Part Two

This part focuses on the practical task of my internship -

* OMC NOC
* CME Operation
* Site Visit.

|  |
| --- |
| Chapter 5: OMC NOC |

In OMC NOC mainly Network alarms are checked. If there is a major alarm is found then maintenance are done from the NOC by the server, if it is not possible then expert teams are sent to the BTS or BSS to maintenance the network. Here for 2G and 3G there are some different servers to check alarms. For example some alarm check screen shots are shown of 3G Huawei which is using M2000 server software. [*Fig 4.1 – 4.6*]

**5.1. Introduction to Alarm**

**Alarm Categories**

Alarms can be categorized based on two principles:

* By alarm content: event alarms and fault alarms
* By alarm handling and clearance: history fault alarms and shielded alarms

These four categories of alarms are described as follows:

* Fault alarms, such as a board fault alarm, are generated when faults occur to hardware devices or exceptions occur to key functions. Fault alarms are more severe than event alarms. Fault alarms can be cleared.
* Event alarms, such as a congestion alarm, are occasionally generated during the equipment operation. The event alarms indicate only the equipment status at a certain point of time. The system generates some event alarms periodically. Event alarms do not need manual handling.
* History fault alarms refer to the cleared and acknowledged fault alarms.
* Shielded alarms are generated during a short period of time. The alarms matching the correlation rules set on the M2000 client are shielded alarms, and they are stored in the M2000 shielding library. Shielded alarms can only be fault or event alarms.

**Alarm Severity Levels**

Alarm severity level indicates how severe a generated alarm is. Sorted in the descending order, alarms have four severity levels: critical, major, minor, and warning .

* Critical alarms, such as the power circuit fault alarm or the output clock fault alarm, affect the whole system operation. Critical alarms require immediate handling.
* Major alarms, such as alarms about disconnected fibers or physical line faults, occur only to boards or lines. If not handled timely, these alarms may affect the services.
* Minor alarms, such as the alarm for bit errors in some physical lines, refer to common status alarms that indicate the working status of boards or lines.
* Warning alarms indicate status changes or events which do not affect the system performance or subscriber services, but may interest the operator. Some warning alarms prompt when the equipment returns to normality.

**Alarm Types**

Based on the alarm source, the following types of alarms are available:

* Power alarms: Related to the power supply system.
* Environment alarms: Related to the equipment environment, such as the temperature, humidity, and connection control.
* Signaling alarms: Related to communication signaling.
* Trunk alarms: Related to trunk circuits.
* Hardware alarms: Related to boards such as the clock and CPU.
* Software alarms: Related to the software.
* Running alarms: Related to and generated during the system operation.
* Communication alarms: Related to the communication system.
* QoS alarms: Related to the service quality.
* Processing error alarms: Related to exceptions.

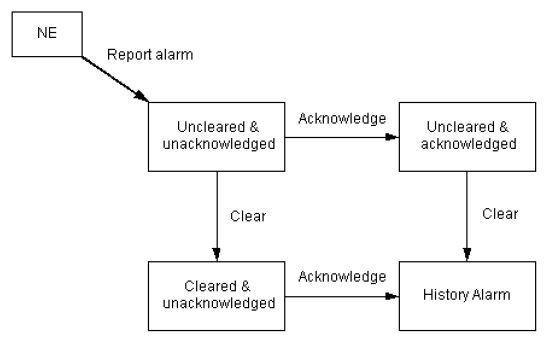
**Alarm Statuses**

Fault alarms can be in the following four statuses:

* Uncleared and unacknowledged
* Uncleared and acknowledged
* Cleared and unacknowledged
* Cleared and acknowledged

For an acknowledged and cleared alarm, the M2000 moves the alarm from the current fault alarm library to the history fault alarm library. Accordingly, the alarm changes to a history fault alarm.

For an unacknowledged or uncleared alarm, the alarm remains in the current fault alarm library as a current fault alarm.

****

*Fig 5.1: How a current fault alarm changes to a history fault alarm.*

**5.2. Alarm Handling Procedure**

After the M2000 detects an alarm, it is recommended to handle a alarm according to the following procedures. [*Fig 5.2*]

1. **Receive an alarm**

Follow the alarm handling procedure after receives an alarm. To ensure that it is notified in time after an alarm occurs. It is needed to set alarm notification methods on the M2000.

1. **View the alarm details**

View the alarm details, including the alarm location, alarm help, and alarm maintenance experience after an alarm occurs.

1. **Acknowledge the alarm**

Acknowledge the alarm to avoid others from handling the same alarm. After acknowledged, it indicates that the alarm has been handled.

1. **Collect the fault information**

Identify the alarm and query the alarm information to find out the symptom of the alarm.

1. **Analyze the cause of alarm**

Analyze the cause of alarm base on the alarm symptom.

1. **Work out the fault handling scheme**

Work out the fault handling schemeaccording toalarm details, device manuals, network status and maintenance experience.

1. **Carry out the fault handling scheme**

Carrey out the fault handling schemeto rectify the fault that leads to the alarm.

1. **Clear the alarm**

Clear the conditions that cause alarm. After the alarm is cleared, the M2000 receives a clearance alarm.

1. **Check whether the fault is rectified**

Check the handling results after rectify the fault.

