elaman

GERMAN SECURITY SOLUTIONS

Falcon C+

User Manual

GOVERNMENTAL SECURITY SOLUTIONS

GSM-Monitoring System

FALCON C+
User Manual

1. General Definition of Purpose

The Falcon Monitoring System is a mobile application monitoring system used for GSM networks and operates in the 900/1800MHz standard.

The Falcon allows the complete monitoring of the entire GSM data traffic, including the monitoring of voice, SMS and fax traffic. All data will be automatically stored and can be recalled selectively from the various data banks for further use.

The Falcon system fulfils the following main functions:

- Fully passive (non-detectable) off air interception of GSM communication in different modes:
    - ❖ Interception of communication in A5.1 protocols (Ki is necessary)
    - ❖ Interception of communication in A5.2 protocols (real time A5.2 decoder is integrated)
    - ❖ Interception of communication in A5.0 protocols in real time

- Control of the Downlink (base station to mobile phone channel) and of the Uplink (return channel from mobile phone to base station)
- Automatic coordination of the system, automatic channel search of the Base Station Control Channels (BCCH) and registration of their parameters.
- Automatic registration and decoding of telephone conversations based on pre defined adjustable filter criteria and respective storage of these conversations on the integrated 4 channel digital recorder.
- Automatic creation of an archive for recorded telephone conversations with sorting to the subscribers monitored.
- Automatic registration and storage of all available protocols in the GSM network of the monitored base station
- Control of 8 receivers (4 duplex receivers) for the automatic monitoring and recording of max. 4 telephone conversations
- Switching on and off for recording of conversations, text messages (SMS) as well as data transmission (fax messages). The fax messages are stored in a Hexadecimal protocol
- Display of Operating Mode of the 4 Duplex receivers and the activated filter function on the display of the computer

2. Preparation of the system for use

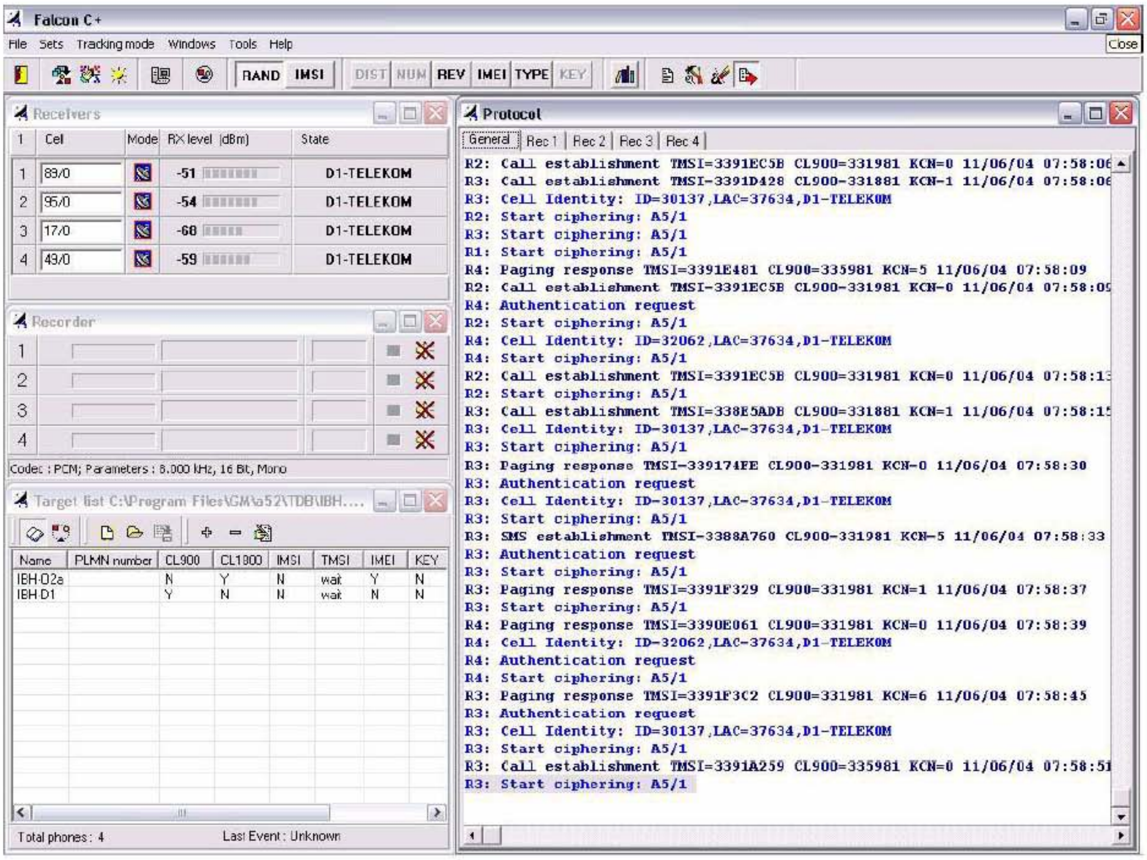
The Falcon system is ready for use without any special preparations. It is merely necessary to ensure that the following connections are made:

- Connect mains power supply cable 230VAC (for stationary application) or 12VDC power supply cable (for mobile application e.g. from a vehicle) to the Falcon Unit
- Connect USB connector cable between Falcon Unit and computer (notebook)
- Connect both dual band magnet base antennas to the Falcon Unit
- Switch on power supply to the Falcon Unit
- Switch on computer (Notebook)
- Start program application Falcon C+ on the computer (Notebook)

The system starts the monitoring process automatically. The user can now set the respective operating modes and filter functions according to his requirements. The target list and the network list are prepared as a software module and can be designed and altered by the user as needed.

3. Operating Instructions

Make sure that all necessary preparations for system use were carried out. After starting the application Falcon C+ on the computer, the following main user window of the main program application is displayed:



1	Cel	Mode	RX level (dBm)	State
1	89/0		-51	D1-TELEKOM
2	95/0		-54	D1-TELEKOM
3	17/0		-68	D1-TELEKOM
4	49/0		-59	D1-TELEKOM

Codec : PCM; Parameters : 8.000 kHz, 16 Bit, Mono

Name	PLMN number	CL900	CL1800	IMSI	TMSI	IMEI	KEY
IBH-O2a		N	Y	N	wait	Y	N
IBH-D1		Y	N	N	wait	N	N

Total phones : 4 Last Event : Unknown

```
R2: Call establishment TMSI=3391EC5B CL900=331981 KCN=0 11/06/04 07:58:06
R3: Call establishment TMSI-3391D428 CL900-331881 KCN-1 11/06/04 07:58:06
R3: Cell Identity: ID=30137,LAC=37634,D1-TELEKOM
R2: Start ciphering: A5/1
R3: Start ciphering: A5/1
R1: Start ciphering: A5/1
R4: Paging response TMSI=3391E481 CL900=335981 KCN=5 11/06/04 07:58:09
R2: Call establishment TMSI-3391EC5B CL900-331981 KCN-0 11/06/04 07:58:09
R4: Authentication request
R2: Start ciphering: A5/1
R4: Cell Identity: ID=32062,LAC=37634,D1-TELEKOM
R4: Start ciphering: A5/1
R2: Call establishment TMSI=3391EC5B CL900=331981 KCN=0 11/06/04 07:58:13
R2: Start ciphering: A5/1
R3: Call establishment TMSI=338E5ADB CL900=331881 KCN=1 11/06/04 07:58:15
R3: Cell Identity: ID-30137,LAC-37634,D1-TELEKOM
R3: Start ciphering: A5/1
R3: Paging response TMSI-339174FE CL900-331981 KCN-0 11/06/04 07:58:30
R3: Authentication request
R3: Cell Identity: ID-30137,LAC-37634,D1-TELEKOM
R3: Start ciphering: A5/1
R3: SMS establishment TMSI-3388A760 CL900-331981 KCN-5 11/06/04 07:58:33
R3: Authentication request
R3: Start ciphering: A5/1
R3: Paging response TMSI=3391F329 CL900=331981 KCN=1 11/06/04 07:58:37
R3: Start ciphering: A5/1
R4: Paging response TMSI=3390E061 CL900=331981 KCN=0 11/06/04 07:58:39
R4: Cell Identity: ID-32062,LAC-37634,D1-TELEKOM
R4: Authentication request
R4: Start ciphering: A5/1
R3: Paging response TMSI=3391F3C2 CL900=331981 KCN=6 11/06/04 07:58:45
R3: Authentication request
R3: Cell Identity: ID=30137,LAC=37634,D1-TELEKOM
R3: Start ciphering: A5/1
R3: Call establishment TMSI=3391A259 CL900=335981 KCN=0 11/06/04 07:58:51
R3: Start ciphering: A5/1
```

During the operation of the program, the channels of the base station which are to be monitored, the mode of decoding of information in these channels, the signal strengths of the down and uplinks, the switching on of the receivers, and all network protocols are displayed. The main program contains numerous sub programs, sub menus and settings to control the Falcon system, which can be called up or activated by the user depending on the operational necessity.

The main window of the application consists of the:

- 1. Header Row, in which the application name and the current software version is displayed
- 2. Header Row, in which the various menus, the modes of operation and the different filters can be called up and activated e.g. File, Sets (Basic Adjustments), Tracking Mode (Modes of Operation), Windows (sub menus), Tools (sub files like recorder data etc.), Help
- 3. Header Row consists of user buttons for quicker selection of sub menus, mode of operation and filter functions

In the left top part of the main window the following is displayed:
Window which displays the Operating Mode of the 4 Duplex receivers

In the left middle part of the main window the following is displayed:
Window which displays the Operating Mode of the 4 channel recorder

In the left bottom part of the main window the following are displayed and made available through a further Header Row:
Target list with the user defined criteria and filters (filled in by the user)
Cell list that contains the registered base stations with all criteria of recognition like provider name, LAC, ID, BCCH, signal strength etc.

