm still raised?  
NO: Stop.
2. YES: Is the hard disk on the server full?  
Check with command `df/var/opt/eri_sn`  
YES: Cleanup on the hard disk and make another data backup to get rid of the fault.  
Stop.
3. NO: Use the command `/etc/init.d/eri_ldap status` to check if the ldap resource is running:  
Is it running?  
YES: Contact an expert

**Note:** Must be executed with root privileges.

4. NO: Use the command `/etc/init.d/eri_ldap start`

Does it start?

NO: Contact an expert.

**Note:** Must be executed with root privileges.

5. YES: Do a data backup. Wait for the data backup to complete.

Is the alarm still raised?

NO: Stop

YES: Contact an expert.

## 2.21 FAULT CODE 1:22 - ROLLBACK OF LDAP DATA HAS FAILED

### 2.21.1 DESCRIPTION OF FAULT CODE

As a part of certain system initiated error recovery routines, the ldap data in all LIMs may be reloaded from a backup in order to reset the system to the last known state with data consistency. This means that all changes made since the latest dump occasion will be lost.

Examples of such recovery measures are data reload as a part of LIM reload and data reload when a command that alters exchange data fails to be completed. This fault code is raised if rollback of ldap data fails. One reason for it to fail is that the server where the ldap master is running is unreachable.

### 2.21.2 MEASURE

1. Is Fault code 34 LIM out of order for the ldap master server present in the alarm log.  
Normally LIM 1  
YES: Handle fault code 34.  
Stop
2. NO: Do a data\_restore. Wait for the data\_restore to complete. Is the alarm still raised?  
NO: Stop.
3. YES: Is it possible to log on to the ldap master server with ssh?  
NO: Contact and expert.  
Stop.
4. YES: Use the command `/etc/init.d/eri_ldap status` to check if the ldap resource is running.  
Is it running?  
YES: Contact an expert

**Note:** Must be executed with root privileges.

5. NO: Use the command `/etc/init.d/eri_ldap start`  
Does it start?  
NO: Contact an expert

**Note:** Must be executed with root privileges.

6. YES: Do a data\_restore. Wait for the data\_restore to complete. Is the alarm still raised?  
NO: Stop.  
YES: Contact an expert.

## 2.22 FAULT CODE 1:23 - ROLLBACK OF LDAP DATA SUCCESSFUL

### 2.22.1 DESCRIPTION OF FAULT CODE

As a part of certain system initiated error recovery routines, the ldap data in all LIMs may be reloaded from a backup in order to reset the system to the last known state with data consistency. This means that all changes made since the latest dump occasion will be lost.

Examples of such recovery measures are data reload as a part of LIM reload and data reload when a command that alters exchange data fails to be completed.

### 2.22.2 MEASURE

1. subflow 3  
The fault code does not indicate any fault but is merely informative.
2. Are there any other fault codes in the alarm log?  
YES: subflow 4  
NO: subflow 12
3. Return to the main flow.

## 2.23 FAULT CODE 1:24 - CANNOT WRITE TO MASTER LDAP

### 2.23.1 DESCRIPTION OF FAULT CODE

A program unit has detected that it cannot write to the master LDAP. (The program unit that is most likely to detect this and raise the alarm is DBOVR.).

This can be caused by a broken network connection to the master LDAP host, the master LDAP host being down, LDAP not running on the master LDAP host, or LDAP errors on the master host.

### 2.23.2 MEASURE

1. Use the diagnostic\_ldap command collect LDAP status data.
2. Print the full alarm information using *alarm-p - format detail* or *alarm-p - format full*.  
  
The additional text field usually has some extra information that is useful.
3. Check if you also have the alarms  
1:25 Broken connection to master LDAP,  
1:28 Master LDAP out of order, or

1:29 Local LDAP server not running.  
In that case attend to those alarms first.

Repairing that fault will most likely repair this fault also.

4. Read the **/var/log/messages** and check for more information that can explain the problem.
5. Use the *host* command on all involved LIMs to verify that the host name to IP address (and reverse) lookup works OK. All LIMs shall be able to translate all other LIM names.
6. Use the *ping* command to verify that you have network connectivity between all LIMs.
7. Use the *date* command to verify that all LIMs have the same time. Check that NTP (Network Time Protocol) is running OK.
8. Use the *df* command on the LDAP master and on the LIM sending the alarm, to verify that no disk partition is full.
9. Use the *mount* command to verify that the file systems are mounted *read-write* and not *read-only*.
10. On all involved LIMs (LDAP master and replicas) check the file permission. Use the command  
  
*ls -lr /var/opt/eri\_sn/ldap*  
  
The group "ldap" shall have write permissions.
11. If nothing else helps, do */etc/init.d/eri\_ldap restart* on the LDAP master
12. Restart the system by the command *restart --system*
13. If nothing above has solved the problem, stop the master LDAP, clear away binary data-base files, and then start the master LDAP. This will force the master LDAP server to read everything from the LDIF file created at the last data\_backup.  
  
  - */etc/init.d/eri\_ldap stop*
  - *rm /var/opt/eri\_sn/ldap/master/\**
  - *rm /var/opt/eri\_sn/ldap/local/\**
  - *rm /var/opt/eri\_sn/ldap/recovery/\*/\**
  - */etc/init.d/eri\_ldap start*
14. Contact an expert.

## 2.24

## FAULT CODE 1:25 - BROKEN CONNECTION TO MASTER LDAP

### 2.24.1

### DESCRIPTION OF FAULT CODE

The IP connection to the master LDAP server is broken. This can be caused by broken network connection to the master LDAP host, the master LDAP host being down, LDAP not running on master LDAP host or LDAP errors on the master host.

### 2.24.2

### MEASURE

1. Use the *diagnostic\_ldap* command collect LDAP status data.

2. Print the full alarm information using *alarm-p - format detail* or *alarm-p - format full*.  
The additional text field usually has some extra information that is useful.
3. Check if you also have the alarms  
1:26 Broken connection to local LDAP server, or  
1:29 Local LDAP server not running.  
In that case attend to those alarms first.  
Repairing that fault will most likely repair this fault too.
4. Check if you also have the alarms  
1:27 Local LDAP out of order, or  
1:28 Master LDAP out of order.  
In that case look into those alarms too to gather information.
5. Read */var/log/messages* and check for more information that can explain the problem.
6. Use the *host* command on all involved LIMs to verify that the host name to IP address (and reverse) lookup works OK. All LIMs shall be able to translate all other LIM names.
7. Use the *ping* command to verify that you have network connectivity between all LIMs.
8. Use the *date* command to verify that all LIMs have the same time. Check that NTP (network time protocol) is running OK.
9. Use the *df* command on the LDAP master and on the LIM sending the alarm to verify that no disk partition is full.
10. Use the *mount* command to verify that the file systems are mounted *read-write* and not *read-only*.
11. On all involved LIMs (LDAP master and replicas) check the file permission using the command  
*ls -lr /var/opt/eri\_sn/ldap*. The group *ldap* shall have write permissions.
12. If nothing else helps, do */etc/init.d/eri\_ldap restart* on the LDAP master.
13. Restart the system by the command *restart --system*.

