GSM network monitoring using TEMS
Radio resources functions in GSM

1.1. TEMS features

TEMS (**TE**st **M**obile **S**ystem) is a software programme developed by Erisoft Company (ERICSSON) for testing and monitoring the radio interface in a cellular network (e.g. GSM 900). The main features of TEMS are:

- Visualisation of the general information about the monitored system (radio interface parameters, signalling messages);
- Possibility of establishing a test hypothesis;
- Possibility of selecting the cells;
- Saving messages and sequences in .log type files and the subsequent running of these files;
- Remote control of the MS;
- control of the messages specific to the third level of the protocol stack;
- control of authorization;
- possibility of printing separately the windows
- reading/monitoring/ saving geographical coordinates from an external positioning equipment;
- reading and changing the SIM card information
- sending short messages (SMS) to another MS.

1.2. Monitored information Control

Logging = the process by which the messages received from the associated MS are saved in a .log type file, using TEMS. In the absence of any external influence, TEMS may display a large amount of information and messages during the initiation of a communication with the MS connected to the computer.

The dialog box **Externals-Control MS logging** makes possible the control of the information that will be displayed.

- **Idle mode reports:** different parameters can be recorded: the channel number (ARFCN), the BS identity code (BSIC) and the received signal level (RxLev) for the served cell and for other 6 adjacent cells which generate the strongest signals at BS level, while the MS is on hold.
- **Dedicated mode report:** report of the received signal level (RxLev), signal quality (RxQual), transmitted power level (Tx power), timing advance (TA), channel number (ARFCN) and BS identity code (BSIC) for the served cell, signal power (RxLev) and BSIC for the strongest 6 signals generated by adjacent cells and radio link time counters. In GSM, the BS receives messages from the MSs placed in that cell which it supervises at very close time intervals. These messages must not overlap therefore each segment is provided with a very small guard interval. So in GSM there is a compensation mechanism for the variable propagation time which consists in shifting the MS transmission time depending on its position with respect to the BS. The value of this shift (called **time advance**) is deduced by the network and transmitted to the MS. After establishing a connection, BTS continuously measures, evaluates the time advance and transmits it to the MS through a SACCH channel two times per second.
- **No service mode report** – when the MS is not activated.

1.3. The quality and the power of the received signal in GSM

In GSM system, the quality of the received signal is computed as the ratio between the number of erroneously received bits and the total number of bits, previously known at the MS.

The parameter specific to GSM which characterizes the received signal quality is RxQual. Between RxQual and the bit error rate there is a correspondence given in Table 1.

BER (%)	0-0.2	0.2-0.4	0.4-0.8	0.8-1.6	1.6-3.2	3.2-6.4	6.4-12.8	12.8-
RxQual	0	1	2	3	4	5	6	7

Table 1 – Correspondence between BER and RxQual

In GSM, the received signal power is measured in RxLev levels. The correspondence between RxLev and dBm is given in Table 2:

dBm	-110	-109	...	-48	-47
RxLev	0	1	...	62	63

Table 2- Correspondence between RxLev and dBm

1.4. Cell selection

If the MS is on hold, there is possible to strainedly position it on a certain cell or on a group of cells characterised by BCCH ARCFN. This action will inhibit any process of cell re-selection, which would normally have developed, and any handover (if one desires this). Subsequently, the selected cell will be used regardless of the power and the quality of the signals transmitted by the adjacent channels. The MS will remain positioned on the imposed channel until one presses the button **Clear** or until it is restarted. In the on **Hold** mode, there can be selected one or more target frequencies from a list of maximum 42 frequencies. In **dedicated** mode there can choose a target frequency on which the MS will strainedly transfer the link; one can also select certain radio frequencies that the MS can avoid when the handover is performed. In this case, the MS will not report the power of the signal on these carriers.