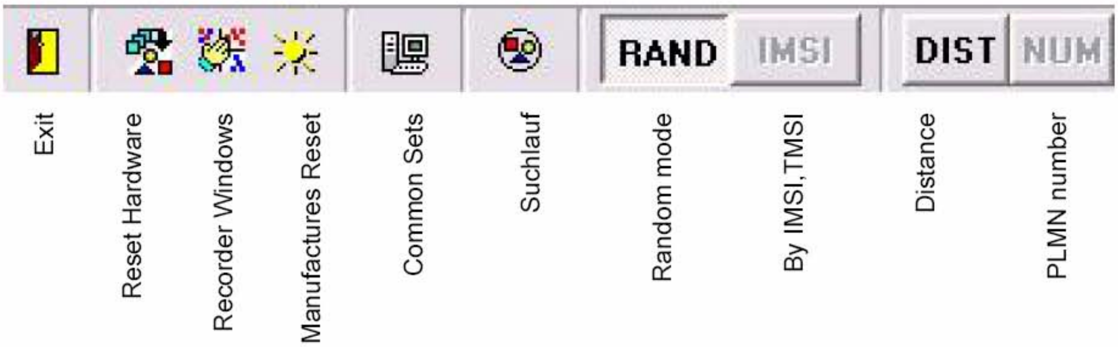
In the right part of the main window (protocol) the following is displayed:
Protocols and events of the entire data traffic in the base station to be monitored

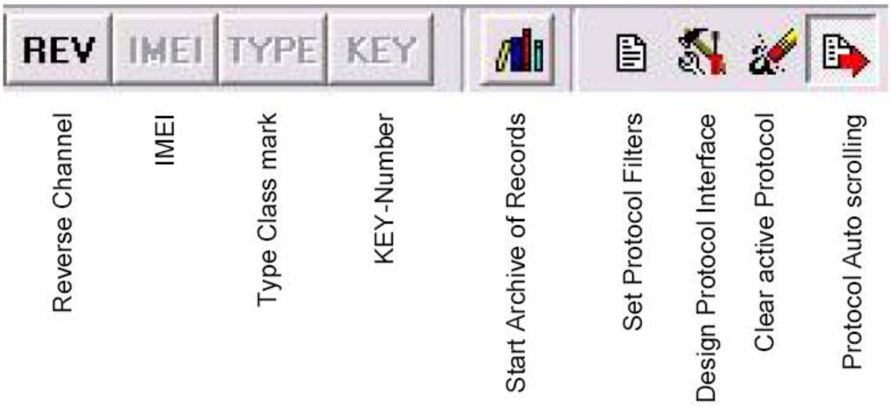
These windows can be moved, maximised, made smaller, minimized and closed by the user.
These changes can be made with the usual windows commands.

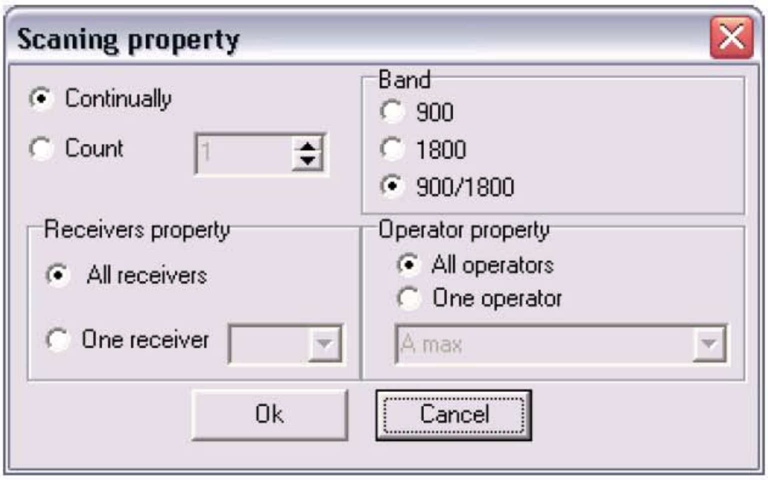
With the command Recorder windows in the menu Windows or with button all windows are restored to their original default setting.

3.1. Toolbar

User Buttons in the main menu allow quick access to the different sub menus and basic settings of the System.







Scaning property

● Continually
○ Count 1

Band
○ 900
○ 1800
● 900/1800

Receivers property
● All receivers
○ One receiver

Operator property
● All operators
○ One operator
A max

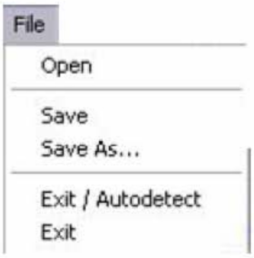
Diagnose
This button serves to diagnose the system and should under no circumstance be used during normal operation.

Scanning Property
If this button is pressed, the dialog window for the scanning mode of the receivers is called up.

In this menu the operator can define in which frequency range the receiver should carry out the scanning operation.

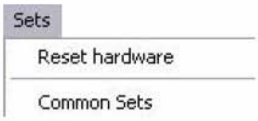
3.2. Menu

3.2.1. File Menu



- *EXIT –*
  The operation of the FALCON is shut down, whereas the basic settings and the protocols are stored on the hard disk of the computer (Notebook) in an orderly manner.

3.2.2. Sets Menu

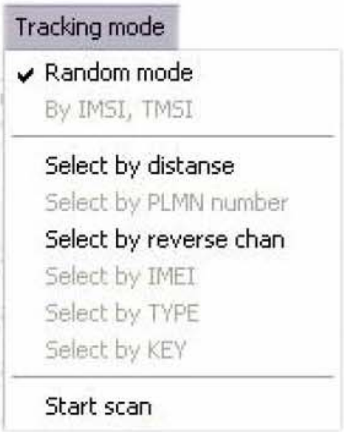


In this menu, the general settings for the operation of the FALCON are made.
(*see also 5. Parameter Settings – FALCON, page 24*)

- Reset Hardware –
  With this command, the receivers are set on the corresponding channels, and the basic settings of the parameters are carried out.

- Common Sets –
  With this command the operator reaches the parameter menu. The corresponding dialog window to enter the parameters opens.

3.2.3. Tracking Mode Menu



In this menu the operator can set the different modes of operation for the FALCON.

There is a choice of 3 main modes of operation, whereby only one mode of operation will work at a time i.e. only one main mode of operation of the FALCON is possible, not simultaneous operation:

- Random Mode – RAND

  In this mode of operation all phone conversations and SMS are registered and recorded in the radio cell to be monitored.

- Type Classmark – TYPE
  In this mode of operation only mobile phones of a pre-defined type are registered, and their conversations and SMS taken to protocol and recorded.

- By IMSI, TMSI – IMSI
  In this mode of operation, only subscribers that are registered in the target list by their IMSI, TMSI are monitored.

To every main mode of operation, several sub modes of operation can be designated to work with the main mode at the same time, enabling the operator to monitor a target selectively and based on different criteria.

- `Select by distance` – DIST
  If this filter criteria is active, only mobile phones which are operating in the pre-defined distance from the base station will be monitored.

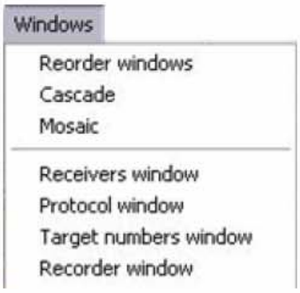
- `Select by PLMN number` – NUM
  If this filter criteria is active, only mobile phones who have their PLMN number registered in the target list will be monitored.

- `Select by reverse chan` – REV
  If this filter criteria is active, only conversations where the reverse channel of the mobile phone (Uplink) is received, will be monitored. With this filter function, it makes it easier to monitor mobile phones which are in close vicinity of the FALCON system.

- `Select by IMEI` – IMEI
  If this filter function is active, only mobile phones who have their IMEI registered in the target list are monitored.

- `Select by KEY` – KEY
  If this filter function is active, only mobile phones who have their KEY registered in the target list are monitored

3.2.4. Windows Menu



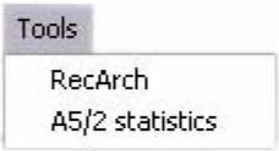
The commands in this menu are used for the control of the different Windows of the main menu. The settings or attributes of these Windows can be changed/ defined by the user and can be sorted in different ways as required.

- `Recorder Windows` – With this command, all win dows are restored to their original default setting.
- `Cascade` – here the different windows are presented in an overlaying/cascade format in the usual windows manner
- `Mosaic` – here the menus are displayed in a quadratic/mosaic format in the usual windows manner

In the second part of this menu, the following functions are available:

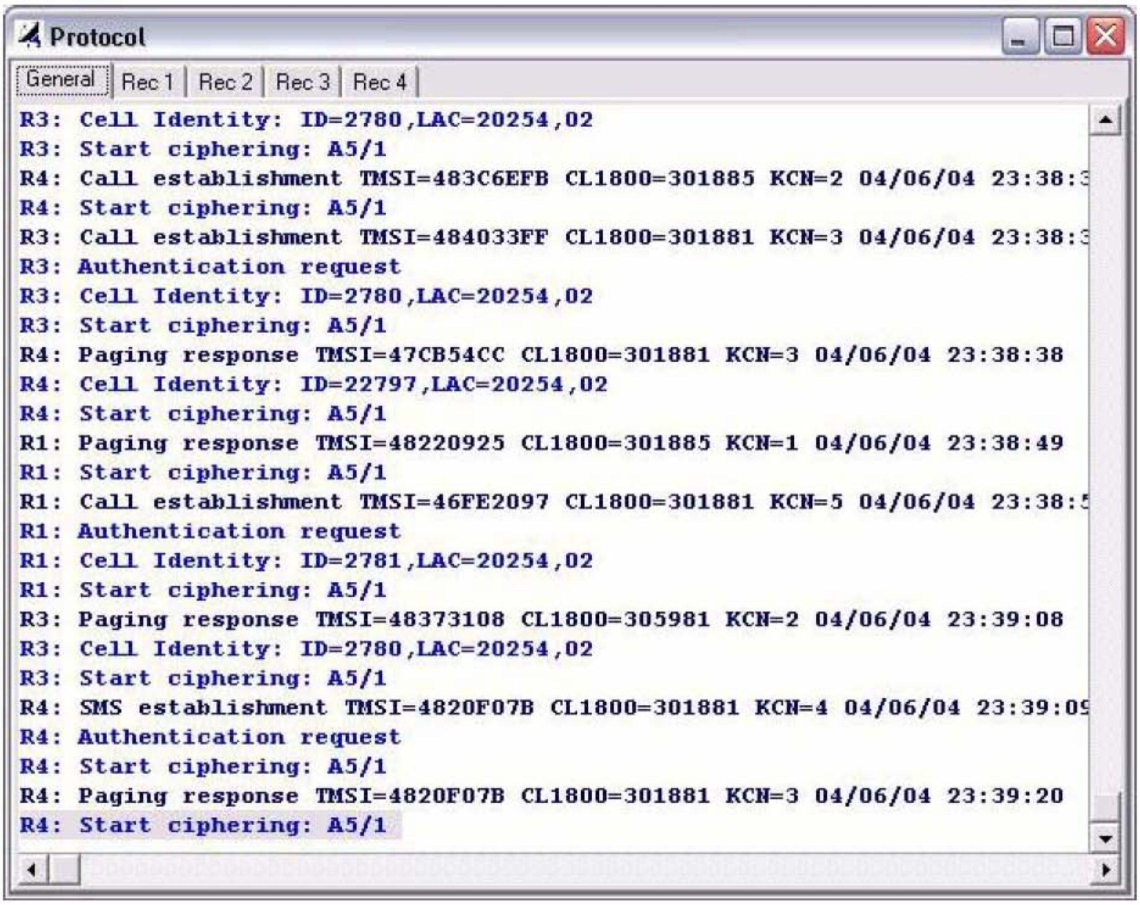
- Receivers window – to activate the Receiver Window
- Protocol window – to activate the Protocol Window
- Target numbers window – to activate the Target List Window
- Recorder window – to activate the Recorder Window