1. **Record the maintenance experience**

Record the maintenance experience when the alarm handling is complete.

|  |
| --- |
| Receive an alarm |

|  |
| --- |
| View the alarm detail |

|  |
| --- |
| Acknowledge the alarm |

Information Collection

|  |
| --- |
| Collect fault information |

|  |
| --- |
| Analyze the causes of the fault |

Fault Collection

|  |
| --- |
| Workout the fault handling scheme |

Fault

Removal

|  |
| --- |
| Carryout the fault handling scheme |

|  |
| --- |
| Clear the alarm |

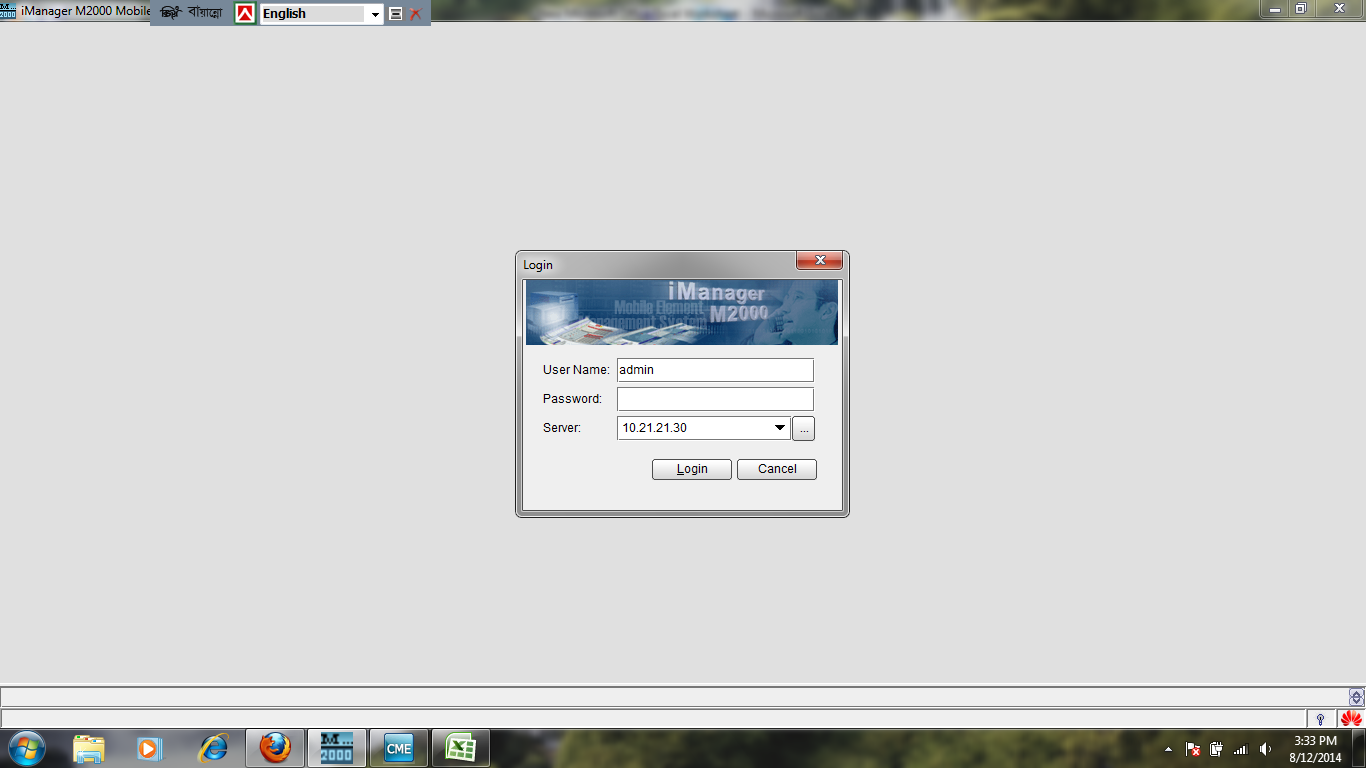
Check whether the fault is removed?