1.5. .log Files

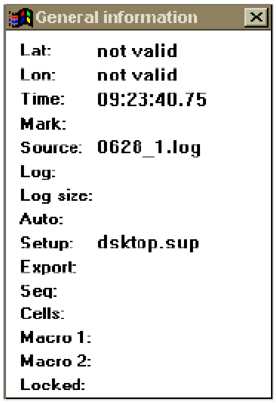
Using .log files, there can be recorded messages or different sequences that run while the MS is monitored by TEMS. These files are very useful for the GSM networks operators, as they are parts of the written documentations and of the tests concerning the functionality of a GSM network. There can be run recorded sequences in the case of a subsequent monitoring. It is impossible to run a .log file when the MS is activated and monitored by TEMS programme.

2. Visualisation of the information regarding the monitored GSM network

2.1. Abstract

One of the most important features of the TEMS is the possibility of monitoring messages and other information in the logging process or after subsequent visualisation of the .log file that one obtained. This is possible by activating different windows from the **Monitor** menu (the represented information is updated regardless of the activation of the windows).

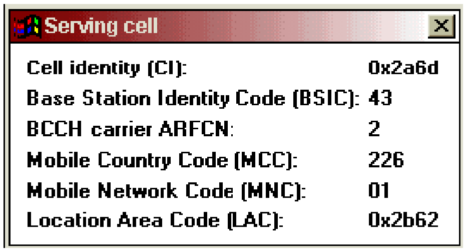
In the window for general information (**General information**) (fig. 1) there can be found several fields, the most important being explained in table 3.



```
Lat:      not valid
Lon:      not valid
Time:     09:23:40.75
Mark:
Source:   0628_1.log
Log:
Log size:
Auto:
Setup:    dsktop.sup
Export:
Seq:
Cells:
Macro 1:
Macro 2:
Locked:
```

Fig 1 – General Information Window

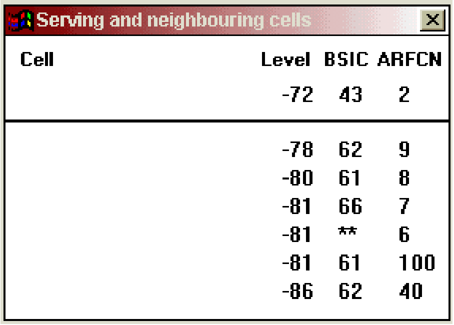
Serving cell window (current cell) contains information regarding the cell on which the MS is synchronised: cell identity (CI), BS identifier (BSIC), BCCH ARFCN, mobile country code (MCC), mobile network code (MNC) and the location area code (fig.2)



```
Cell identity (CI):                 0x2a6d
Base Station Identity Code (BSIC):  43
BCCH carrier ARFCN:                 2
Mobile Country Code (MCC):          226
Mobile Network Code (MNC):          01
Location Area Code (LAC):           0x2b62
```

Fig 2 – Information regarding the served cell

Serving and neighbouring cells window (current cell and adjacent cells) provides information about served cell and 6 other adjacent cells that provide the strongest signals at the MS. The displayed information refers to the cells names (defined by the user), BSIC, BCCH ARFCN and the power level (RxLev or dBm) of each cell. One cell is identified by BSIC-ARFCN and cell name. The message ** in the BSIC field means that the information transmitted from that BS could not have been decoded by the MS (fig.3)

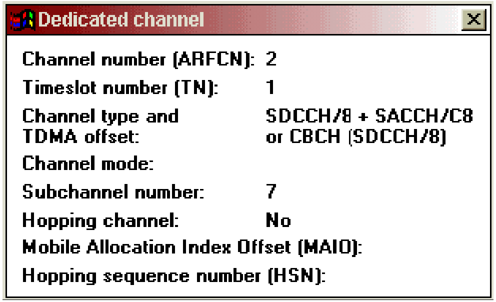


```
Cell                  Level  BSIC  ARFCN
                       -72    43    2

                       -78    62    9
                       -80    61    8
                       -81    66    7
                       -81    **    6
                       -81    61    100
                       -86    62    40
```

Fig 3 – Information concerning the served cell and the adjacent cells

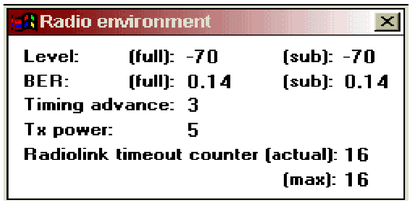
Information regarding the communication channel (**Dedicated channel**) comprises: channel number (ARFCN), used timeslot number (TN), channel type and TDMA offset, etc (fig 4).