3.2.5. Tools Menu



In this menu, the operator has access to the data that was registered by the FALCON.
In this menu there is also an access to the A5/2 statistics.

3.3. The Protocol window



```
R3: Cell Identity: ID=2780,LAC=20254,02
R3: Start ciphering: A5/1
R4: Call establishment TMSI=483C6EFB CL1800=301885 KCN=2 04/06/04 23:38:3
R4: Start ciphering: A5/1
R3: Call establishment TMSI=484033FF CL1800=301881 KCN=3 04/06/04 23:38:3
R3: Authentication request
R3: Cell Identity: ID=2780,LAC=20254,02
R3: Start ciphering: A5/1
R4: Paging response TMSI=47CB54CC CL1800=301881 KCN=3 04/06/04 23:38:38
R4: Cell Identity: ID=22797,LAC=20254,02
R4: Start ciphering: A5/1
R1: Paging response TMSI=48220925 CL1800=301885 KCN=1 04/06/04 23:38:49
R1: Start ciphering: A5/1
R1: Call establishment TMSI=46FE2097 CL1800=301881 KCN=5 04/06/04 23:38:5
R1: Authentication request
R1: Cell Identity: ID=2781,LAC=20254,02
R1: Start ciphering: A5/1
R3: Paging response TMSI=48373108 CL1800=305981 KCN=2 04/06/04 23:39:08
R3: Cell Identity: ID=2780,LAC=20254,02
R3: Start ciphering: A5/1
R4: SMS establishment TMSI=4820F07B CL1800=301881 KCN=4 04/06/04 23:39:0
R4: Authentication request
R4: Start ciphering: A5/1
R4: Paging response TMSI=4820F07B CL1800=301881 KCN=3 04/06/04 23:39:20
R4: Start ciphering: A5/1
```

In the protocol window all events of the Falcon System are registered and displayed like for example:

- Data in the monitored radio cell of the base station
- Sorting of the receivers to the channels monitored
- Sorting of IMSI, the TMSI, the phone number, SMS and data traffic etc.

All this data is made available to the user for a quick assessment of the situation within the monitored cell. The data is stored in full in the memory of the computer (notebook) and is readily available for further use and later analysis of the radio traffic of the monitored cell.

The protocol window possesses a line structure; this means each line carries the information of an event in the data traffic of the cell. Through a right click of the mouse, the user has quick access to the displayed data.

The following belong to the main group of data:

- Data of the base station control channel (Common Control Channel)
- Connection data during establishment of the connection between mobile phone and base station (Establishment Connection)
- Data in the dedicated voice channel (will only be dedicated for the duration of the conversation). Only the signal of the base station will be registered and analysed (Dedicated Channel)

- System message like for example data of the working regime, change of channel, hopping, error messages in the GSM system etc.
- Data for network diagnosis and test signals in the GSM network (Test Messages)

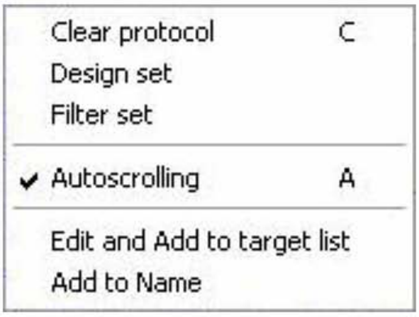
Each data group possesses its own format. The search filters integrated in the Falcon permit a direct access to this data.
Following is an explanation with regard to the direct and indirect channel (Uplink/Downlink):
Events in the control channel of the base station (CCCH- Common Control Channel) are displayed as follows:

- R - number of the active receiver, activity, date and time of the event
- Event – here events of the data exchanges in the cell can be displayed.

(more information see *6. Additional Information to GSM-Network, Page 33*)

3.3.1. Submenu of the Protocol Window

Through click of the right mouse button on the required event line in the protocol window, the corresponding sub menu is displayed. The chosen event line is displayed with yellow shading.



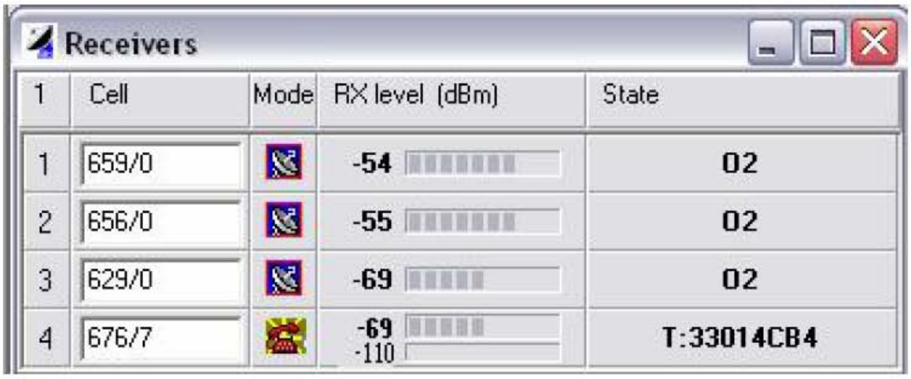
The menu is divided into 3 groups:

1. Group
   This group contains commands for adjustment of the design and the choice of filters like:
   - Clear Protocol – the contents of the protocol window is deleted with this command
   - Design Set – the design like for example the colour, the font, font size and other display attributes can be changed with this command
   - Filter Set – the different choices of filter can be activated with this command

2. Group
   - Autoscrolling – with this command autoscrolling in the protocol window is either switched on or off

3. Group
   - Edit and add to target list – data of the protocol can be sorted to the target immediately (phone number, IMSI, TMSI)
   - Add to name – parameters of the protocol can be sorted to a target

3.4. The Receiver Window



Receivers

1	Cell	Mode	RX level (dBm)	State
1	659/0		-54	02
2	656/0		-55	02
3	629/0		-69	02
4	676/7	☎	-69 -110	T:33014CB4

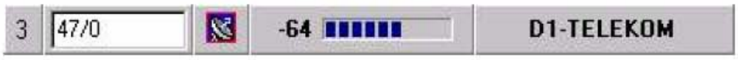
The dynamic condition of the 4 duplex receivers is displayed in the receiver window. The following details are displayed:

- The number of receiver from 1-4
- The mode of the receiver, active or inactive
- The signal strength of the down and uplink (upper line-signal strength of base station, lower line –signal strength of the mobile phone) The information is given in dBm.

This information is very useful for an effective placement of the antennas of the Falcon system.

- Display of the network provider and of the TDMA – Slots

3.4.1. Receiver Line



3	47/0		-64	D1-TELEKOM

This line contains different information about the receiver like:

3

Number field of the receiver
This field displays the receiver number. A certain receiver is always dedicated to the information of the protocol.

47/0

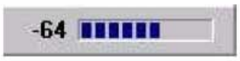
`Field for channel number and TDMA slot`

The channel being received from the base station on which the receiver is set is displayed in this field.
In the 900 MHz standard the channels 1-125 are used.
In the 1800 MHz standard the channels 512-885 are used.
The figure after the channel number (0-7) stipulates the TDMA-Slot that is being used. If frequency-hopping mode is used in the GSM network, the word "*HOPPING*" is displayed and no channel is shown.

After selecting this field by mouse click, a channel number can be entered and newly dedicated to the receiver.

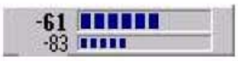
Field for receiver mode

This field displays if the receiver is active or inactive. In this display mode the receiver is set on the control channel of the base station (CCCH Common Control Channel). In this display mode the receiver monitors a dedicated voice channel.



Field for signal strength

In this field the current signal strength of the monitored channel is displayed. The bar display gives a reading of the signal strength of the base station in dBm (Downlink).



Is a mobile phone received (Uplink), its signal strength is displayed underneath.
With help of these signal strength readings being displayed, the operator is in the position to obtain optimum reception of the monitored base station as well as target (mobile phone) by carrying out antenna manoeuvres until signal strength is at its best.

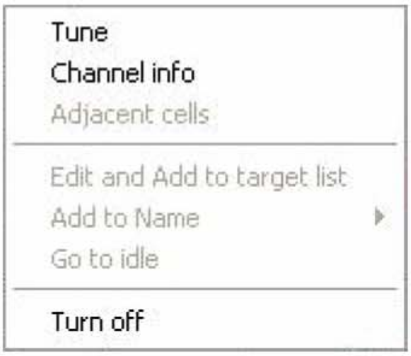
Status Field

In this field, different items can be displayed in connection with the GSM network like:

- If the receiver is set on the CCCH Channel of the base station, the name of the network provider is displayed. Is the name not known the MCC (Mobile Country Code) and MNC (Mobile Network Code) are displayed.
- If the receiver is in search mode, *searching* is displayed
- If the receiver is operating in a dedicated *SDCCH/4* (Stand Alone Dedicated Control Channel) respectively *SDCCH/8* is displayed, depending on whether the system is operated with 4 or 8 channels.