|  |
| --- |
| Record the maintenance experience |

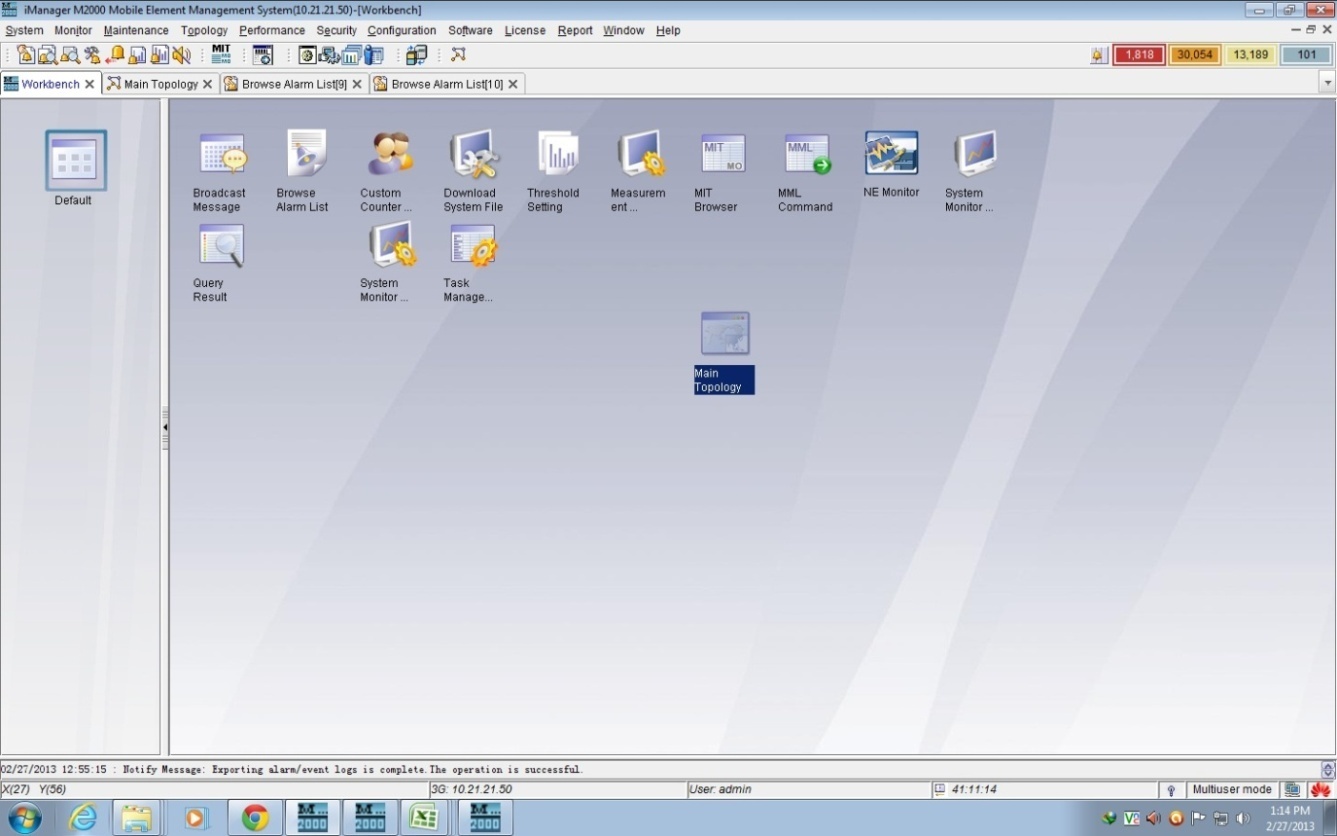
*Fig 5.2: Alarm Handling Procedure.*

**5.3. Alarm Handling with M2000**

iManager M2000 Mobile Element Management System (M2000 for short) is the network management system (NMS) for Huawei mobile communications products. [*Fig 4.3 & 4.4*] It works in the widely used Client/Server mode. The M2000 system contains a set of servers and multiple clients connected to the servers. The M2000 clients run on the Windows platform. The clients provide friendly graphical interfaces for operations and maintenance on the NEs.