Dedicated channel

Channel number (ARFCN): 2
Timeslot number (TN): 1
Channel type and TDMA offset: SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8)
Channel mode:
Subchannel number: 7
Hopping channel: No
Mobile Allocation Index Offset (MAIO):
Hopping sequence number (HSN):

Fig 4 – Information about the dedicated channel

Radio environment window contains information about the radio link parameters: power (RxLev) and received signal quality (RxQual) (the measure units may be defined in the **Preferences** menu), timing advance and transmitted power level (fig.5).


Radio environment

Level: (full): -70 (sub): -70
BER: (full): 0.14 (sub): 0.14
Timing advance: 3
Tx power: 5
Radiolink timeout counter (actual): 16
(max): 16

Fig. 5 –Transmission environment

2.2. Contents of work

1. Run log_1_1.log using **Replay logfile** from **Log** menu. Visualize and write the general information about GSM network: Cell Identity, BSIC, BCCH carrier ARFCN, MCC, MNC, LAC (use **Serving Cell**, **Serving and neighbouring cells** from the **Monitor** menu**).** Use Table 4.

Cell Identity	*BSIC*	*BCCH ARFCN*	*MCC*	*MNC*	*LAC*

Table 4 – General Information about GSM network

2. Run log_1_1.log and change the cell names according to Table 5 (the modifications will be saved in the file a.cel). For this purpose use the **File / Define Cell Names...** menu.

New name	*BSIC*	*ARFCN*
Cel_start	44	93
Cel_1	46	103
Cel_2	40	61
Cel_3	0	5
Cel_4	01	8
Cel_5	**	4
Cel_6	0	2

Table 5 – Change of cells names

3. For the same file visualize and comment the information specific to the reporting modes (*idle* and dedicated) with the aid of the function **Mode reports** from the **Monitor** menu. Explain what the terms “idle” and “dedicated” refer to.

2.3. Questions

1. What is the value of LAI code of the location area in which the file recording was done?
2. During file running, there can be noticed (or could be noticed) the modification of the MNC parameter. Explain the possible occurrence of this phenomenon.
3. In reporting mode there appears the TA parameter (**Time advance**). Define and explain the functioning of this parameter in GSM.

3. Operation on MS

3.1. Abstract

The MS may be remotely accessed through TEMS, by displaying a window that represents the MS keyboard (on which the user can act) and its display. This option is also available in the case when two MSs are monitored in the same time. If the source of information is an associated MS, TEMS allows the reading and even the modification of the information contained in the SIM card of the MS. In different simulations it is possible to increase the transmission power of the MS with respect to the current one.

3.2. Contents of work

Visualize the information contained in the SIM card. Run **sim_card.exe**. The information is grouped in many fields, some of them may be modified (activate **Write** command).

In the field **Access Control** visualize information which refers to the MS access class. There are 15 classes, 10 of them are allocated for standard subscriptions and 5 are allocated to other services:

- 15th class – network operator;
- 14th class – emergency services;
- 13th class – public utilities (fire brigade, ambulance, police etc.);
- 12th class – security services;
- 11th class – used at the will of the operator.

The 10th class of subscription enables the authorisation or the interdiction of emergency calls (112). Using the **SIM service table** field, view information that refers to the services that were allocated and really active in the MS. This field identifies the services offered by the MS's SIM card. These services depend on the SIM card version (one must not confuse with the services that the operator offers to the subscriber) (Table 6).

Service 1	Possibility of activating/disabling the PIN code
Service 2	Possibility of using the short numbering
Service 3	Reserved for 2nd stage use
Service 4	Possibility of storing short messages
Service 5	Possibility of storing information about charging
Service 6	Possibility of storing information related to the configuration of a modem used for a data communication
Service 7	Possibility of selecting a network from a list of agreed networks

Table 6 – Services offered by SIM card

Two bits are allocated to each service: the first bit indicates whether the service is allocated (1) or not (0). The structure of the two bytes is presented in figure 6.