## 2.25 FAULT CODE 1:26 - BROKEN CONNECTION TO LOCAL LDAP

### 2.25.1 DESCRIPTION OF FAULT CODE

The IP connection to the LDAP server on local host was broken. This can be caused by incorrect network configuration, LDAP not running on localhost, or LDAP errors on this computer.

### 2.25.2 MEASURE

1. Use the *diagnostic\_ldap* command collect LDAP status data.
2. Print the full alarm information using *alarm-p - format detail* or *alarm-p - format full*.



The additional text field usually has some extra information that is useful.

3. Check if you also have the alarms  
1:25 Broken connection to master LDAP,  
1:28 Master LDAP out of order, or  
1:29 Local LDAP server not running.  
In that case attend to those alarms first.  
  
Repairing that fault will most likely repair this fault too.
4. Read `/var/log/messages` and check for more information that can explain the problem.
5. Use the `host` command on all involved LIMs to verify that the host name to IP address (and reverse) lookup works OK. All LIMs shall be able to translate all other LIM names.
6. Use the `ping` command to verify that you have network connectivity between all LIMs.
7. Use the `date` command to verify that all LIMs have the same time. Check that NTP (network time protocol) is running OK.
8. Use the `df` command on the LDAP master and on the LIM sending the alarm to verify that no disk partition is full.
9. Use the `mount` command to verify that the file systems are mounted *read-write* and not *read-only*.
10. On all involved LIMs (LDAP master and replicas) check the file permission using the command `ls -lr /var/opt/eri_sn/ldap`. The group `ldap` should have write permissions.
11. If nothing else helps, do  
  
`/etc/init.d/eri_ldap restart` on the LDAP master.
12. Restart the system by the command `restart --system`
13. If nothing above has solved the problem, stop the master LDAP, clear away binary data-base files, and then start the master LDAP. All data will be replicated from the master LDAP server.
  - `/etc/init.d/eri_ldap stop`
  - `rm /var/opt/eri_sn/ldap/master/*`
  - `rm /var/opt/eri_sn/ldap/local/*`
  - `rm /var/opt/eri_sn/ldap/recovery/*/*`
  - `/etc/init.d/eri_ldap start`
14. Contact an expert.

## 2.26

## FAULT CODE 1:27 - LOCAL LDAP OUT OF ORDER

### 2.26.1

### DESCRIPTION OF FAULT CODE

The IP connection to the local LDAP server is operational, but the local LDAP server cannot give reasonable answers to queries.

### 2.26.2

### MEASURE

1. Use the `diagnostic_ldap` command collect LDAP status data.

2. Print the full alarm information using *alarm-p - format detail* or *alarm-p - format full*.  
The additional text field usually has some extra information that is useful.
3. Check if you also have the alarms  
1:25 Broken connection to master LDAP,  
1:26 Broken connection to local LDAP,  
1:28 Master LDAP out of order, or  
1:29 Local LDAP server not running.  
In that case attend to those alarms first.  
  
Repairing that fault will most likely repair this fault also.
4. If you have a newly started system, or you have had problems with the LDAP master recently, wait a few moments to see if replication from the LDAP master repairs this automatically
5. Read the */var/log/messages* and check for more information that can explain the problem.
6. Use the *host* command on all involved LIMs to verify that the host name to IP address (and reverse) lookup works OK. All LIMs should be able to translate all other LIM names.
7. Use the *ping* command to verify that you have network connectivity between all LIMs.
8. Use the *date* command to verify that all LIMs have the same time. Check that NTP (Network Time Protocol) is running properly.
9. Use the *df* command on the LDAP master and on the LIM sending the alarm, to verify that no disk partition is full.
10. Use the *mount* command to verify that the file systems are mounted *read-write* and not *read-only*.

11. On all involved LIMs (LDAP master and replicas) check the file permission. Use the command  
`ls -lr /var/opt/eri_sn/ldap`  
 The group ldap should have write permissions.
12. If nothing else helps, do `/etc/init.d/eri_ldap restart` on the LDAP master.
13. Restart the system by the command `restart --system`
14. If nothing above has solved the problem, stop the master LDAP, clear away binary database files, and then start the master LDAP. This will force the master LDAP server to read everything from the LDIF file created at the last data\_backup.
  - `/etc/init.d/eri_ldap stop`
  - `rm /var/opt/eri_sn/ldap/master/*`
  - `rm /var/opt/eri_sn/ldap/local/*`
  - `rm /var/opt/eri_sn/ldap/recovery/*/*`
  - `/etc/init.d/eri_ldap start`
15. Contact an expert.

## 2.27 FAULT CODE 1:28 - MASTER LDAP OUT OF ORDER

### 2.27.1 DESCRIPTION OF FAULT CODE

The IP connection to the local LDAP server is operational, but the local LDAP server cannot give reasonable answers to queries.

### 2.27.2 MEASURE

1. Use the `diagnostic_ldap` command collect LDAP status data.
2. Print the full alarm information using `alarm-p - format detail` or `alarm-p - format full`.  
 The additional text field usually has some extra information that is useful.
3. Check if you also have the alarms  
 1:25 Broken connection to master LDAP, or  
 1:29 Local LDAP server not running.  
 In that case attend to those alarms first.  
 Repairing that fault will most likely repair this fault also.
4. Read the `/var/log/messages` and check for more information that can explain the problem.
5. Use the `df` command on the LDAP master and on the LIM sending the alarm, to verify that no disk partition is full.
6. Use the `mount` command to verify that the file systems are mounted *read-write* and not *read-only*.
7. On all involved LIMs (LDAP master and replicas) check the file permission. Use the command  
`ls -lr /var/opt/eri_sn/ldap` The group ldap should have write permissions.
8. If nothing else helps, do `/etc/init.d/eri_ldap restart` on the LDAP master.