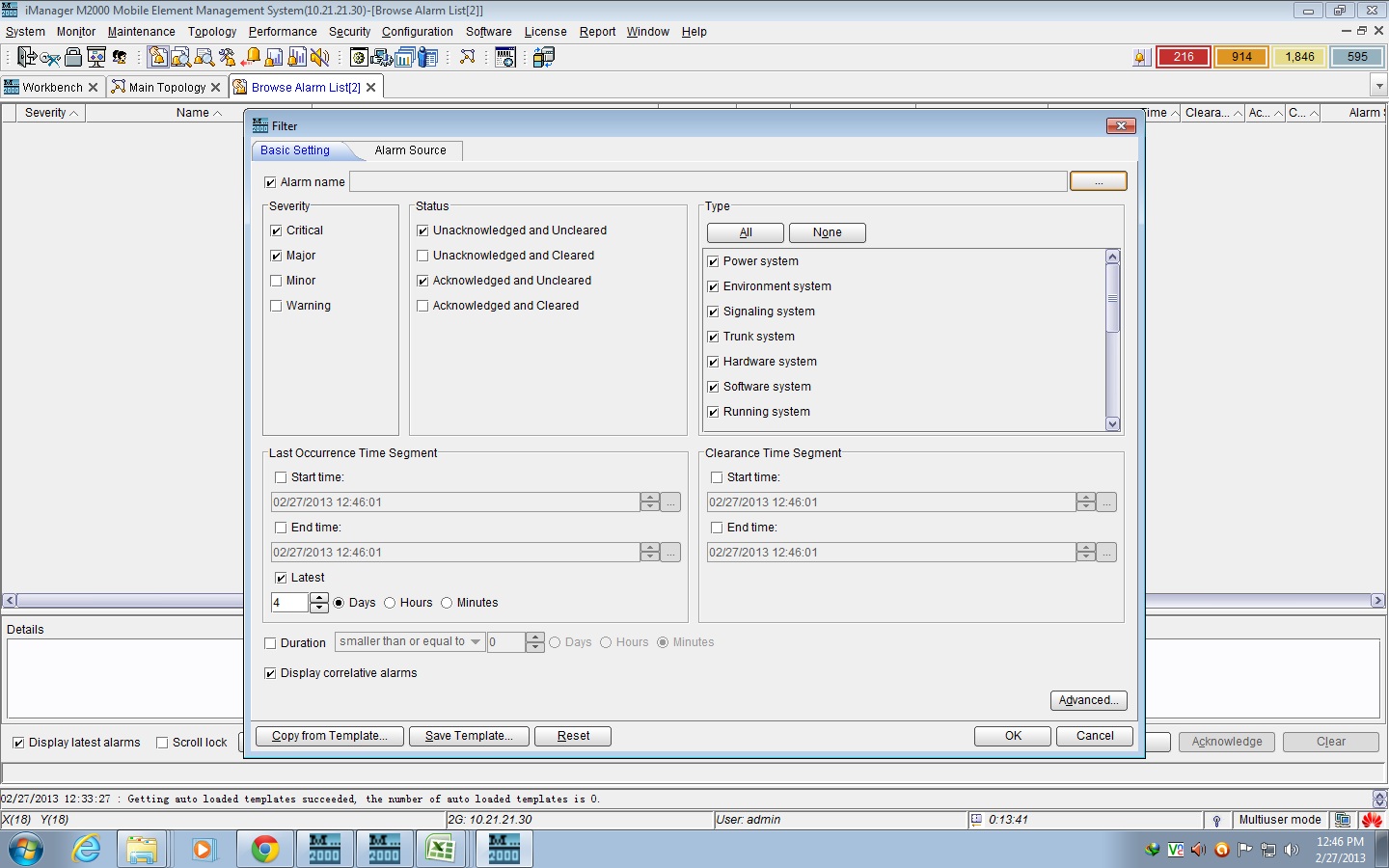


*Fig 5.3: iManager M2000 before Login.*

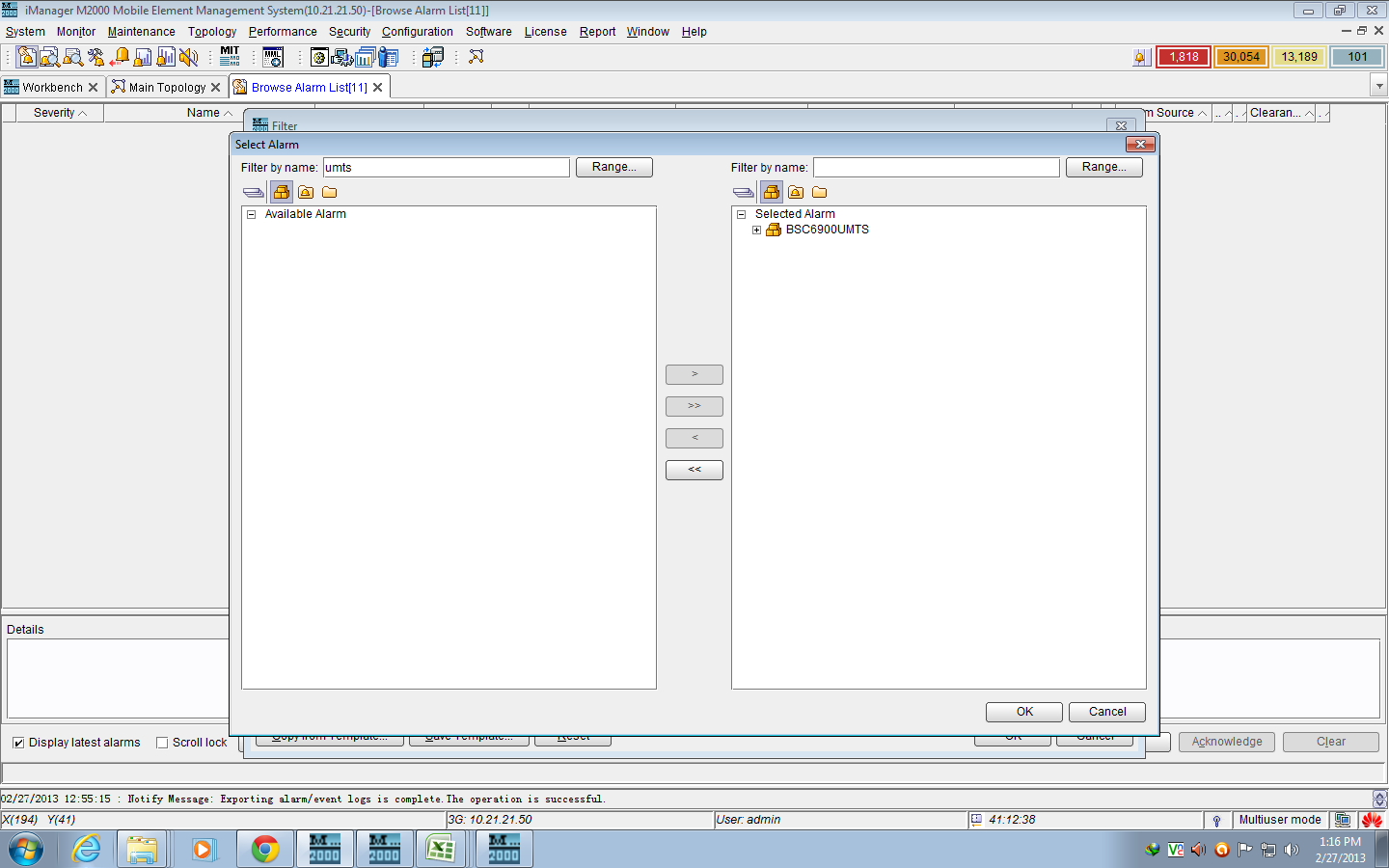


*Fig 5.4: iManager M2000 after Login.*

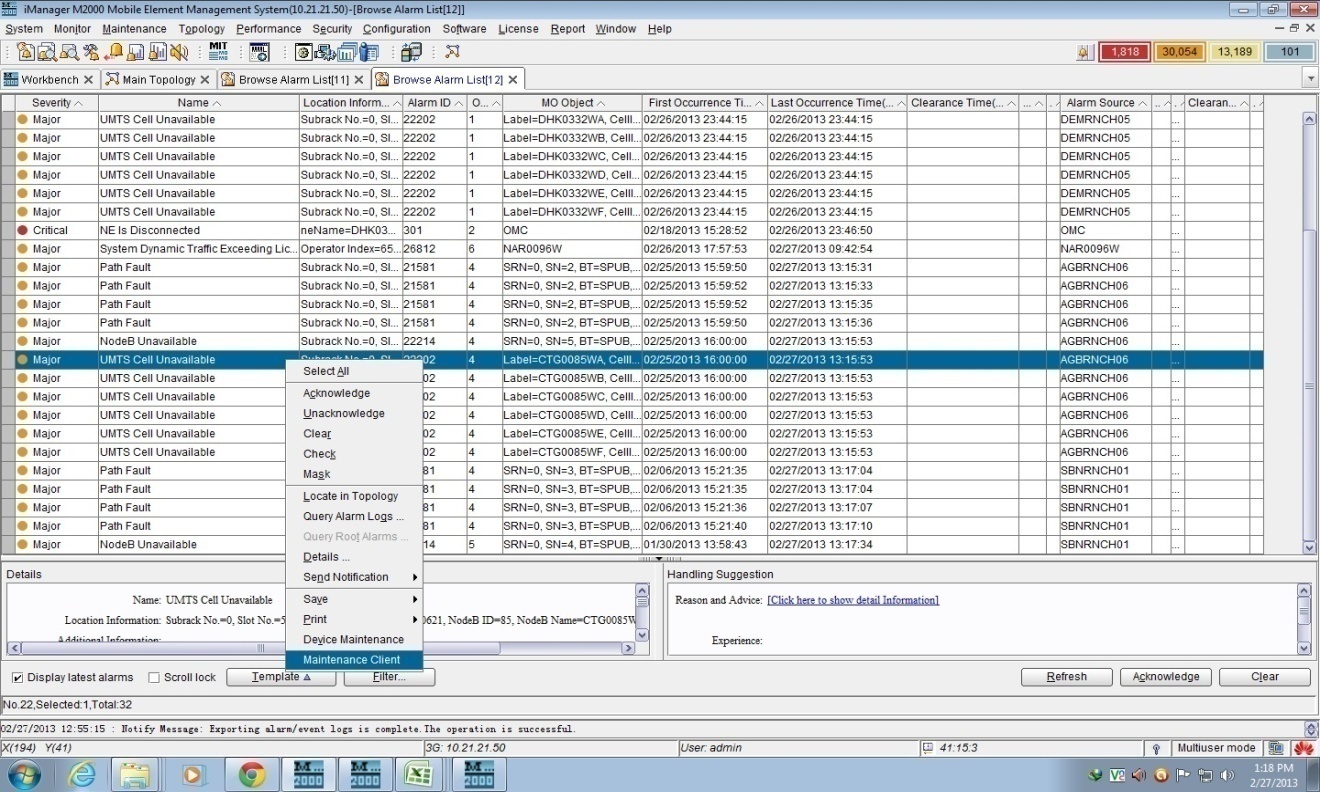
To check an alarm in the software we are to login in here. After login we can find various topologies of the full network structure. To go the main topology we have to enter there first.