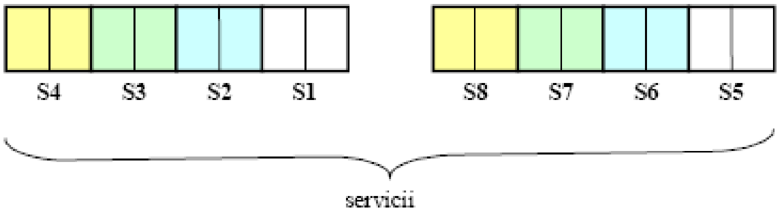


Fig 6 – **SIM service table** field structure

BCCH information field allows MSs to store the last adjacent cells' list that was transmitted to the network in order to accelerate the process of cell selection when the MS is activated, a fact that biases the scanning of the channels that were memorized in the list. The **BA-NO** parameter refers to the frequency band in which the adjacent cells' BCCH channels are found (for GSM, BA-NO has the value 0).

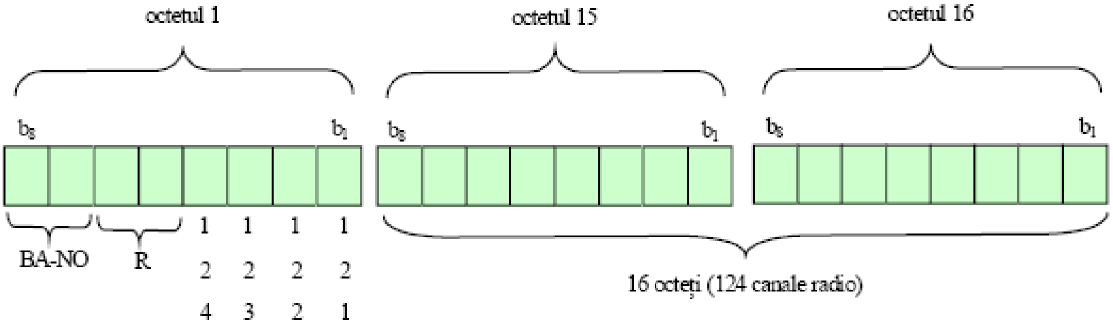


Fig 7 – **BCCH information** field structure

LAI identifies the location area of the PLMN and consists in: the Mobile Country Code MCC (3 digits), Mobile Network Code MNC (2 digits) and the location area code.

T3212 represents a time interval used to control the periodical update of MS location (the value is given in 1/10 hours; a value of 0 for T3212 shows that the MS does not use the periodical update)
Updating status allows the visualisation of location update state and may have the following values:

- 0 –updated location
- 1 – outdated location
- 2 – attempt to update the location in a forbidden PLMN network
- 3 – attempt to update the location in a forbidden location area

Ciphering key represents the encryption key of the 64 bit communication which results after the performance of the A8 algorithm at MS level.

3.3. Questions

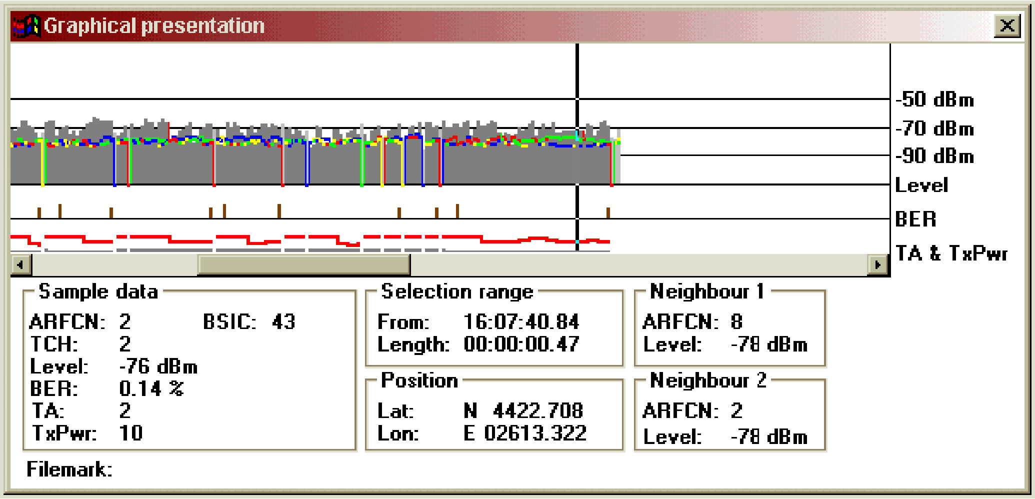
1. Using simcard.exe, determine if for the monitored SIM it is possible to activate the PIN code and to store the short messages in SIM. Which of these services are allocated and / or active?
2. Can there be visualized information related to fees using this SIM?
3. With this SIM, can there be selected a certain network from a list of agreed networks?
4. Determine if the location of the MS was updated.