9. Restart the system by the command `restart --system`
10. If nothing above has solved the problem, stop the master LDAP, clear away binary database files, and then start the master LDAP. This will force the master LDAP server to read everything from the LDIF file created at the last `data_backup`.
  - `/etc/init.d/eri_ldap stop`
  - `rm /var/opt/eri_sn/ldap/master/*`
  - `rm /var/opt/eri_sn/ldap/local/*`
  - `rm /var/opt/eri_sn/ldap/recovery/*/*`
  - `/etc/init.d/eri_ldap start`
11. Contact an expert.

## 2.28 FAULT CODE 1:29 - LOCAL LDAP SERVER NOT RUNNING

### 2.28.1 DESCRIPTION OF FAULT CODE

The LDAP server process on localhost (of the LIM sending the alarm) is not running. When sending this alarm the LDAP supervisor program (LDAPSUP) will periodically try to restart the local LDAP server.

### 2.28.2 MEASURE

1. Use the `diagnostic_ldap` command collect LDAP status data.
2. Print the full alarm information using `alarm-p - format detail` or `alarm-p - format full`.  
The additional text field usually has some extra information that is useful.
3. If the alarm is very new, wait for 5 minutes to see if LDAPSUP manages to restart the local LDAP server.
4. Read `/var/log/messages` and check for more information that can explain the problem.
5. Use the `df` command on the LDAP master and on the LIM sending the alarm to verify that no disk partition is full.
6. Use the `mount` command to verify that the file systems are mounted *read-write* and not *read-only*.
7. On all involved LIMs (LDAP master and replicas) check the file permission using the command `ls -lr /var/opt/eri_sn/ldap`. The group `ldap` should have write permissions.
8. If nothing else helps, do `/etc/init.d/eri_ldap restart` on the LDAP master.
9. Restart the system by the command `restart --system`

10. If nothing above has solved the problem, stop LDAP, clear away binary database files, and then start LDAP. On master this will force the master LDAP server to read everything from the LDIF file created at last data\_backup. On replica the data will be replicated from master.
  - `/etc/init.d/eri_ldap stop`
  - `rm /var/opt/eri_sn/ldap/master/*`
  - `rm /var/opt/eri_sn/ldap/local/*`
  - `rm /var/opt/eri_sn/ldap/recovery/*/*`
  - `/etc/init.d/eri_ldap start`
11. Contact an expert.

## 2.29 FAULT CODE 1:30 - THERE ARE ANALYZED CORE FILES TO REPORT

### 2.29.1 DESCRIPTION OF FAULT CODE

The command *check\_core\_files* (usually run scheduled as a cron job) has detected that there are analyzed core files on your system. A zip archive file with the analyzed core files is stored in */tmp*.

A core file is created at some program crashes and contains information about the state of the program that crashed. The core files can be analyzed automatically by *check\_core\_files*, user initiated by running the command *core\_report*, or manually by a skilled service engineer using a debugger. If the analysis is done by *check\_core\_files* or *core\_report*, the analysis creates a zip archive file with collected relevant information regarding the crash. The zip archive file holds text files with analyzed information about the cause of the crash. The program designer uses the information in this zip archive file to correct the program that crashed.

### 2.29.2 MEASURE

1. Check the alarm list to see which LIM is affected.
2. Log into the affected LIM and move the zip archive file from */tmp* to a safe location, for example, an administrative computer.
3. Contact your service partner to report the trouble in the system. Attach the zip archive file with the analyzed core information to the trouble report.

## 2.30 FAULT CODE 1:31 - TOO MUCH MEMORY PAGING

### 2.30.1 DESCRIPTION OF FAULT CODE

This alarm indicates that there has been too much memory paging (also known as page faults).

Memory paging happens when the operating system has to fetch program (binary) code from disk into RAM to continue executing the program. This is normal at program startup, but it will also happen when a system has too little physical memory and processes are paged (partly swapped) to disk.

A small amount of memory paging is normal. Excessive memory paging severely decreases the system performance. If possible ensure that memory intensive processes, for example **Safety backup**, are always run at low traffic time.

## 2.30.2

## MEASURE

1. Print the complete alarm information using *alarm*. Check the additional text field of the alarm for more information.
2. Use commands like *top* and *vmstat* to investigate why there is a shortage of physical memory.
3. Is any process abnormally big? Are big programs running that should not run on the MX-ONE Service Node? Do you need to add more physical memory (RAM)?
4. If you cannot find an obvious cause and correct it, contact an expert.

## 2.31

## FAULT CODE 1:32 - SLOW EVENT RESPONSE

## 2.31.1

## DESCRIPTION OF FAULT CODE

The event response time supervision has detected that the process on the MX-ONE Service Node react too slowly to events. The most likely cause of this situation is an overloaded CPU.

## 2.31.2

## MEASURE

1. Print the complete alarm information using *alarm*. Check the additional text field of the alarm for more information.
2. Use commands like *top* and *vmstat* to investigate why the processes reacts so slowly to events.
3. Are more telephony traffic running than the system is designed for? Is there any process consuming a lot of CPU?
4. If you cannot find an obvious cause and correct it, contact an expert.

## 2.32

## FAULT CODE 1:33 - INTER-LIM CONNECTION IS LOST

## 2.32.1

## DESCRIPTION OF FAULT CODE

The supervision of inter-LIM communication has detected that some LIMs can not communicate with each other. Every LIM supervises its connections to other LIMs. The inter-LIM communication are using sctp/ip.

It is the LIM with lowest LIM number that is reachable for other LIMs, that is responsible for the alarm sending.

Most likely reasons for the fault are as follows:

- `eri_sn` is not running in the LIM
- Server is down

- Network faults, such as cables, switches, routers, network cards
- Misconfigured firewalls, routers or switches.

## 2.32.2

### MEASURE

1. Use command **status -interlim** to find out which network path that is failing.
2. Use command **status -interlim -d -lim** for the failing servers. If a detailed list is received for a LIM, **eri\_sn** is running on that server. Or log on locally to the failing servers to check if **eri\_sn** is running.  
Check with command **/etc/init.d/eri\_sn status**  
  
If all the server connections are up, the alarm is cleared automatically within 3 minutes.
3. Use **ping** to check if network path is working.  
  
Specify both local and remote address to use.
4. Use **tcpdump** or **wireshark** on both servers missing connection. Check for **sctp** messages between the servers. Check if **sctp** messages are being sent or received for the missing connection.
5. Are there firewalls in the network path blocking **sctp**? Use command **traceroute** to trace the ip traffic between the servers.
6. If you cannot find the cause of the fault, contact an expert.

## 2.33

### FAULT CODE 1:34 - CONFIG MIRROR HAS FAILED

## 2.33.1

### DESCRIPTION OF FAULT CODE

This alarm indicates that there is a communication error in the SSH server network.