3.4.2. Sub Menu of the Receiver Window

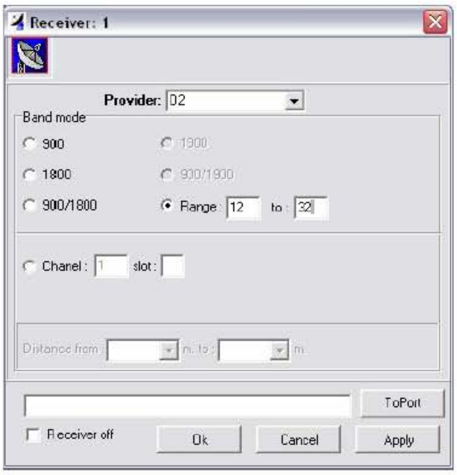
If the cursor is placed on this button, a receiver sub menu can be opened by a right mouse click:



The following commands can be carried out:

- Tune – the sub menu for the receiver is opened. The receiver can be configured
- Channel Info – the sub menu channel info is opened
- Adjacent cells – this menu shows the adjacent cells of the GSM network
- Edit and add to target list – information from the protocol can be sorted to the target list (dialog window)
- Add to name – parameters can be sorted to a target person
- Go to idle – this command can only be executed, if the receiver is receiving a conversation and is used to reset the receiver to standby after a conversation is concluded
- Turn off – the receiver is switched off

3.4.2.1. Tune



Receiver: 1

Provider: 02

Band mode

○ 900 ○ 1900

○ 1800 ○ 900/1900

○ 900/1800 ● Range: 12 to: 32

○ Chanel: 1 slot:

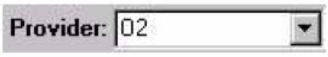
Distance from: m. to: m.

ToPort

□ Receiver off

Ok Cancel Apply

In this menu the settings for each of the 4 duplex receivers can be carried out. Parameters for the receivers are entered manually, this means:



Provider: 02

`Choice of Network Providers`

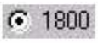
Under provider there is a list of GSM network providers from different countries, which can be updated as required by the user.

`Choice of Frequency Band`

Under band mode the user can manually choose in which frequency range the GSM monitoring should take place:

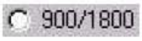
○ 900

`Search in frequency range 900MHz`



● 1800

`Search in frequency range 1800MHz`

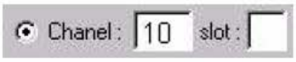


○ 900/1800

`Search in frequency range 900 and 1800 MHz`

● Range: 12 to: 23

`Search in interval of channels`

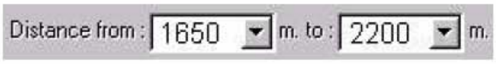


● Chanel: 10 slot:

`Setting the receiver to a specific channel and TDMA – Slot`

With this receiver setting please note that only the following channels and TDMA-Slots can be set:

900MHz Band:	Channel 1-124
1800MHz Band:	Channel 512-885
TDMA Slot:	0-7



Distance from : 1650 m. to : 2200 m.

Search in a defined distance

When the receiver is operated in this mode, only mobile phones that are being operated in the specified distance form the base station are monitored. Mobile phones that are located outside this zone from the base station are being ignored.

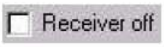
This choice of criteria is very helpful in order to concentrate on certain specific targets, which are to be monitored.

Please note that this choice of criteria can only be activated, if the receiver is set on a fixed channel of the base station to be monitored.

In the search mode of the receiver, this choice of criteria is inactive.

Working in the mode – to port

This mode setting is not supported by the provided software version.



□ Receiver off

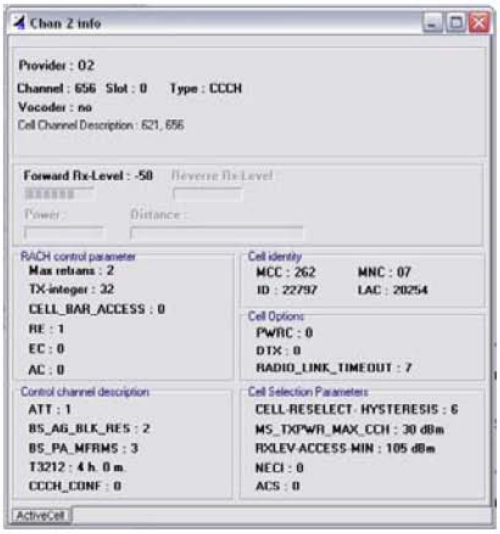
Receiver off

Thorough this field the selected receiver can be switched on respectively off.

Buttons for receiver settings

- *Ok* – the dialogue for receiver settings is confirmed and concluded. The receiver works with the adjusted settings.
- *Cancel* – the dialogue for receiver settings is cancelled, whereas the initially made settings remain unchanged
- *Apply* – the receiver settings are immediately transferred to the receiver, without closing the dialogue window

3.4.2.2. Channel Info



Chan 2 info

Provider : 02
Channel : 656 Slot : 0 Type : CCCH
Vocoder : no
Cell Channel Description : 621, 656

Forward Rx-Level : -58 Reverse Rx-Level :
Power : Distance :

RACH control parameter
Max retrans : 2
TX-integer : 32
CELL_BAR_ACCESS : 0
RE : 1
EC : 0
AC : 0

Cell identity
MCC : 262 MNC : 07
ID : 22797 LAC : 20254

Cell Options
PWRC : 0
DTX : 0
RADIO_LINK_TIMEOUT : 7

Control channel description
ATT : 1
BS_AG_BLK_RES : 2
BS_PA_MFRMS : 3
T3212 : 4 h. 0 m.
CCCH_CONF : 0

Cell Selection Parameters
CELL-RESELECT- HYSTERESIS : 6
MS_TXPWR_MAX_CCH : 30 dBm
RXLEV-ACCESS-MIN : 105 dBm
NECI : 0
ACS : 0

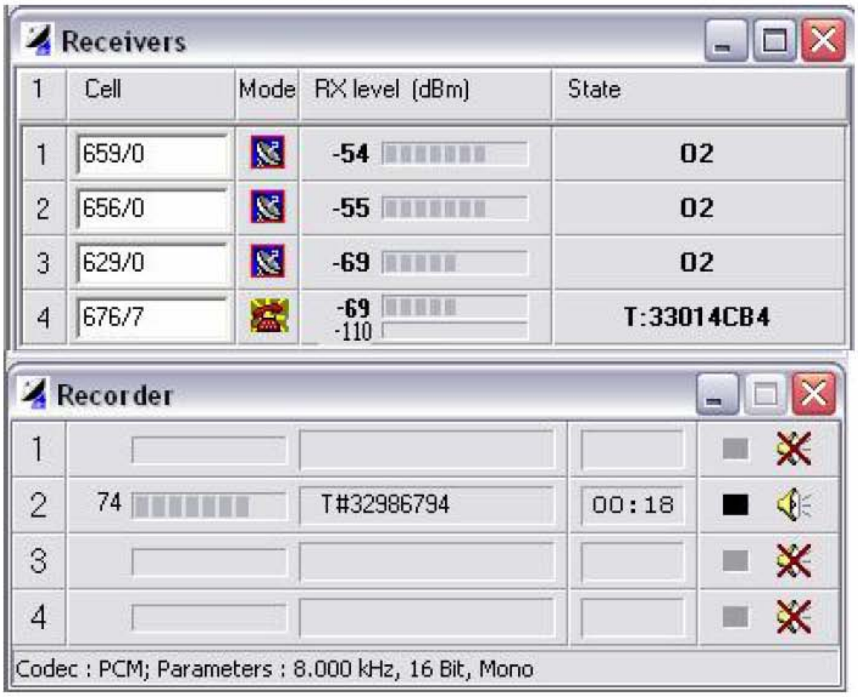
In this menu, details about the characteristics of the GSM network to be monitored are given.

The following GSM network parameters are made available to the user for assessment:

- `Provider` – Name of the network provider out of the MCC (Mobile Country Code) and MNC (Mobile Network Code) list
- `Channel, Slot, Type` – displayed will be the number of the control channel, the slots and the type of channel (Stand Alone Control Channel) on which the receiver is set
- `Vocoder` – type of speech coder used for the traffic channel
- `Cell Channel Description` – description of the channel in short format
- `Neighbour Cells` – list of neighbour cells of the GSM network
- `Forward RX level` and `reverse RX level` – alphanumerical display and bar diagram display of receiving signal field strength in dBmW of the up and downlink
- `Power` – Output power of the mobile phone to be monitored in dBmW and in bar diagram display
- `Distance` – distance in meters between the base station and the mobile phone to be monitored
- `T3212` – Time slot for validity of the TMSI in the network
- `MCC` – Mobile Country Code
- `MNC` – Mobile Network Code

In the window *Channel* Info further parameters of the GSM network are displayed which are however of no great importance for the operational tasks and use of the Falcon System.

3.5. The Recorder Window



Receivers

1	Cell	Mode	RX level (dBm)	State
1	659/0		-54	02
2	656/0		-55	02
3	629/0		-69	02
4	676/7	☎	-69 -110	T:33014CB4

Recorder

1					
2	74	T#32986794	00:18	■	
3					
4					

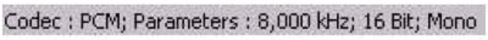
Codec : PCM; Parameters : 8.000 kHz, 16 Bit, Mono

Through this program window the user can work on the audio information. The audio information is transferred from the Main Unit to the computer (Notebook) of the Falcon through the USB-Cable.

- The following functions for each of the 4 recorders can be controlled through this window:
- START and STOP of recording
- PAUSE
- Parallel recording with all 4 recorders simultaneously
- Listening in of the recording in real time on any of the 4 recorders

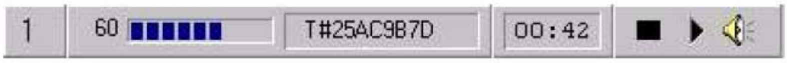
One receiver is designated for each recorder. The recording takes place automatically, can however be interrupted by the operator.