5. Determine if the monitored mobile network uses a periodical updating.
6. Explain which are the implications of setting the parameter T3212 at the minimum possible value, and respectively at the maximum possible value.

4. The parameters of the GSM radio interface

A very useful tool for graphically displaying the information is **Graphical presentation** (the graphical representation window; figure 1), in which one can visualize the following parameters (in real time or by running a recorded file):

- power of the received signal (RxLev) (from the current BS and from two neighbouring cells that supply the strongest signals at the MS);
- quality of the received signal (RxQual);
- time advance (TA);
- transmitted power (TxPwr);
- number of the channel (ARFCN) (for the current cell and for the two neighbouring cells);
- position (Lat and Lon) if an equipment for determining the position during the recording is used.



Sample data
ARFCN: 2 BSIC: 43
TCH: 2
Level: -76 dBm
BER: 0.14 %
TA: 2
TxPwr: 10

Selection range
From: 16:07:40.84
Length: 00:00:00.47

Position
Lat: N 4422.708
Lon: E 02613.322

Neighbour 1
ARFCN: 8
Level: -78 dBm

Neighbour 2
ARFCN: 2
Level: -78 dBm

Filemark:

Fig 8 – Presentation of the monitoring in the graphical mode

The power level and the quality of the received signal are represented by vertical lines and the level of the strongest signals received from two neighbouring cells is represented by coloured horizontal lines. The time advance (TA) is graphically represented by a vertical line and the emission power by a horizontal line. **The colours of the vertical bars** from the graphical representations of the level of the received signal reflect the state of the MS at that moment: light-grey = the MS is *idle*; dark-grey colour = the establishing of a link (the MS is in the *dedicated* mode). There can be used several different colours for the graphical representation of the signal received from the two neighbouring cells. If the strongest signal from a neighbouring cell decreases under the value of another signal received from another neighbouring cell and afterwards reverts to the previous value, the same colour will be kept in the graphical representation. A handover of the communication link on another frequency is illustrated by a vertical line which corresponds to a change of the ARFCN for the current cell.

4.2. Contents of work

Run **log_21.log** with **Replay logfile** from **Log** menu. Visualize and write in Table 7 the general information regarding the monitored GSM network and the served cell (use **Serving Cell** from the menu **Monitor**).

Cell Identity	*BSIC*	*BCCH ARFCN*	*MCC*	*MNC*	*LAC*

Table 7 – General information about the GSM network

BCCH ARFCN represents the radio carrier on which the logical BCCH channel is transmitted. It is transmitted on the first time slot (0) from this carrier, together with the FCCH channels (the frequency correction) and SCH (synchronization) and it is used for broadcasting the general information about the cell: the minimum level of the signal for access, the maximum possible power level in the cell, the location area identifier, the list with the neighbouring cells, the organization of the logical channels in the cell.

For the same file, using **Graphical presentation** window from the menu **Monitor - Status information**, Table 8 will be filled in (the units of the monitored parameters can be modified by means of the function **Preferences** from the menu **File**).