## 2.33.2

### MEASURE

1. Check if there are other alarms indicating which server that is not reachable.  
Use the command **alarm -p --alarm-code all -format detail**
2. Use the **ping** command to locate the failing node.
3. When the failing node is located check its cable connections.
4. Is the SSH application running?  
As root, from LIM 1 run the command **ssh mxone\_admin@limx**, where **limx** is the address of the failing LIM.
5. If you cannot find any obvious cause and correct it, contact an expert.

## 2.34

### FAULT CODE 1:36 - HIGH LOAD IN PROGRAM UNIT

## 2.34.1

### DESCRIPTION OF FAULT CODE

This alarm indicates that job execution is delayed in a specific program. This happens if a high amount of jobs are executed in the program (overload), or if the server is

heavily (over) loaded by some other process or processes. The program unit reduces or restricts traffic internally when the alarm is raised.

## 2.34.2

## MEASURE

1. Print the complete alarm information. Use the command *alarm -p --format detail*. Check the additional text field of the alarm for more information
2. Use commands like *top* and *vmstat* to investigate if something in the system is misbehaving.
3. Is more telephony traffic running than what the system is designed for? Does any process consume much of the CPU power?
4. If you cannot find any obvious cause and correct it, contact an expert.

## 2.35

## FAULT CODE 1:37 - DATA BACKUP NEEDED

## 2.35.1

## DESCRIPTION OF FAULT CODE

This alarm is raised when the amount of uncommitted changes (the differences between the LDAP data and the most recent LDIF file) becomes dangerously large.

## 2.35.2

## MEASURE

Please run the command *data\_backup* at once.

For reference, see the operational directions for *ADMINISTRATOR USER'S GUIDE*, in the chapter *BACKUP AND RESTORE*.

## 2.36

## FAULT CODE 1:38 - LINUX SOFTWARE RAID ALERT

## 2.36.1

## DESCRIPTION OF FAULT CODE

The Raid disk supervision program has received an alert that the Linux Software Raid system needs attention.

**Note:** All raid management requires *root authority*.

## 2.36.1.1

*Schematic layout*

The Linux software RAID system is made up by two disks, normally named *sda* and *sdb*. Each disk has two partitions, *sda1* and *sda2*, and *sdb1* and *sdb2*, respectively.

The RAID partition *md0* is made up by *sda1* and *sdb1*. The RAID partition *md1* is made up by *sda2* and *sdb2*.



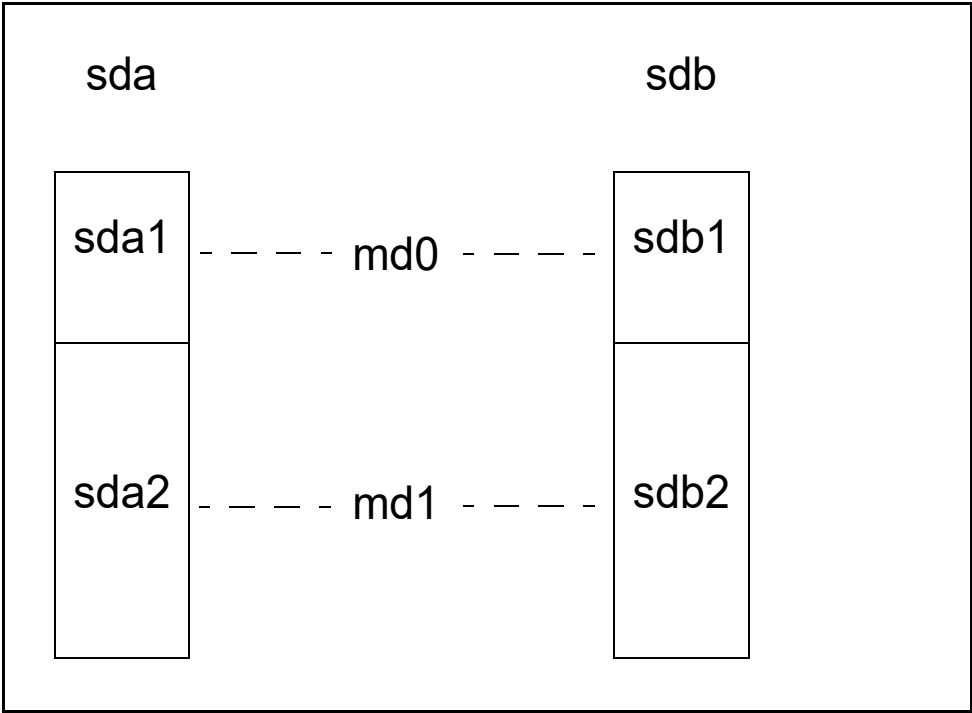


Figure 1: Schematic RAID layout

## 2.36.1.2

*Check status of Software Raid*

Key command *mdadm -D /dev/md<X>* or

```
/dev/md1:
Version: 00.90.03
Creation Time: Wed Jun 27 13:06:28 2012
Raid Level: Raid1
Array Size: 155774208 (148.56 GiB 159.51 GB)
Used Dev Size: 155774208 (148.56 GiB 159.51 GB)
Raid Devices: 2
Total Devices: 2
Preferred Minor: 1
Persistence: Superblock is persistent
Update Time: Fri Oct 19 14:37:23 2012
State: clean
Active Devices: 2
Working Devices: 2
Failed Devices: 0
Spare Devices: 0
UUID: 6d45f0eb:2604ac7f:68323a81:f45b2983
Events: 0.5279156
Number Major Minor RaidDevice State
  0      8      2      0      active sync /dev/sda2
  1      8     18      1      active sync /dev/sdb2
```

**Figure 2: Printout from command *mdadm -D /dev/md1* when RAID is OK. Both discs are available.**

```
/dev/md1:
Version: 00.90.03
Creation Time: Wed Jun 27 13:06:28 2012
Raid Level: raid1
Array Size: 155774208 (148.56 GiB 159.51 GB)
Used Dev Size: 155774208 (148.56 GiB 159.51 GB)
Raid Devices: 2
Total Devices: 2
Preferred Minor: 1
Persistence: Superblock is persistent
Update Time: Fri Oct 19 15:38:40 2012
State: clean, degraded
Active Devices: 1
Working Devices: 1
Failed Devices: 1
Spare Devices: 0
UUID: 6d45f0eb:2604ac7f:68323a81:f45b2983
Events: 0.5281601
Number Major Minor RaidDevice State
 0 0 0 0 removed
 1 8 18 1 active sync /dev/sdb2
 2 8 2 - faulty spare
```