The Recorder Window displays the following additional information, like:



Codec : PCM; Parameters : 8,000 kHz; 16 Bit; Mono Status Line – In general

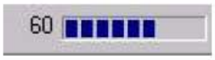
3.5.1. Recorder Line



There is one status line for each of the 4 recorders, which gives information on the activity of the particular recorder.

`Channel Number`

The number of the recorder is identical with the number of the receiver from which the audio information is being provided.

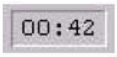


`Signal Strength`

In this status line the dynamic signal strength of the signal to be recorded is displayed. The display is in an alphanumerical format as well as in a bar diagram.

`Designation of the Audio-File`

In this status line the file name of the audio recording under which it will be stored in the recorder archive is displayed. During the monitoring of a conversation the file name is created automatically. In addition, the TMSI of the subscriber whose conversation is being recorded is displayed. When the cursor is placed on this field, additional information on the audio file can be called up by a right click of the mouse.



`Recording Duration`

This field displays how long the recording is already active. The display is in minutes and seconds.

Description of Recorder User Buttons

● ■

`START/STOP`

When the cursor is placed on these buttons, the recorder can be started or stopped with the left mouse button.

▶ ❚❚

`PAUSE/Continuation of recording`

When a recording is carried out, the pause button can stop it manually, respectively the recording can be continued by clicking the continuation button.

🔈 🔇

`ON/OFF of Listening In Channel`

Through these buttons it is possible to listen in to a running recording. The switching on and off of the computer's (Notebook) speakers is carried out with these buttons.

3.6. The List Window

User Buttons of the List Window

This button activates the List Window Target List.

This button activates the List Window Cell List.

With this button a new list (Target List or cell List) can be created.

With this button a list stored on the hard disk of the computer (Notebook) can be loaded/opened.

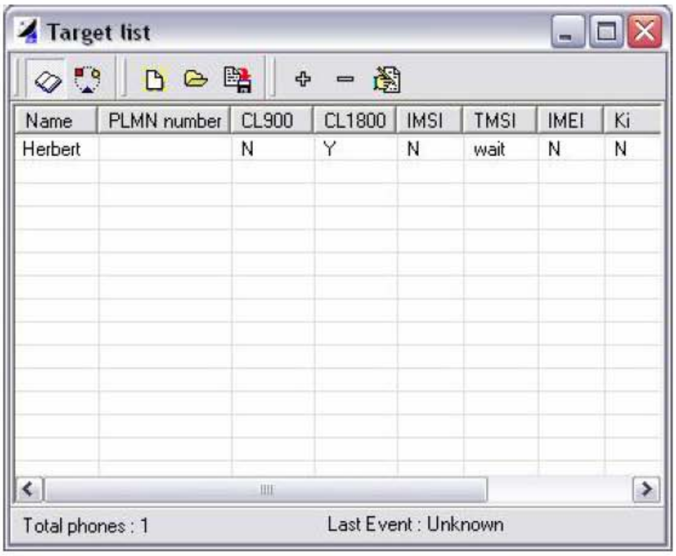
With this button, the active list can be stored on the hard disk of the computer (Notebook). A standard windows dialogue window will open in this process, where the file name and the folder can be defined.

With the button ADD, a new row for data can be added to the list.

With the button REMOVE, a row of data can be removed from the list.

With the button CHANGE, the contents of the data row can be changed.

3.6.1. Target List



Target list

Name	PLMN number	CL900	CL1800	IMSI	TMSI	IMEI	Ki
Herbert		N	Y	N	wait	N	N

Total phones : 1   Last Event : Unknown

This window is used for the creation of a target list and for the definition of the search criteria to be used for each target (mobile phones to be monitored). Sorting of the data can be carried out within each column by the usual windows commands.

3.6.1.1. Meaning of each Column in the Table

1. *Name* – here a name can be designated to any target in order to thereafter ease the identification of the subscriber.

2. *PLMN Number* – this is the number that has to be dialled in order to call the subscriber (Public Land Mobile Network). If the PLMN Number from incoming and outgoing calls is identified by the FALCON, the monitoring can be carried out by this criteria. Should the option of withholding own number sending be activated, no monitoring can be carried out by this criteria.

   3 different types of information can be displayed in the column PLMN Number:
   - Unavailable – means that the network is not able to identify the incoming number
   - Anonymous – means that the sender has activated the option of withholding own number sending, or the network does not support this service
   - Absent – this message is displayed if the number of the caller has not been transferred in the network

   The selection based on PLMN – Number is only possible, if Down- as well as Uplink are available. The selection based on PLMN – Number makes it easy to control incoming calls made to the monitored subscriber.

3. *CL 900* and *CL 1800* – are parameters of the mobile phone (Classmark/key type) of the subscriber during operation in both frequency ranges (Networks).
   - Is YES displayed, the subscriber will be monitored/selected based on the type of mobile phone he is using
   - Is NO displayed, monitoring of all mobile phones of this type in the radio cell is taking place

4. *IMSI* – is the number of identification of the subscriber (International Mobile Subscriber Identity) that is stored on the SIM card.
   - Is YES displayed, the subscriber will be monitored based on his IMSI.

5. *TMSI* – is the two-digit number of the subscriber in the GSM Network (Temporary Mobile Subscriber Identity).
   - Is YES displayed, the subscriber will be monitored in the GSM network based on this number.

   The IMSI or TMSI of the subscriber to be monitored can be obtained by giving the subscriber a purposely-aimed call. The IMSI/TMSI of the subscriber will then be displayed in the protocol window of the FALCON and can then immediately be utilized as search criteria in the TARGET LIST.

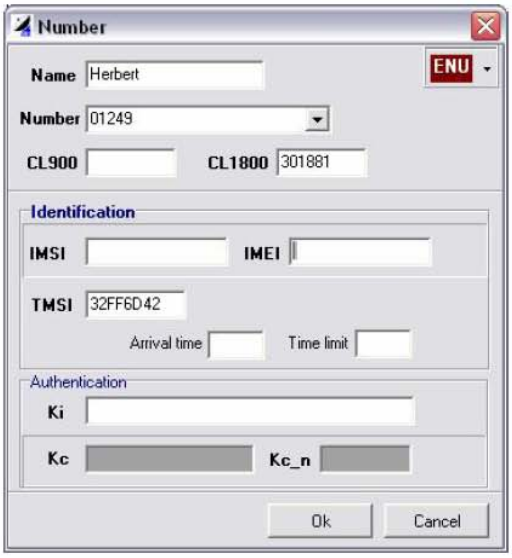
6. *Ki* – is the individual key of authentication/identification of the subscriber. The Ki is stored on the SIM card of the subscriber as well. Is the GSM-network operating in an encrypted mode, the Ki is used as decisive search criteria.
   - Is YES displayed, the subscriber will be monitored based on this search criteria.

7. *Kc* – is a special key for the current conversation, which is being held encrypted in the GSM-network. This key will never be transmitted in the network. It will be calculated in the mobile phone as well as in the network and serves to decode the conversation.

8. *Last Event* – shows the last activities of this subscriber in the network.

3.6.1.2. Edit the Data Line

When the cursor is placed on the field NAME and it is activated with the right mouse button, the window Number opens.



Number

Name: Herbert

Number: 01249

CL900:

CL1800: 301881

Identification

IMSI:

IMEI:

TMSI: 32FF6D42

Arrival time:

Time limit:

Authentication

Ki:

Kc:

Kc_n:

In this window, the target can be defined and respective search criteria can be pinpointed/entered. In the process of monitoring a target the details are partly updated automatically respectively manually.

Description of Fields for entering Information

Name: Test

In order to create a new target in the Target List, a name has to be given so that sorting of different data to this name at a later stage can be carried out. Any choice of name can be entered for the subscriber to be monitored.

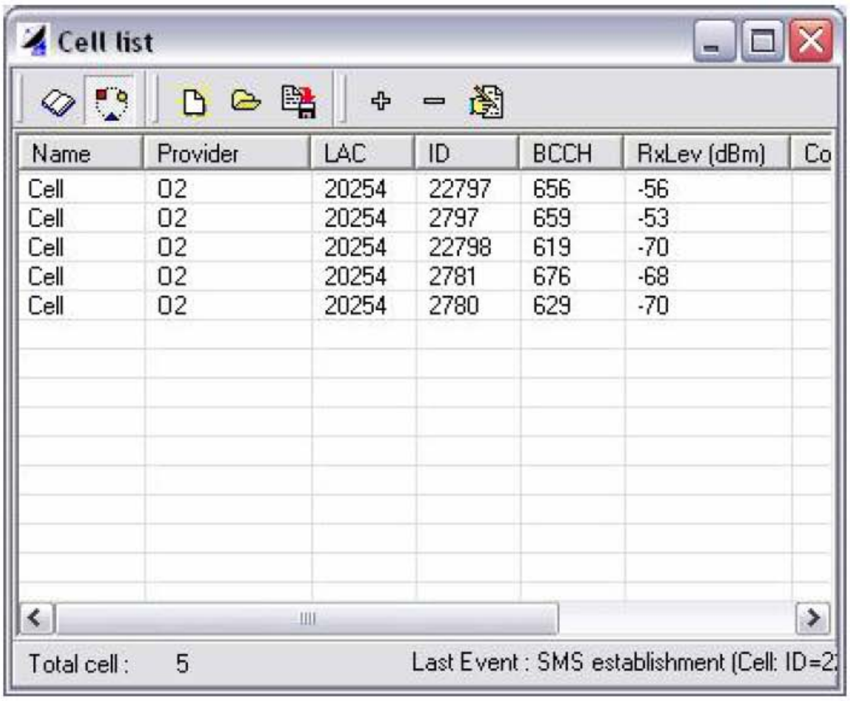
Number: 012345

The phone number to be monitored is entered in this field. Apart from numbers, the symbols +;-;? Can be used. All other symbols if entered will be ignored and the system will show an error message.