*Fig 5.5: Checkbox Condition for Shortlisted Alarm List.*

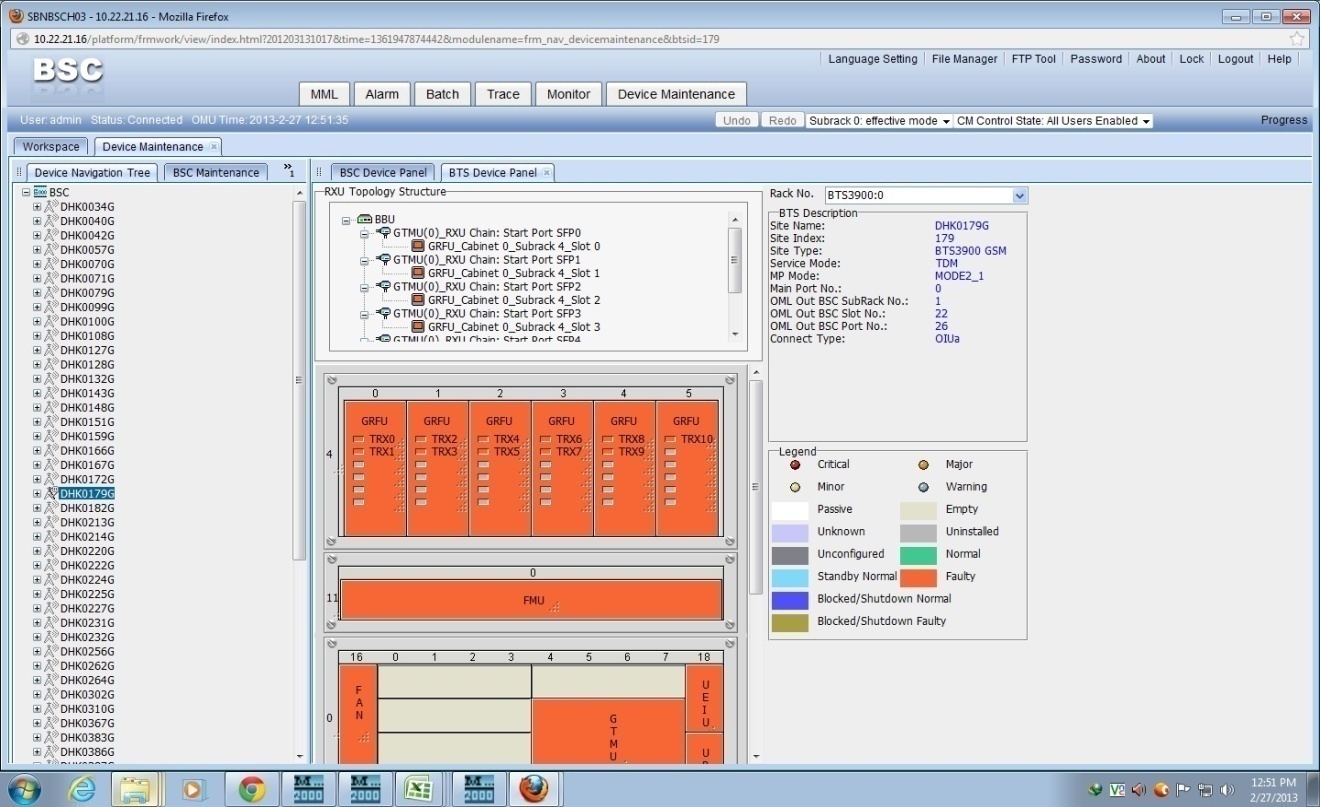


*Fig 5.6: Browsing Alarm list.*



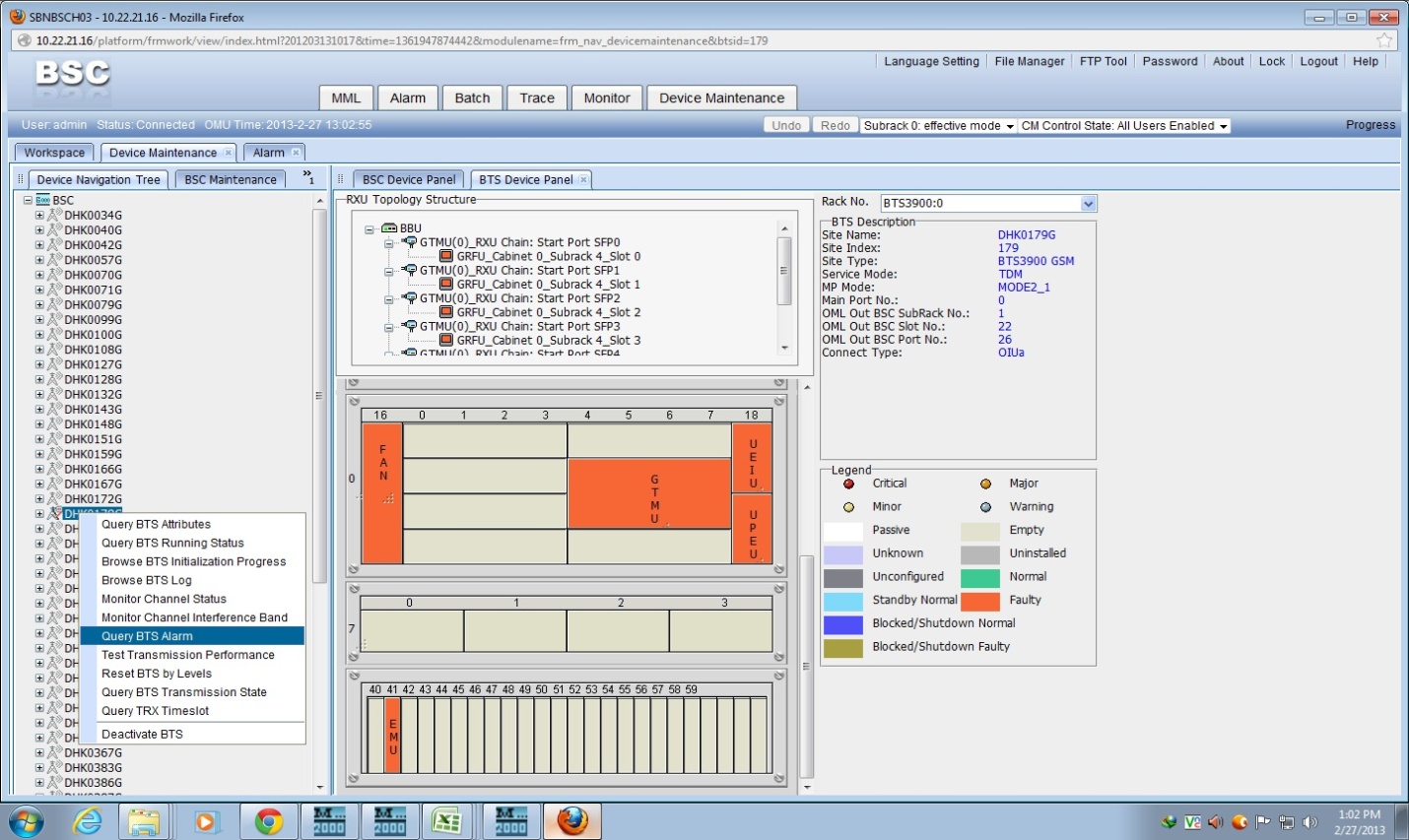
*Fig 5.7: Major alarms & maintenance Clint.*

Here to check distinguish alarms. We have another access called Maintenance Client to go through further alarms of that particular BTS.