**Figure 3: Printout from command *mdadm -D /dev/md1* when RAID is NOK. Only one disc is available.**

Use command `cat /proc/mdstat`

```
Personalities: [raid1] [raid0] [raid5] [raid4] [linear]
md1:   active raid1 sda2[0] sdb2[1]
      155774208 blocks [2/2] [UU]
md0:   active raid1 sda1[0] sdb1[1]
      513984 blocks [2/2] [UU]
unused devices: <none>
```

**Figure 4:** Printout from command `cat /proc/mdstat` when RAID is OK.

```
Personalities: [raid1] [raid0] [raid5] [raid4] [linear]
md1: active raid1 sdc2[2] sda2[3](F) sdb2[1]
      155774208 blocks [2/1] [_U]
[>.....] recovery = 0.1% (233024/155774208) finish=133.4min speed=19418K/sec
md0: active raid1 sdc1[0] sda1[2](F) sdb1[1]
      513984 blocks [2/2] [UU]
unused devices: <none>
```

**Figure 5:** Printout from command `cat /proc/mdstat` when new disk is initiated, recovery ongoing.

## 2.36.2

## MEASURE

1. Remove the two partitions of the failing disk from the Raid configuration.  
Take the following two commands, where {broken\_drive} is either sda or sdb.  

```
> mdadm --manage /dev/md0 --fail /dev/{broken_drive}1 \
--remove /dev/{broken_drive}1
> mdadm --manage /dev/md1 --fail /dev/{broken_drive}2 \
--remove /dev/{broken_drive}2
```

**Note:** If the /dev/{broken\_drive}X already has been removed the command will fail. Continue with step 2.
2. It is important that the system must be shut down before the faulty drive is physically replaced with a replacement drive, i. e. *hot-swap* is not recommended.  
The new disk should be of the same model and the same size as (or larger than) the one remaining drive (healthy one) in the system.  
Reboot the system. Normally the system will boot from the healthy disk in either drive 0 (drive 1 being replaced) or drive 1 (drive 0 being replaced).  
**Note:** If, for any reason, there is message indicating no boot disk found or there is no action shown on the monitor, reboot the system and press <F7> to enter the manual boot option in the BIOS. Choose the one to boot. Drive number is indicated as P0 (drive 0) or P1 (drive 1).
3. Check which drive letter that was assigned to the disk. Check the content of `/var/log/messages`. (The disk could, for example, get drive letter c, to be sdc.)
4. Prepare the new drive to get the same partitioning as the one in use.  

```
> sfdisk -d /dev/{good_drive} | sfdisk /dev/{new_drive} --Linux
```

5. Add the new disk to the RAID configuration.

**Note:** Adding new disk to the RAID configuration is very disc intensive activity and therefore should run at low traffic times.

```
> mdadm --manage /dev/md0 --add /dev/{new_drive}1
> mdadm --manage /dev/md1 --add /dev/{new_drive}2
```

6. Wait until the new disk has been mirrored (raid synchronized) from the operational disk.

```
> cat /proc/mdstat
```

Wait until the disk is 100% synchronized.

**Note:** If the result is a failed spare, it is removed after a reboot of the server. Continue with step 7.

7. Make the new drive bootable, that is, write to the Master Boot Record (MBR).

```
> grub
```

Enter the following commands in the grub shell.

```
> device (hd0) /dev/{new_drive}
> root (hd0,0)
> setup (hd0)
> quit
```

8. Enter the command alarm to erase (reset) alarms in the alarm log.

Clear the alarms.

## 2.37

## FAULT CODE 1:39 - NOT ENOUGH FREE SPACE ON DISK PARTITION

### 2.37.1

### DESCRIPTION OF FAULT CODE

The internal supervision has detected that one or more of the disk partitions used by the MX-ONE is becoming too filled. If there is not enough free space on these disk partitions, the MX-ONE will not be able to operate.

The disk partitions can become filled up for several different reasons:

- System maintenance.  
Manual system maintenance and installation typically involve copying files. If old unused files are left on the disk, the disk will eventually fill up.
- Log files.  
The log files in /var/log/messages can grow. Especially if the system is experiencing trouble the logging might become intensive and the log files might fill up the disk.
- Berkeley DB transaction log files.  
When configurations are made in the system the Berkeley DB transaction log files grow. These transaction log files are truncated during data\_backup. If too many configuration changes are made between data\_backups, the transaction log files might fill up the disk.
- Temporary files.  
Many users, and many programs create temporary files in either /tmp or /var/tmp. These files must be removed regularly.

## 2.37.2

### MEASURE

Type *alarm -p -f detail* to get the complete alarm information.

Look in the additional text field of the alarm, to find information about what partition is getting filled up.

Continue by using normal linux/Unix commands like *du* and *ls* to find the files that fill up the disk partition.

If the behavior is caused by:

- users or administrators leaving too many old files around - delete old un-needed files.
- log files in /var/log/messages - investigate the reason for the excessive logging (this might be another fault that must be solved). Then remove the log files (or move them to some off-line storage).
- Berkeley DB transaction log files in /var/opt/eri\_sn/ldap/... - then do data\_backup and the transaction log files should get truncated.
- Temporary files in /tmp or /var/tmp - just delete the temporary files.

Further information can be found in the operational directions for *ADMINISTRATOR USER'S GUIDE*, in the chapter *HARD DISK MAINTENANCE*.

## 2.38

### FAULT CODE 1:40 - MANDATORY DIRECTORY MISSING

#### 2.38.1

#### DESCRIPTION OF FAULT CODE

The internal supervision has detected that a mandatory file system directory no longer exists in the file system. Without the mandatory directory in the file system the MX-ONE will not be able to operate.

The most likely reason for a mandatory file system directory to no longer exist is that someone has deleted it. This can happen if the system administrator makes a serious mistake, and (less likely) if there is serious bug in installation and upgrade scripts.

#### 2.38.2

#### MEASURE

Type *alarm -p -f detail* to get the complete alarm information.

Look in the additional text field of the alarm, to find information about what mandatory file system directory is missing.

Contact Mitel service for expert advice on how to create the missing directory with suitable content.

As an alternative to contacting Mitel service the MX-ONE can be reinstalled from scratch.

## 2.39 FAULT CODE 1:50 - BOARD REVISION CONTROL

### 2.39.1 DESCRIPTION OF FAULT CODE

The internal board revision supervision has detected inconsistency on board revisions in the system

### 2.39.2 MEASURE

Type *alarm -p -f detail* to get the complete alarm information.  
Additional text field stipulate which issue needs to be rectified.