The question mark ? can be inserted instead of any unknown digit of the phone number. This function is especially helpful if the operator does not possess the complete phone number of the target person.

All further fields of the menu are updated if the requested data will become available in the course of the monitoring process.

3.6.2. Cell List



Cell list

Name	Provider	LAC	ID	BCCH	RxLev (dBm)	Co
Cell	02	20254	22797	656	-56	
Cell	02	20254	2797	659	-53	
Cell	02	20254	22798	619	-70	
Cell	02	20254	2781	676	-68	
Cell	02	20254	2780	629	-70	

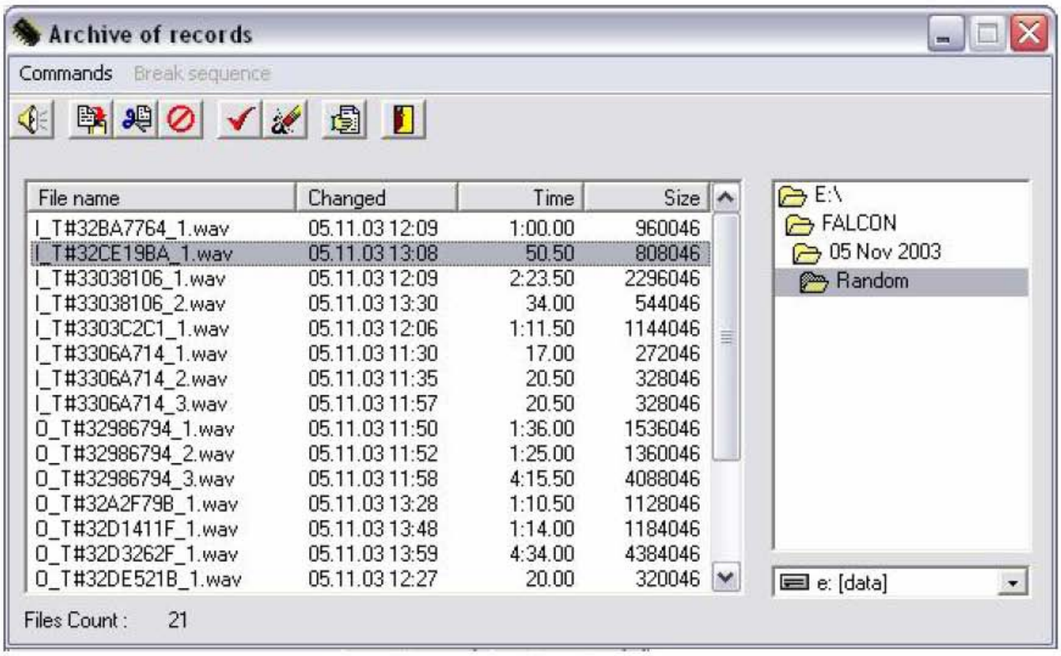
Total cell : 5 Last Event : SMS establishment (Cell: ID=2

All details that characterize the base stations are registered in the program window Cell List. The table is created during the search mode of the receiver (during start-up of FALCON) and can be updated by the operator during the monitoring process.
Every column of this table can be sorted by using the standard windows commands.

3.6.2.1. Meaning of each Column in the Table

1. *Name* – any name of choice can be entered by the operator for the base station (e.g. Hotel Orion)
2. *Provider* – name of network provider in short (is present in a file in FALCON which can be updated as required)
3. *LAC* – is the Location Area Code, which is given out in the GSM-network and fixed for the different areas
4. *ID* – is the number of identification of the base station, which is only given out once in the GSM-network-standard (also from country to country)
5. *BCCH* – is the control channel of the base station (Broadcast Control Channel)
6. *RXLev(dBm)* – receiving field strength for the channel of the base station (Downlink), measured in dBm
7. *Commentary* – in this field the operator can add details with regard to the location of the base station, about the antenna direction etc.

4. Archive – Audio Recordings (Archive of Records)



File name	Changed	Time	Size
I_T#32BA7764_1.wav	05.11.03 12:09	1:00.00	960046
I_T#32CE19BA_1.wav	05.11.03 13:08	50.50	808046
I_T#33038106_1.wav	05.11.03 12:09	2:23.50	2296046
I_T#33038106_2.wav	05.11.03 13:30	34.00	544046
I_T#3303C2C1_1.wav	05.11.03 12:06	1:11.50	1144046
I_T#3306A714_1.wav	05.11.03 11:30	17.00	272046
I_T#3306A714_2.wav	05.11.03 11:35	20.50	328046
I_T#3306A714_3.wav	05.11.03 11:57	20.50	328046
O_T#32986794_1.wav	05.11.03 11:50	1:36.00	1536046
O_T#32986794_2.wav	05.11.03 11:52	1:25.00	1360046
O_T#32986794_3.wav	05.11.03 11:58	4:15.50	4088046
O_T#32A2F79B_1.wav	05.11.03 13:28	1:10.50	1128046
O_T#32D1411F_1.wav	05.11.03 13:48	1:14.00	1184046
O_T#32D3262F_1.wav	05.11.03 13:59	4:34.00	4384046
O_T#32DE521B_1.wav	05.11.03 12:27	20.00	320046

E:\
FALCON
05 Nov 2003
Random

e: [data]

Files Count : 21

The program Archive of Records serves to listen and sort the recorded audio information. Through the buttons in the tool bar fast access to all commands of the program are given.

The user window of the program is divided into 3 main areas:

- List of audio files
- List of folders
- Protocol windows

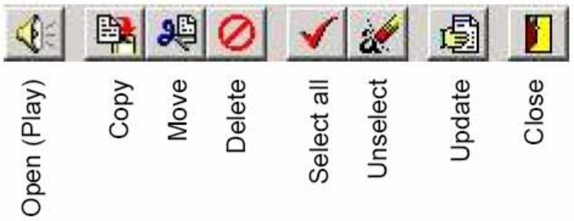
Pressing CTRL and the left mouse button carries out the selection of the files in the usual windows manner.

In the list of the audio files, the following is displayed:

- Name of the audio file (File name)
- Date and time of the recording (Changed)
- Duration of the audio recording (Time)
- File size (Size)

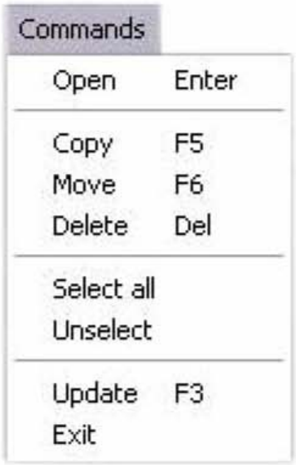
The operator can carry out sorting in the individual columns by using the usual windows commands.

4.1. Toolbar



4.2. Menu

4.2.1. Commands Menu



- Open –
  To listen to a selected file or a group of selected files

- Copy –
  A dialog window is opened. A selected file or a group of selected files can be copied into a different folder. A new folder can be created when doing this.

- Move –
  A dialog window is opened. A selected file or a group of selected files can be moved to another folder. A new folder can be created when doing this.

- Delete –
  A selected file or a group of selected files can be deleted. Files in a selected folder or empty folders can also be deleted.

- Select all –
  All files in a selected folder are selected.

- Unselect –
  The selection is cancelled

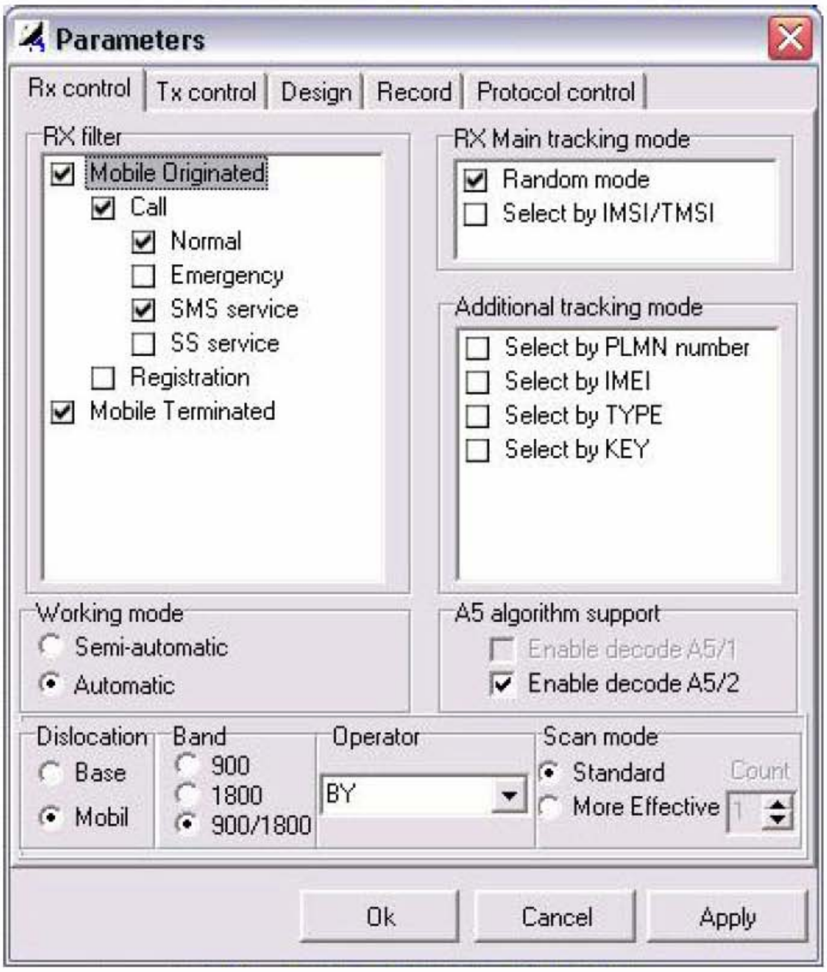
- Protocol
  The Protocol window displayed on/off.

- Update –
  The displayed information is updated

- Exit –
  The application will be shut down. The current settings and data are stored in the Archive of Records of the computer (Notebook).