T (hh:mm:ss)	19:24:44.03	19:24:48.35	19:25:06.09	19:25:19.05	19:25:35.39
Current cell received signal level					
[RxLev]					
[RxQual]					
TA					
TxPwr					
Adjacent cell 1 received signal level					
[RxLev]					

Table 8 – The level of the signal and the quality of the link

4.3. Questions

1. Notice that TA changes its value while running the file log_2.log. Explain the physical significance of the increase (decrease) of the value of the parameter TA.
2. Using TEMS there can be adjusted the level of the signal transmitted by the MS only ascendant. Why?

5. Handover in GSM

5.1. Abstract

Handover is a procedure specific to the cellular networks, by which the communication link is taken over by another BS that ensures better conditions for the link as compared to the current BS. In GSM, the handover procedure is based on a very tight cooperation between the MS, BS and the commutation center. The handover can be classified in:

- *hard handover:* performed with the purpose of avoiding the loss of a current link, when the MS leaves the current cell.

- *soft handover:* performed with the purpose of optimizing the global level of interference in the network; it can be enhanced if the MS establishes the current link by means of another BS.
- *traffic handover:* performed if the MS is located in a cell in which the traffic is very heavy, while in the neighbouring cells not too many communication links take place.

In GSM, besides the classical handover, the intercellular (hard) and the *intracellular* handover can also be used (the MS locates on another channel inside the current cell).

The decision of performing a handover is done based on the evaluation of the parameters:

- RxLev – the power of the received signal, measured either by the MS, or by the BS;
- RxQual – the quality of the received signal evaluated either at the MS, or at the BS;
- TA – parameter that enables the estimation of the distance between the MS and the BS.

These parameters, together with the power levels received from other 16 BSs, are sent at each 480 ms towards the current BS, where they are compared with the threshold values for handover, starting the handover algorithm when one or more threshold values are reached. The master station will receive a message from the BS, containing a list of the neighbouring cells in decreasing order of the power level of the received signal, together with the cause that led to the need of performing a handover: the signal quality, the received power or the increase of the distance between the mobile and the BS. The master station will interrogate the first cell from the list and, in case the availability of a traffic channel is confirmed, the new cell will receive an allocation message from the master station, by means of the signalling network. In the same time, by means of the current BS, one shall transmit towards the MS the handover command that contains information concerning the cell that will serve it hereafter.

The values of the handover thresholds determine the quality and the capacity of the system and are fixed by the network operator. If the threshold values are too high, lots of handover requests will take place, which actually are not necessary; if the threshold values are too low, it is possible to increase the number of communications interrupted for the GSM network.

5.2. Contents of work

Run **log_2.log** with **Replay logfile**. For t=09:23:49.85 one handover is performed from the current cell (ARFCN=6, BSIC=41) to another cell (ARFCN=10, BSIC=41).

Fill table 9 using **Graphical presentation**.

T	**Current cell**			**Adjacent cell 1**		**Adjacent cell 2**	
(hh:mm:ss)	ARFCN	RxLev	RxQual	ARFCN	RxLev	ARFCN	RxLev
09:23:48.90							
09.23:50.34							

Table 9 – The radio environment before and after the handover

Run **log_23.log** and fill in Table 10, using **Graphical presentation**. The time moments indicated in the table are immediately before some handover procedures and immediately posterior to the handover.

T *(hh:mm:ss)*	**Before handover**		**After handover**	
	ARFCN	RxQual	ARFCN	RxQual
19:43:01.20				
19:43:57.58				
19:44:33.68				
19:44:38.31				
19:46:10.52				
19:46:36.05				
19:46:42.49				

Table 10 – The radio environment before and after the handover

For the same file, which runs this time with the help of the cursors (,→) fill in Table 11, corresponding to the values of TA between the moments t=19:44:38.31 and t=19:46:10.52, by using the window **Graphical presentation** from the menu **Monitor**.

T(hh:mm:ss)					
TA					

Table 11 – Values of TA during the running of the file

Based on these values of TA, draw the path of MS, relatively to BS.

5.4. Questions

1. What may cause handover at t=09:23:49.85 in case of log_2.log?

2. After performing the handover at t=09:23:49.85 (log_2.log), it can be remarked that the identity of the cell in unchanged. Explain the occurence of this phenomenon.

3. At t=09:24:26.44 (log_2.log) the modification of the value of the parameter ARFCN takes place, from 10 to 6, without signalling this phenomenon as a handover by TEMS. Why?