## 2.40 FAULT CODE 1:51 - TRACE STOPPED

### 2.40.1 DESCRIPTION OF FAULT CODE

A trace that was set for finding problems in the system has triggered.

### 2.40.2 MEASURE

Type *alarm -p -f detail* to get the complete alarm information.  
Use "trace -display" to display trace data. Contact the user who initiated the trace individual that was triggered, so further actions can be made.

## 2.41 FAULT CODE 1:52 - NO CONTACT WITH EXTERNAL DATABASE

### 2.41.1 DESCRIPTION OF FAULT CODE

The system has lost contact with an external database (for example an LDAP database for the blacklisting or alpha-tagging functions).

### 2.41.2 MEASURE

Type *alarm -p -f detail* to get the complete alarm information.  
Use this information to investigate the reason for the lost contact. Try to re-establish contact.

## 3 DOMAIN 2 - ACS

### 3.1 FAULT CODE 2:1 - CERTIFICATE EXPIRATION NOTIFICATION

#### 3.1.1 FAULT CODE DESCRIPTION

This alarm will be sent when there is less than 1 month left until the certificate expires. It will be sent once every day as a reminder and it will inform about the date of expiration. This alarm does not indicate that anything is wrong, it is just informational.

#### 3.1.2 MEASURES

Renew the certificate. See the operational directions for *CERTIFICATE MANAGEMENT*.

### 3.2 FAULT CODE 2:2 - CERTIFICATE EXPIRATION ALARM

#### 3.2.1 FAULT CODE DESCRIPTION

This alarm will be sent after the certificate has expired. It will be sent every day until a new certificate has been installed. This alarm means that there is no security available.

#### 3.2.2 MEASURES

Renew the certificate. See the operational directions for *CERTIFICATE MANAGEMENT*.

### 3.3 FAULT CODE 2:4 - SIP TRUNK HEART BEAT FAILED

#### 3.3.1 FAULT CODE DESCRIPTION

This alarm will be sent when the supervision of heart beat failed.  
No signal received during the time supervision from other end.  
Normally OPTIONS signaling is used as beat signal.

#### 3.3.2 MEASURES

Use command *alarm -p --format full*. The “Additional text” field will explain the problem in greater detail.

The reason can be:

- The connection does not exist.

- DNS entry does not exist.
- The target computer exists but is changed or reconfigured.
- The target computer does not exist.

Use the linux commands *ping* and *traceroute* to examine the network configuration, and determine if the network path to the host is working.

## 3.4 FAULT CODE 2:5 - SIP TRUNK FAILED TO REGISTER

### 3.4.1 FAULT CODE DESCRIPTION

This alarm will be sent when there is problems when REGISTER is sent to other side of a SIP trunk connection.

### 3.4.2 MEASURES

Use command *alarm -p --format full*. The “Additional text” field will explain the problem in greater detail.

The reason can be:

- The connection does not exist.
- DNS entry does not exist.
- User has no access rights.
- The target computer exists but is changed or reconfigured.
- The target computer does not exist.

Use the linux commands *ping* and *traceroute* to examine the network configuration, and determine if the network path to the host is working.

Examine the return code in the additional text field, in the alarm print out.

See: RFC 3261

## 3.5 FAULT CODE 2:7 - CSTA SERVER, FAULTY COMMUNICATION CHANNEL (CSTA3)

### 3.5.1 DESCRIPTION OF FAULT CODE

CSTA server cannot communicate with an external application.

#### **ADD INFO 1**

2: XML

3: TR87

### 3.5.2 MEASURES

-



## 3.6 FAULT CODE 2:8 - CSTA SERVER, LOAD REGULATION REPORTS OVERLOAD (CSTA3)

### 3.6.1 DESCRIPTION OF FAULT CODE

CSTA server has received a service request, but load regulation reports overload, the request is denied.

### 3.6.2 MEASURES

(Same as for alarm 0:320).

Check for any of the following alarms:

- Fault code 1:1 High CPU load
- Fault code 1:31 Too much memory paging
- Fault code 1:32 Slow event response

If any of these alarms are found, they should be solved first. The fault condition triggering those alarms is most likely also the cause of this alarm.

The alarm indicates that an investigation of traffic load in this system should be performed. A reduction of the number of extensions or external lines, move of certain applications, or a more powerful server processor might prevent this alarm in the future.

The number of calls/second which can be handled by a MX-ONE Service Node depends on the selected processor of the server.

## 3.7 FAULT CODE 2:9 - CSTA SERVER REPORTS NO RESPONSE FROM CLIENT (CSTA3)

### 3.7.1 DESCRIPTION OF FAULT CODE

CSTA server reports too many unsent messages in the output buffer. Real time service is no longer possible. The connection to the external application is closed.

### 3.7.2 MEASURES

The CSTA server is queuing messages in the output buffer, since the CSTA client or network is blocking CSTA server from writing on the TCP/TLS stream.

Or it could be time-out in the heart-beat function.

Check the external application and/or network to see if it is possible to increase throughput. Move the client application to a faster/better machine. Increase the bandwidth in the network. Increase the number of CSTA clients, thus lowering the load on each client.

Or it could be that the client has not responded within stipulated time. Check the client service state, and if there is failure in the network, for example a broken switch or unplugged cable.

## 3.8 FAULT CODE 2:10 - CSTA SERVER REPORTS SLOW RESPONSE FROM CLIENT (CSTA3)

### 3.8.1 DESCRIPTION OF FAULT CODE

CSTA server reports increasing number of unsent messages in the output buffer. Real time service may be jeopardized.

### 3.8.2 MEASURES

The CSTA server is queuing messages in the output queue, since the CSTA client or network is blocking CSTA server from writing on the TCP/TLS stream.

Check the external application and/or network to see if it is possible to increase throughput. Move the client application to a faster/better machine. Increase the bandwidth in the network. Increase the number of CSTA clients, thus lowering the load on each client.

Addinfo = 1, More than 2500 messages are in the CSTA server output queue.

Addinfo = 2, More than 25000 messages are in the CSTA server output queue.

## 3.9 FAULT CODE 2:11 - EMERGENCY CALL EVENT

### 3.9.1 DESCRIPTION OF FAULT CODE

An emergency call is made. The alarm contains information of A-number, called number, location id if applicable, and a sequence number.

The alarm remains active for two hours or until the optional SNMP trap is acknowledged by external Network Management Station.

### 3.9.2 MEASURES

This is an information alarm with call information A-number, B-number, location-id, and sequence number.

### 3.9.3 EXAMPLE OF INFORMATION

Additional text : Emergency call from "320" to number "112", SeqNumber "1". Use this information to assist in the emergency situation.