5. Parameter Settings – FALCON

5.1. Rx control



RX filter
- ☑ Mobile Originated
  - ☑ Call
    - ☑ Normal
    - □ Emergency
    - ☑ SMS service
    - □ SS service
  - □ Registration
- ☑ Mobile Terminated

RX Main tracking mode
- ☑ Random mode
- □ Select by IMSI/TMSI

Additional tracking mode
- □ Select by PLMN number
- □ Select by IMEI
- □ Select by TYPE
- □ Select by KEY

Working mode
- ○ Semi-automatic
- ● Automatic

A5 algorithm support
- □ Enable decode A5/1
- ☑ Enable decode A5/2

Dislocation
- ○ Base
- ● Mobil

Band
- ○ 900
- ○ 1800
- ● 900/1800

Operator: BY

Scan mode
- ● Standard
- ○ More Effective

Count: 1

In the left program window, the event filters that are being used directly by the FALCON are displayed. These event filters differ from the filters that can be activated to select a subscriber in the protocol.

FALCON receives and works only with information and events that are activated/ switched on for the respective event filters.

In case the operator is not interested in certain information and events of the GSM-network, it is advisable to switch off the respective event filters in order not to place an unnecessary burden on the receivers.

The FALCON system can be operated in 3 main modes of operation:

- RANDOM MODE
- BY IMSI/TMSI

5.1.1. Event Filters

1. *RANDOM MODE* – monitoring of a complete GSM radio cell

1.1. MOBILE ORIGINATED – outgoing calls

1.1.1. *CALL* – calls allowed

1.1.1.1. *NORMAL* – general calls

1.1.1.2. *EMERGENCY* – alarm or emergency number calls

1.1.1.3. *SMS* – sent SMS

1.1.1.4. *SS* – additional services of the network provider

1.1.2. *REGISTRATION* – registration in the network allowed

1.1.2.1. *POWER ON* – switching on of the mobile phone power supply

1.1.2.2. *NORMAL* – with the movement of the mobile phone in the network

1.1.2.3. *PERIODIC* – periodic registration

1.1.2.4. *POWER OFF* – switching off of the mobile phone power supply

1.2. *MOBILE TERMINATED* – incoming calls and messages

In every one of these 3 user modes, 1 or more choice of filters for selection of a subscriber can be switched on/activated.

5.1.2. Choice Filters

1. SELECT BY PLMN NUMBER – for the selection by the country (city) code

1.1. CONNECTED NUMBER – for a fixed dedicated number

1.2. CALLING NUMBER – for the phone number of the caller

1.3. DIALING NUMBER – for the dialled number

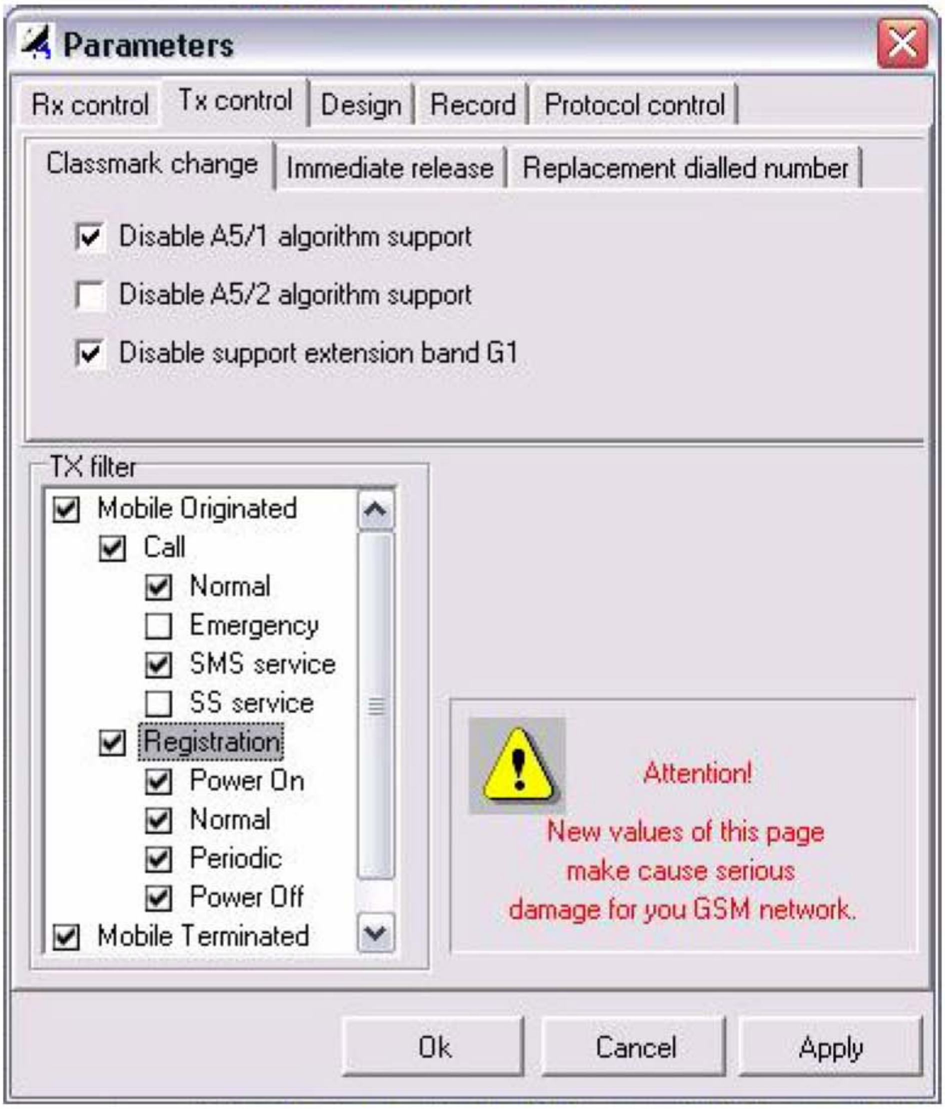
2. SELECT BY IMEI – selection by IMEI number of the mobile phone

2.1. ABSENT – for the conversations where no IMEI number was transferred/transmitted

3. *TYPE CLASSMARK* – choice by type of mobile phone

5.2. TX control

5.2.1. Classmark Change



☑ Disable A5/1 algorithm support

□ Disable A5/2 algorithm support

☑ Disable support extension band G1

TX filter

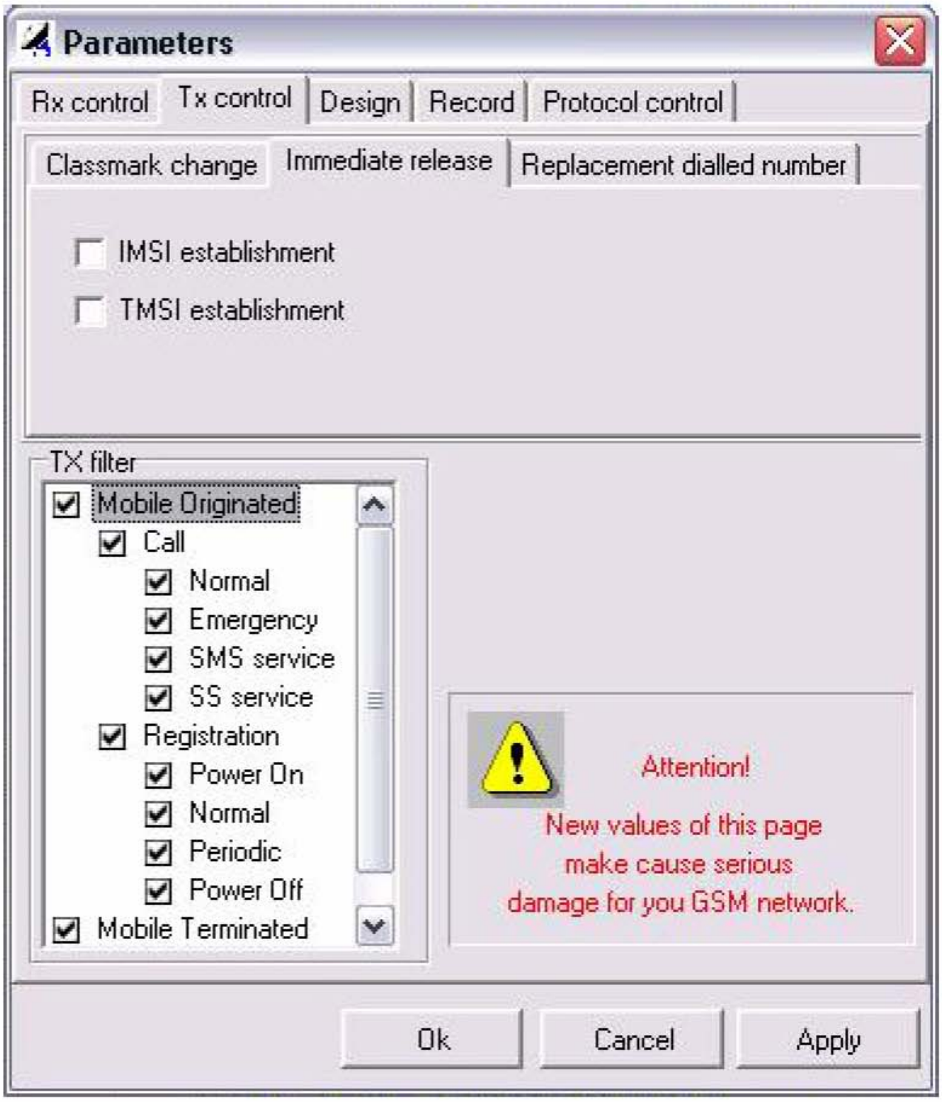
- ☑ Mobile Originated
  - ☑ Call
    - ☑ Normal
    - □ Emergency
    - ☑ SMS service
    - □ SS service
  - ☑ Registration
    - ☑ Power On
    - ☑ Normal
    - ☑ Periodic
    - ☑ Power Off
- ☑ Mobile Terminated

Attention!

New values of this page make cause serious damage for you GSM network.

In this registering card A5/1 and A5/2 algorithm support can be disable.