4. What is the reason for performing the handover at t=19:46:10.52 (file log_23.log)?

5. What is the reason for performing the handover at t=19:44:33.68 (file log_23.log)?

6. After performing the handover at t=19:44:38.31 (log_23.log), it can be remarked that the quality level deteriorated significantly. For what reason, however was that transfer performed, because the power level of the signal was not very low?

7. In what category (hard handover, soft handover, traffic handover) can there be classified the handovers from t=19:43:01.20 t=19:44:33.68 (log_23.log)?

6. Updating the location in GSM

6.1. Abstract

In order to efficiently direct a call towards a MS, GSM needs minimal information regarding its position (in which location area is it found?). By updating the location one understands informing the GSM network about the position of the MS in the geographical GSM network. The results of the location updating pprocedures are stored in VLR, HLR and SIM.

There are three versions of location updating:

- normal location updating;
- periodical location updating;
- *IMSI attach / detach* procedures.

In *normal location updating*, the MS in *idle* mode reports to the network the change of the location area due to the displacement. In the situation of a call to MS, the network verifies if the MS is situated inside a cell that is included in the last reported location area.

There are several situations in which the MS can enter the idle mode without signalling this to the network, which will emit purposeless paging messages to MS in the situation of a call. In order to avoid the overload of the network with incorrect signalling messages, the ***periodical location updating*** of MS is used, a procedure by which the MS sends at specific time intervals T3212 (chosen by the network between 6 min. and 24 h) its own location data. A situation can also appear in which the databases of the network (HLR, VLR) can deteriorate; these databases contain information that changes in time, about the location of MS. In this situation, the SIM of the MS is the only entity that possesses the correct location data, which will be transmitted to the network by means of the location updating procedure. If a MS is switched off (or does not have a SIM), one must avoid the overload of the network with signalling messages toward MS. This can be done by switching a Boolean-type variable at the VLR level, by which the network is informed if the MS is or is not available. When the MS is turned on, the procedure *IMSI attach* is performed, followed by the normal location updating in case the location area has changed. In case MS turns off, the procedure *IMSI detach* is performed, which consists in sending without confirmation a message to the network RIL3-MM IMSI DATACH.

6.2. Contents of the work

Run log_24.log using the command **Step** from the menu **Replay log file**. With **Serving cell** and **Graphical presentation**, Table 12 is filled in. For the first location area, write the parameters of the received signal immediately before passing in the new location area; immediately after this passing, the mentioned parameters correspond to the new location area. It is recommended to run the file with a low speed.

Location area 1					**Location area 2**				
MNC	**LAC**	**ARFCN**	**RxLev**	**RxQual**	**MNC**	**LAC**	**ARFCN**	**RxLev**	**RxQual**

Table 12 – The change of the location area

6.3. Questions

1. Explain the advantages of using the location area from the point of view of sending the paging messages.

2. A location area is controlled by:
    - one or more MSC, but only one BSC;
    - one or more MSC, but only one HLR;
    - one or more BSC, but only one MSC.

3. How can one explain the fact that, when running log_24.log, the change of the location area is not signalled in the moment of performing the handover at 12:13:06.21?

ACRONYM LIST

ARFCN	Absolute RF Channel Number
BCCH	BroadCast Channel
BS	BS
BA–NO	Band Number
BSIC	BS Identity Code
CBCH	CellBroadcast Channel
CC	Call Control
CI	Cell Identity
DCS	Digital Cellular System
IMSI	International Mobile Subscriber Identity
LAC	Location Area Code
LAI	Location Area Identity
MCC	Mobile Country Code
MM	Mobility Management
MMI	Man Machine Interface
MNC	Mobile Network Code
MS	MS
MSC	Mobile Switching Centre
PCH	Paging Channel
LOMS	LOg Mobile Software
PCS	Personal Communication System
RR	Radio Resource
RxLev	Received signal Strength
RxQual	Received signal Quality
SIM	Subscriber Identity Module
TA	Timing Advance
TCH	Traffic Channel
TX Power	Transmitted signal Power