## 4 DOMAIN 3 - OTHER MX-ONE SERVICE NODE

### 4.1 FAULT CODE 3:1 - LIM IS RUNNING ON STANDBY SERVER

#### 4.1.1 DESCRIPTION OF FAULT CODE

The alarm is received when the regular LIM server cannot be reached.

The fault might occur due to network problems, faulty hardware in the server, or that the server is rebooting.

If the server is rebooting it will be operational within 5 to 10 minutes and the alarm will be cleared. If the fault is of a more serious character manual measures might be needed.

Additional text in the alarm list printout states:

- cluster
- host name of the standby server running the LIM
- host name of the regular LIM.

#### 4.1.2 MEASURES

1. Is the alarm older than 10 minutes?
2. YES: Wait 10 minutes before further action is taken.  
Wait to allow the server perform normal recovery before it is ready.
3. Use the Unix command *ping* towards the regular LIM.  
Try to contact the regular LIM over the network.
4. Is there network contact with the regular LIM?  
Either no network contact with the regular LIM or the *ping* is stopped.
5. YES: Is it possible to log on to the regular LIM with *ssh*?  
Does secure shell login work?
6. YES: Read the files  
*/var/log/messages* and */var/log/localmessages*.  
Check logged records that are related to the fault.  
Consult an expert.
7. NO: Is it possible to log on to the regular LIM at site?  
Try local log on.
8. Is the server rebooting?
9. YES: Wait for the server to complete the reboot and also performing recovery.
10. NO: Is the server indicating any hardware fault?
11. YES: Replace faulty hardware and wait for recovery.
12. NO: Is there any network equipment failure?

13. YES: Replace faulty network equipment.
14. NO: Consult an expert.

## 4.2

## FAULT CODE 3:2 - STANDBY SERVER IS OUT OF ORDER

### 4.2.1

### DESCRIPTION OF FAULT CODE

The alarm is received when the standby server cannot be reach.

The fault might occur due to network problems, faulty hardware in the standby server, or that the server is rebooting.

If the server is rebooting it will be operational within 5 to 10 minutes and the alarm will be cleared. If the fault is of a more serious character manual measures can be needed.

Additional text in the alarm list printout states:

- cluster
- host name of the standby server.

### 4.2.2

### MEASURES

1. Is the alarm older than 10 minutes?
2. NO: Wait 10 minutes before further action is taken.  
Wait to allow the server perform normal recovery before it is ready.
3. YES: Use the Unix command *ping* towards the standby server.  
Try to contact the standby server over the network.
4. Is there any contact with the standby server?  
Either no network contact with the standby server or the use of *ping* is stopped.
5. YES: Is it possible to log on to the server with *ssh*?  
Does secure shell log on work?
6. Is it possible to log on to the server at site?  
Try local log on.
7. YES: Read the files  
*/var/log/messages* and */var/log/localmessages*.  
Check logged records that are related to the fault.  
Consult an expert.
8. NO: Is the server rebooting?
9. YES: Wait for the server to complete the reboot and also performing recovery.
10. NO: Is the server indicating any hardware fault?
11. YES: Replace faulty hardware and wait for recovery.
12. NO: Is there any network equipment failure?
13. YES: Replace faulty network equipment.
14. NO: Consult an expert.

## 4.3 FAULT CODE 3:3 - STANDBY CLUSTER HAS FAILED TO SYNCHRONIZE DATA

### 4.3.1 DESCRIPTION OF FAULT CODE

The alarm is received when a standby server has failed to retrieve exchange data from the regular LIMs in the cluster.

If the standby server is running as a LIM, the server where the LIM normally runs might have failed to retrieve exchange data from the LIMs in the cluster.

Additional text in the alarm list printout states:

- cluster
- host name of the standby server or host name of the regular LIM
- info about the cause.

### 4.3.2 MEASURES

1. Enter the command  
*cluster\_data\_check -cluster name.*  
Check the data status of the cluster. The cluster name is found in the Additional text.
2. Is data status for all listed hosts OK?
3. NO: enter the command  
*data\_backup.*  
See backup of data.
4. Wait at least 30 minutes.  
Wait for exchange data synchronization to finish. Synchronization is started after data backup is finished.
5. Enter the command  
*cluster\_data\_check -cluster name.*  
Check the data status of the cluster. The cluster name is found in the Additional text.
6. Is data status for all listed hosts OK?
7. NO: log on to the failing host reported in the alarm.  
Host name is found in the Additional text.
8. Read the files  
*/var/log/messages and /var/log/localmessages.*  
Check logged records that are related to the fault.
9. Consult an expert.

## 5 DOMAIN 5 - MEDIA GATEWAY

### 5.1 FAULT CODE 5:1 - NO CONTACT WITH MEDIA GATEWAY

#### 5.1.1 DESCRIPTION OF FAULT CODE

The alarm is sent when the Service Node has no contact with the Media Gateway.  
Possible faults:

- Cable errors
- Problem with the Media Gateway itself

#### 5.1.2 MEASURE

1. Is the cable between the Service Node and the Media Gateway properly connected? LED indicators should be lit, if existing/relevant.
2. NO: connect the cable.
3. YES: Restart the Media Gateway.
4. Is there a connection after restart?
5. NO: consult an expert.

### 5.2 FAULT CODE 5:9 - MGU POWER PROBLEM

#### 5.2.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the MGU board has detected a power failure in the backplane of one or more of its power supplies, which are -5V, +5 V, -12V, and +12V for the MX-ONE Classic (7U), and +5 V for MX-ONE Lite (3U) and MX-ONE 1U.

#### 5.2.2 MEASURE

If the MGU board is located in an MX-ONE Lite (3U) sub-rack or MX-ONE 1U, replace the chassis. For more information, see the operational directions for *REPLACING MISCELLANEOUS HARDWARE*.

If the MGU board is located in an MX-ONE Classic subrack, replace the DC/DC board.

For more information, see the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

**Note:** In either case, if there is a processor board in the subrack (Mitel ASU Lite, ASU or Mitel ASU-II), it needs to be powered down properly before any action is performed on the hardware.

## 5.3 FAULT CODE 5:13 - TEMPERATURE PROBLEM IN 3U BACKPLANE

### 5.3.1 DESCRIPTION OF FAULT CODE

This alarm is sent by the MGU in the MX-ONE Lite (3U) subrack when it has detected that the backplane temperature has come above 60 degrees Celsius.

The alarm will cease when the temperature falls below 50 degrees Celsius.