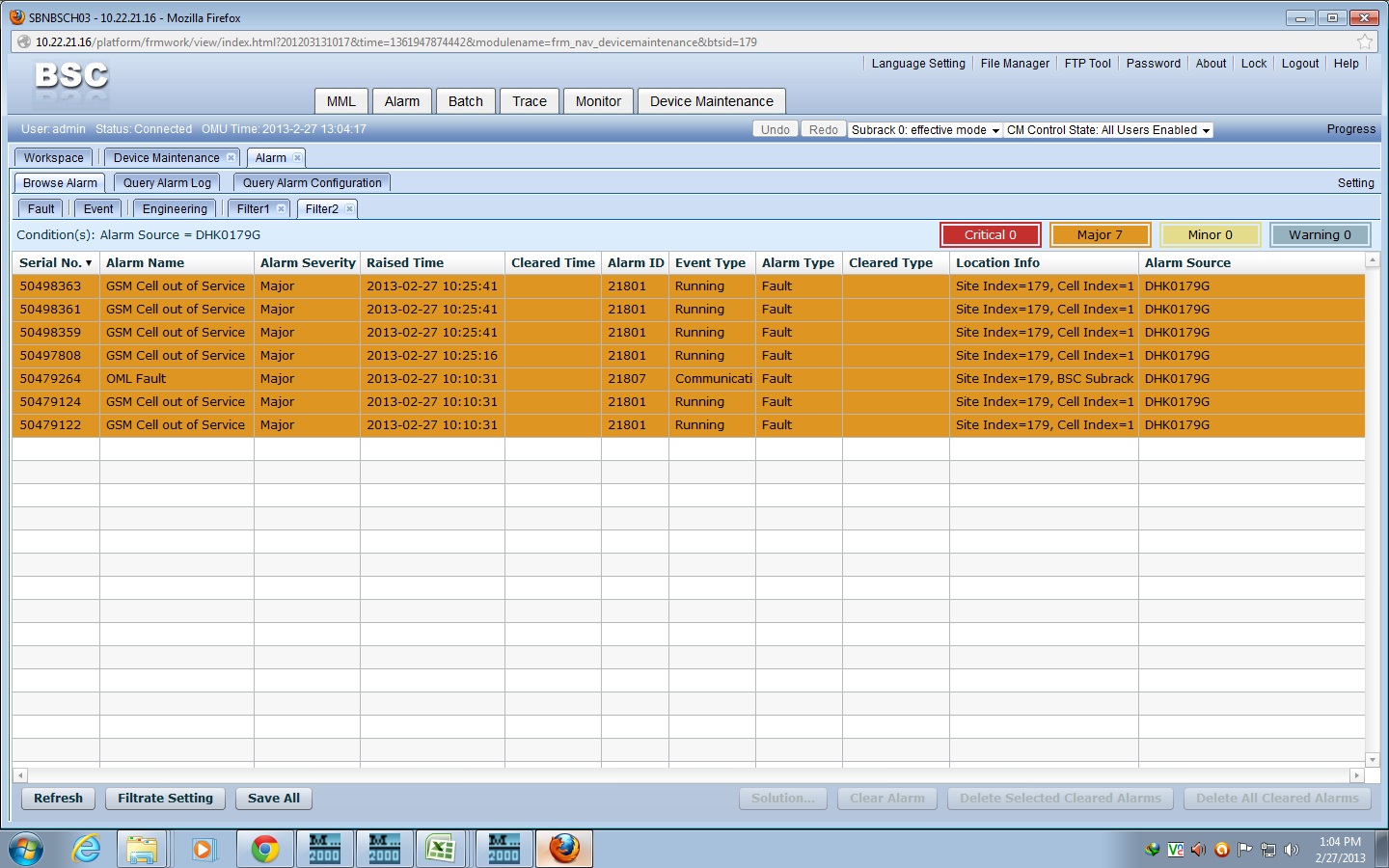


*Fig 5.8: Particular Alarm Checking*

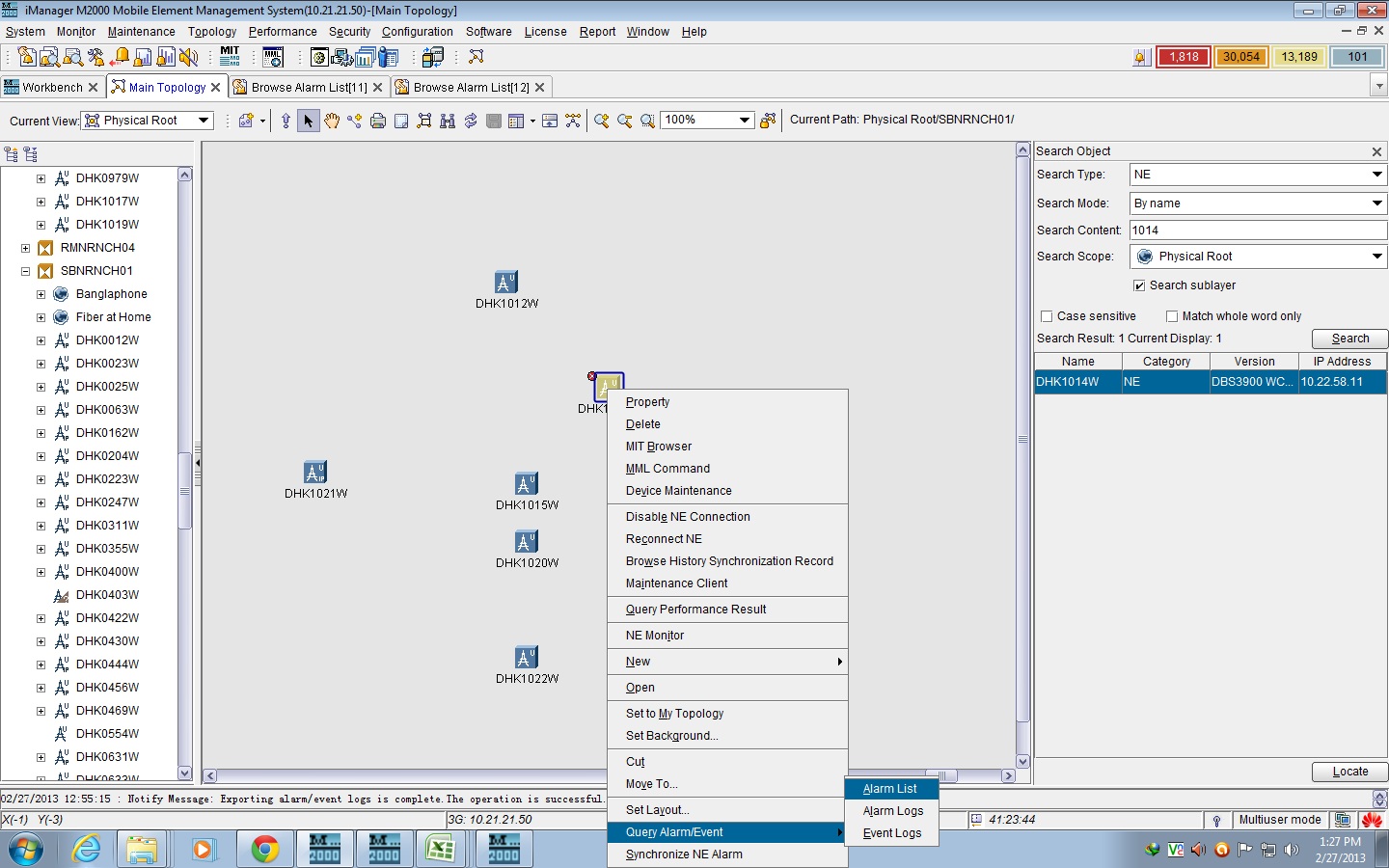
**5.4. Device Panel Fault**



*Fig 5.9: Process to find out the fault.*

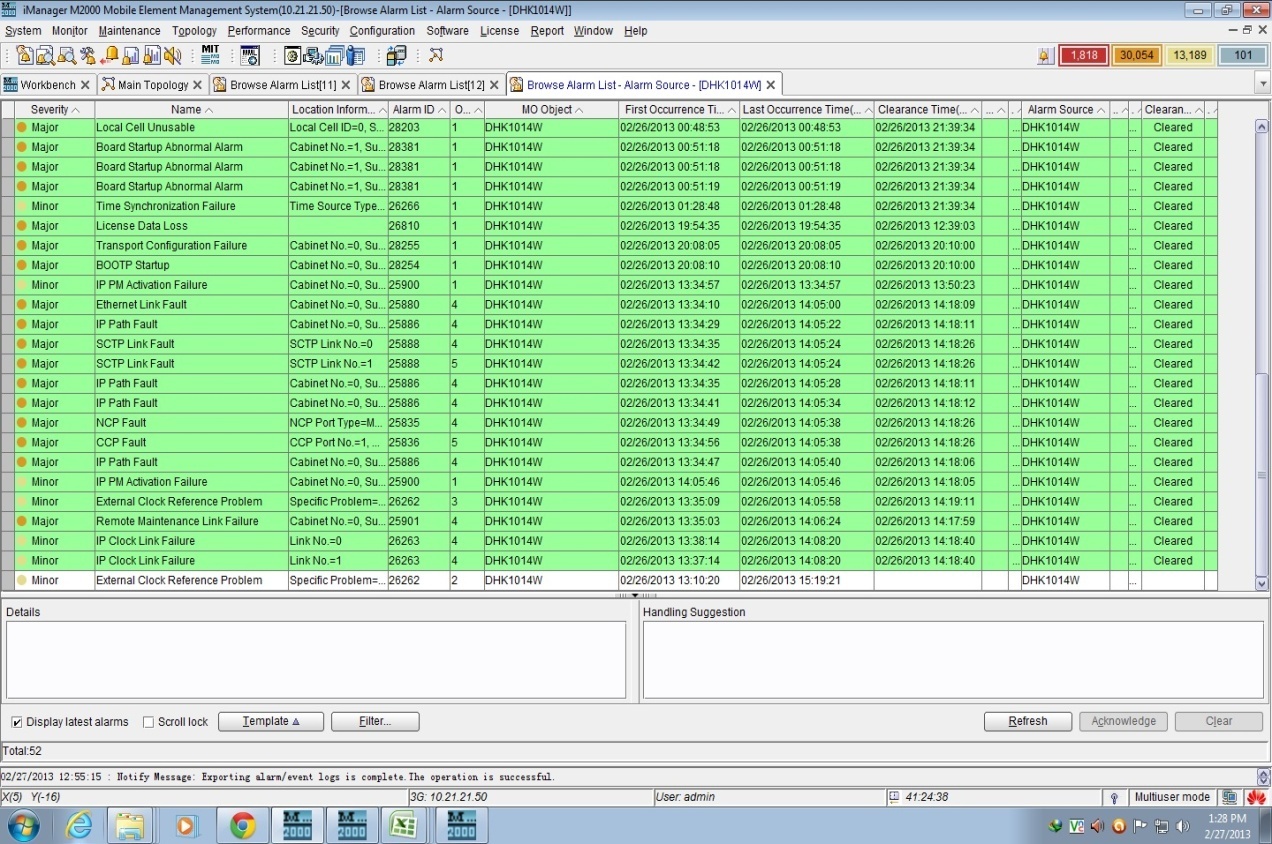


*Fig 5.10: Particular fault of a BTS Diagram.*



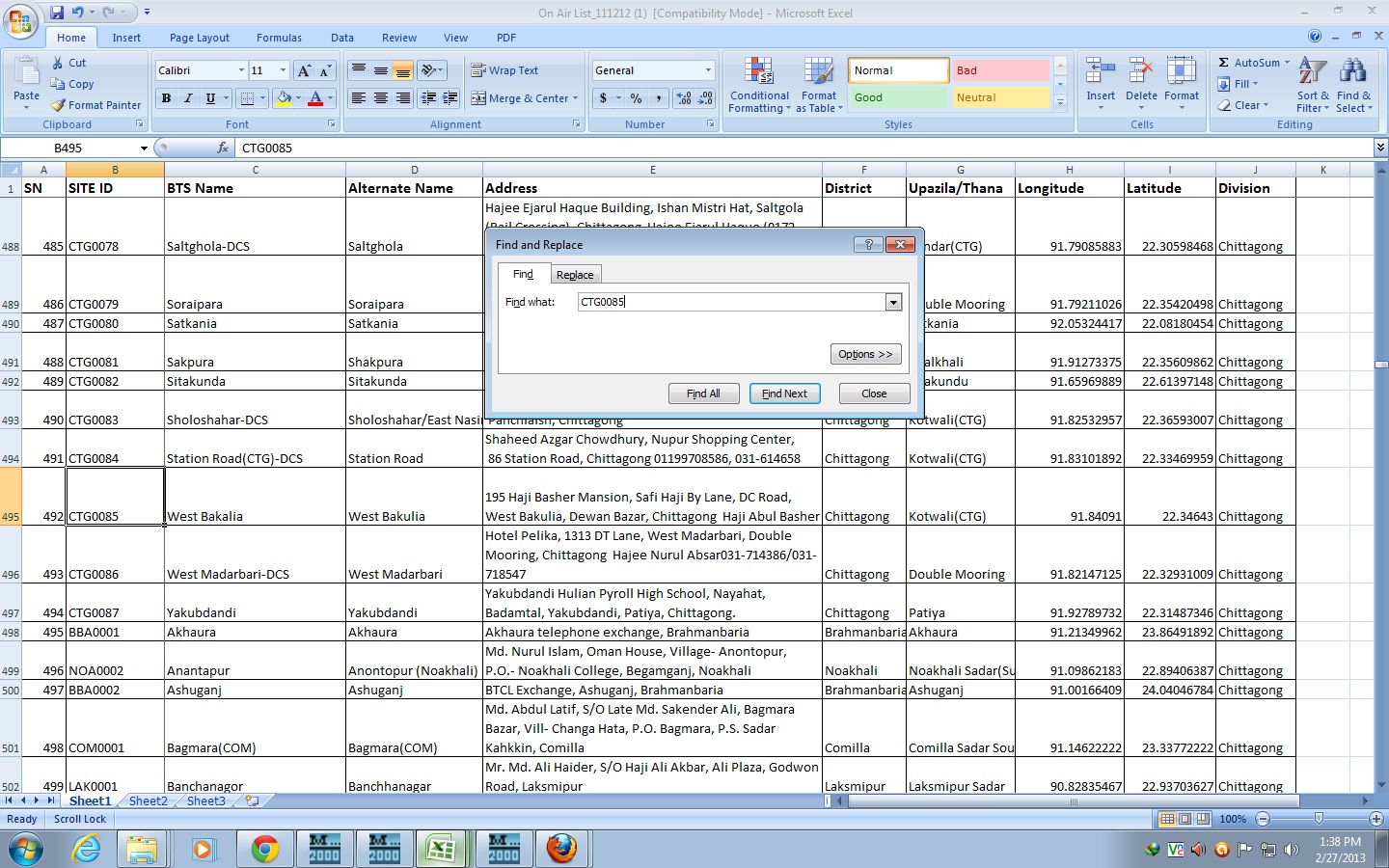
*Fig 5.11: BTS down & no transmission and query alarm list.*

Here we can see a specific alarm integrated to a particular BTS by going to the query Alarm Event system finding alarms, faults, performance etc.



*Fig 5.12: Alarm list, Types & site code collection.*

All the faults occurred in that particular BTS are found in here. We see the faults can occur. Then after seeing this maintenance are taken according to them.



*Fig 5.13: Find out the BTS location from the data sheet and contact with expert team for maintenance.*

Teletalk contains an excel sheet containing data’s of all the BTS under that particular BSS. It contains information of site code, location, area, division, phone number, address etc.