### 5.3.2 MEASURE

Check that the fan unit of the MX-ONE Lite is working properly.  
If not replace the subrack.

For more information, see the operational directions for *REPLACING MISCELLANEOUS HARDWARE*.

## 5.4 FAULT CODE 5:15 - FAN FAILURE IN 3U UNIT

### 5.4.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the MGU board has detected a fan unit failure in the MX-ONE Lite (3U) unit.

### 5.4.2 MEASURE

Check if the LEDs indicating "Fan alarm" are lit (Red V4, V5). This indicates that there is a fault in the fan unit. Replace the fan unit.

For more information, see the operational directions for *REPLACING MISCELLANEOUS HARDWARE*.

## 5.5 FAULT CODE 5:16 - MEDIA GATEWAY SOFTWARE VERSION INCOMPATIBLE WITH MX-ONE SERVICE NODE

### 5.5.1 DESCRIPTION OF FAULT CODE

The Media Gateway software version is incompatible with the software in the MX-ONE Service Node.

### 5.5.2 MEASURE

Please use the correct MGU software (MGW version) for this MX-ONE Service Node release.

Use the command *media\_gateway\_info* to get current information about the Media Gateway version.

## 5.6 FAULT CODE 5:18 - MGU EXTERNAL ALARM A

### 5.6.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the MGU board has detected that the external alarm A has been set to ground (0V).

For the MX-ONE Lite (3U) unit this is the pin 1 in the alarm connector on the rear side.

For the MX-ONE Classic (7U) this is the A1 pin in the connector "Alarm In" in the DC/DC board in the same chassis.

**Note:** This alarm is configurable by the user and could have an other fault code title.

### 5.6.2 MEASURE

Check the operation of the equipment that is connected to the alarm input.

## 5.7 FAULT CODE 5:19 - MGU EXTERNAL ALARM B

### 5.7.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the MGU board has detected that the external alarm B has been set to ground (0V).

For the MX-ONE Lite unit (3U) this is the pin 3 in the alarm connector on the rear side.

For the MX-ONE Classic (7U) this is the B1 pin in the connector "Alarm In" in the DC/DC board in the same chassis.

**Note:** This alarm is configurable by the user and could have an other fault code title.

### 5.7.2 MEASURE

Check the operation of the equipment that is connected to the alarm input.

## 5.8 FAULT CODE 5:20 - MGU LOST CONNECTION TO LAN0 OR LAN1

### 5.8.1 DESCRIPTION OF FAULT CODE

In case of both LAN ports are used (Link Failover), and the link is dropped on the currently active LAN port, the MGU will then change its active port to the other LAN port and send out this alarm. When the link comes back on the now passive LAN port, the fault code will be cleared. Observe that this fault code is not generated if the link is dropped on the passive LAN port.

### 5.8.2 MEASURE

1. Check the cables to the used LAN ports.
2. If the fault is suspected to be in the MGU board, replace the board.



For information, see the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.

3. If the fault is suspected to be in an external switch, replace this unit.

## 5.9 FAULT CODE 5:22 - MGU DEFAULT GATEWAY UNREACHABLE

### 5.9.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the MGU board has lost contact with the default gateway, either on LAN0 or LAN1.

### 5.9.2 MEASURE

1. Check if the cables for the used LAN or LANs are working. Try to see which part of the network that is malfunctioning.
2. If the fault is suspected to be in the MGU board, replace the board.  
For more information, see the operational directions for *REPLACING BOARDS IN MX-ONE MEDIA GATEWAYS*.
3. Check if the fault could be in equipment located between the MGU and the default gateway. Replace such equipment in that case.
4. If the fault is suspected to be in the default gateway, replace this unit.

## 5.10 FAULT CODE 5:24 - VLANS WITH SAME GW MAC ADDRESS

### 5.10.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the two LANs of the MGU, LAN0 and LAN1, have the same MAC address. Due to an MGU internal layer-2 switch such arrangement is not possible.

The MGU does not support the used router.

### 5.10.2 MEASURE

1. Use routers that are supported by the MGU.
2. If the fault is in equipment used between the MGU and the default gateway, replace this equipment.
3. If the fault is in the default gateway, replace the default gateway with a supported unit.

## 5.11 FAULT CODE 5:25 - FILE ERROR FOR VOICE ANNOUNCEMENT DATA

### 5.11.1 DESCRIPTION OF FAULT CODE

This alarm is sent from the MGU board when there are problems to store media files on the board. Possible information with the alarm can be:

- 1) Total media file size exceeds maximum limit (skipping files)  
The maximum limit is 30 MB.
- 2) Number of media files exceeds maximum limit (skipping files)  
There can be maximum 250 files downloaded.
- 3) Removing unsupported file format: <media file name>
- 4) Error downloading to DSP memory, error code: <error code> (download stopped)

### 5.11.2 MEASURE

#### 5.11.2.1 *Exceeded limit*

For fault reason 1) and 2) check which voice records that have been loaded. Use the command

`recorded_announcement_prompt -p`

Remove records to free the memory area. Use the command

`recorded_announcement_prompt -e`

#### 5.11.2.2 *Wrong format*

For reason 3) use a supported file format.

#### 5.11.2.3 *Other error*

The type 4) error should normally never happen. If it does, it can be due to a hardware failure.

Consult an expert.

## 5.12 FAULT CODE 5:29 - FAULTY MEDIA GATEWAY CONFIGURATION

### 5.12.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the Media Gateway type is incorrectly configured. This can happen at upgrade, if a Media Server type is programmed as an MGU, or vice versa.

### 5.12.2 MEASURE

1. Check that if the media gateway is an MGU, i.e. its type is actually programmed as MGU, or if it is a Media Server, its type is programmed as a Media Server.
2. Erase the old Media Gateway, and then program it appropriately, with the correct type.

For information, see the operational directions for *INSTALLING AND CONFIGURING THE MIVOICE MX-ONE*, section *CONFIGURE THE MEDIA GATEWAYS*.

## 5.13 FAULT CODE 5:30 - NO CONTACT WITH MEDIA SERVER (SIP INTERFACE)

### 5.13.1 DESCRIPTION OF FAULT CODE

This alarm is sent when the Service Node has lost contact on the SIP (MSCML) interface to a Media Server.

### 5.13.2 MEASURE

1. Check if the fault code 5:1 is active for the same Media Server.
2. If the fault code 5:1 is active, follow its measures.  
For more information, see the operational directions for *STREAMING ON IDLE. MEDIA SERVER*.
3. If fault code 5:30 has come without fault code 5:1 being active, check the network connection to the Media Server.
4. If the network connection seems OK, check the status of the Media Server.