5.2.2. Immediate release



□ IMSI establishment

□ TMSI establishment

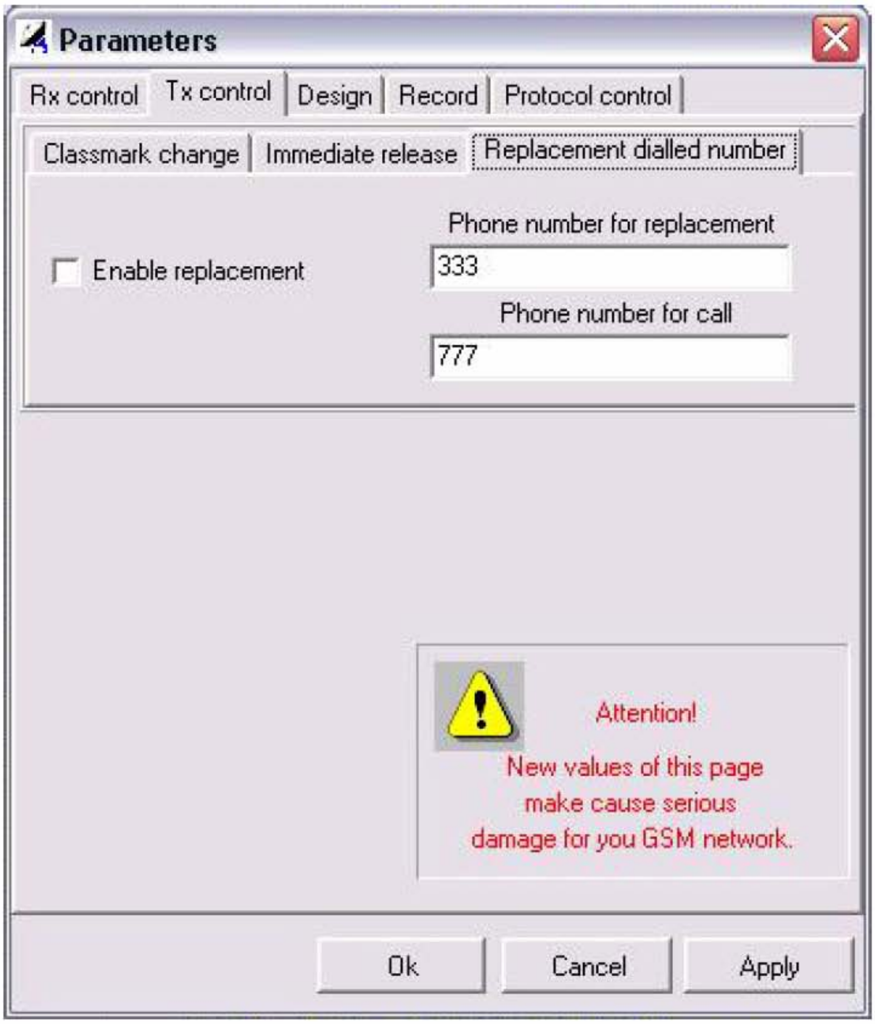
- ☑ Mobile Originated
  - ☑ Call
    - ☑ Normal
    - ☑ Emergency
    - ☑ SMS service
    - ☑ SS service
  - ☑ Registration
    - ☑ Power On
    - ☑ Normal
    - ☑ Periodic
    - ☑ Power Off
- ☑ Mobile Terminated

Attention!

New values of this page make cause serious damage for you GSM network.

In this registering card TMSI and IMSI establishment can be activated.

5.2.3. Replacement dialed number



□ Enable replacement

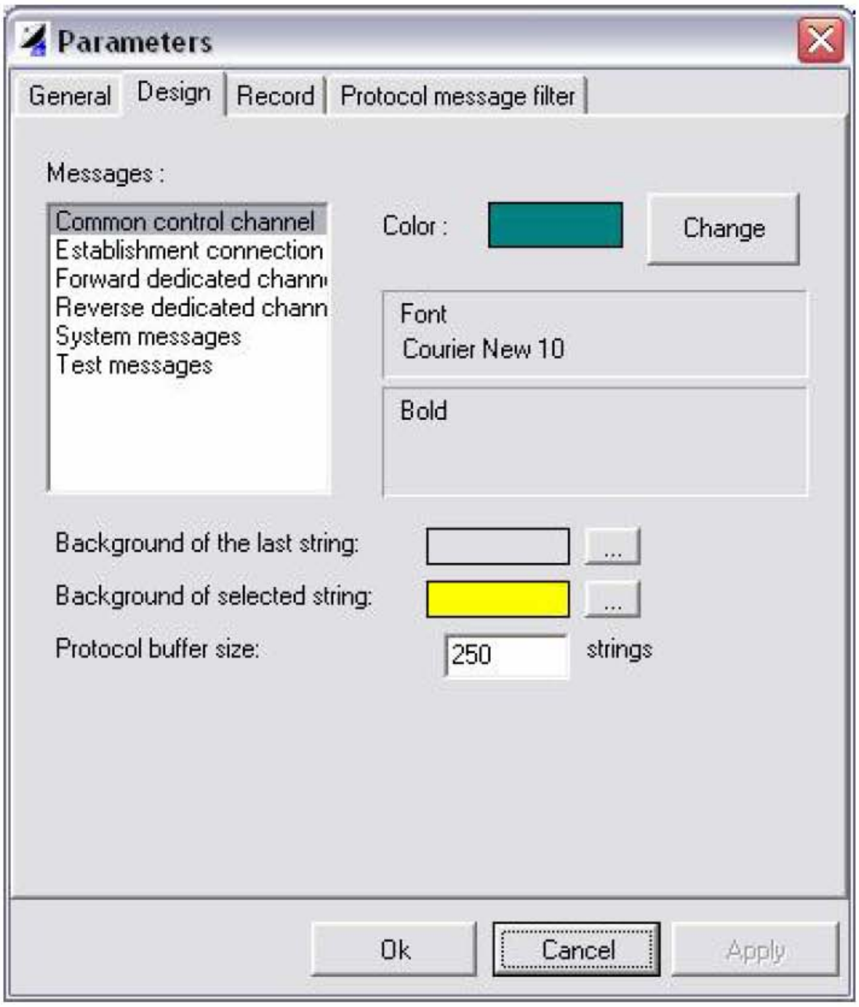
Phone number for replacement: 333

Phone number for call: 777

Attention!
New values of this page make cause serious damage for you GSM network.

- Phone Number for Replacement: - the phone number to be diverted is typed in here
- Phone Number for Call: - aim number is typed here

5.3. Design



Messages :

- Common control channel
- Establishment connection
- Forward dedicated chann
- Reverse dedicated chann
- System messages
- Test messages

Color :

Font
Courier New 10

Bold

Background of the last string:

Background of selected string:

Protocol buffer size: 250 strings

The display attributes of the different messages in the protocol window are set/adjusted in this dialog window.

- Nomination
- Size
- Type
- Attributes
- Colour of Writing
- Protocol buffer size

Background of the last string:

Background colour of the last string

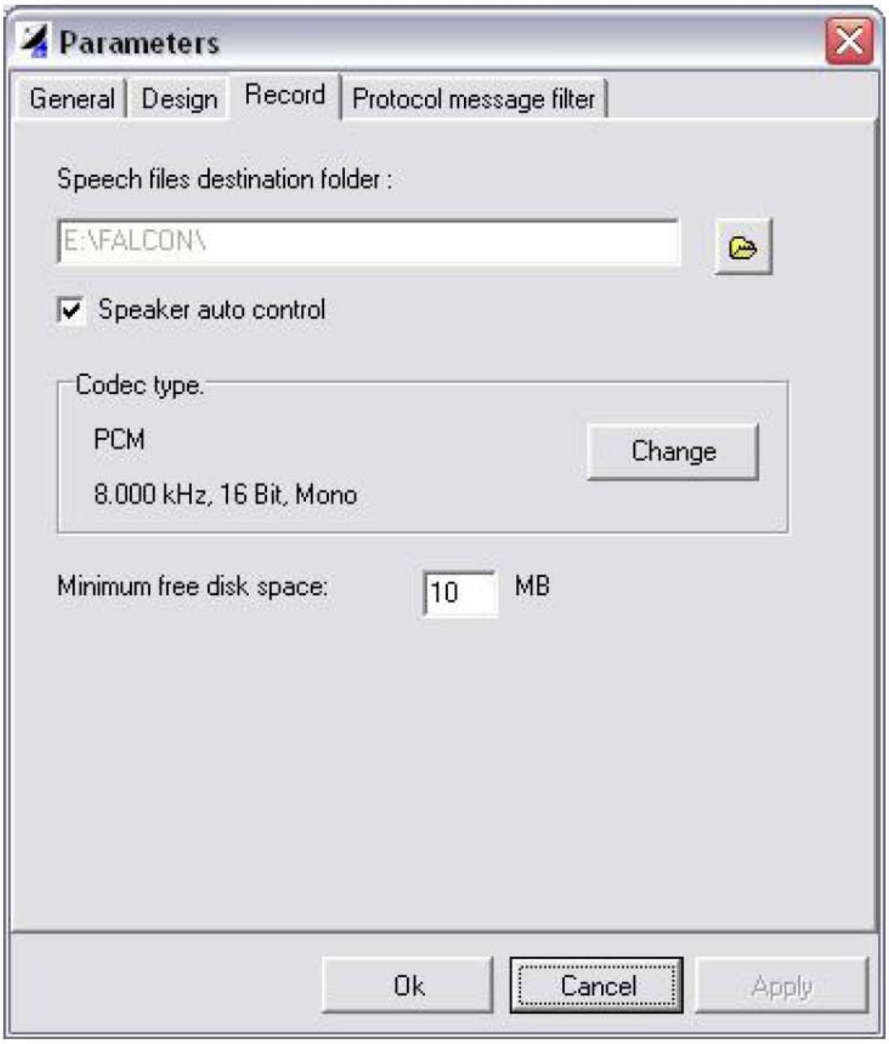
Background of selected string:

Background colour of the selected string

Protocol buffer size: 250 strings

Protocol buffer size. A size of 250 should be set. Higher values lead to slower operation of the FALCON.

5.4. Record



Speech files destination folder : E:\FALCON\

☑ Speaker auto control

Codec type: PCM 8.000 kHz, 16 Bit, Mono

Minimum free disk space: 10 MB

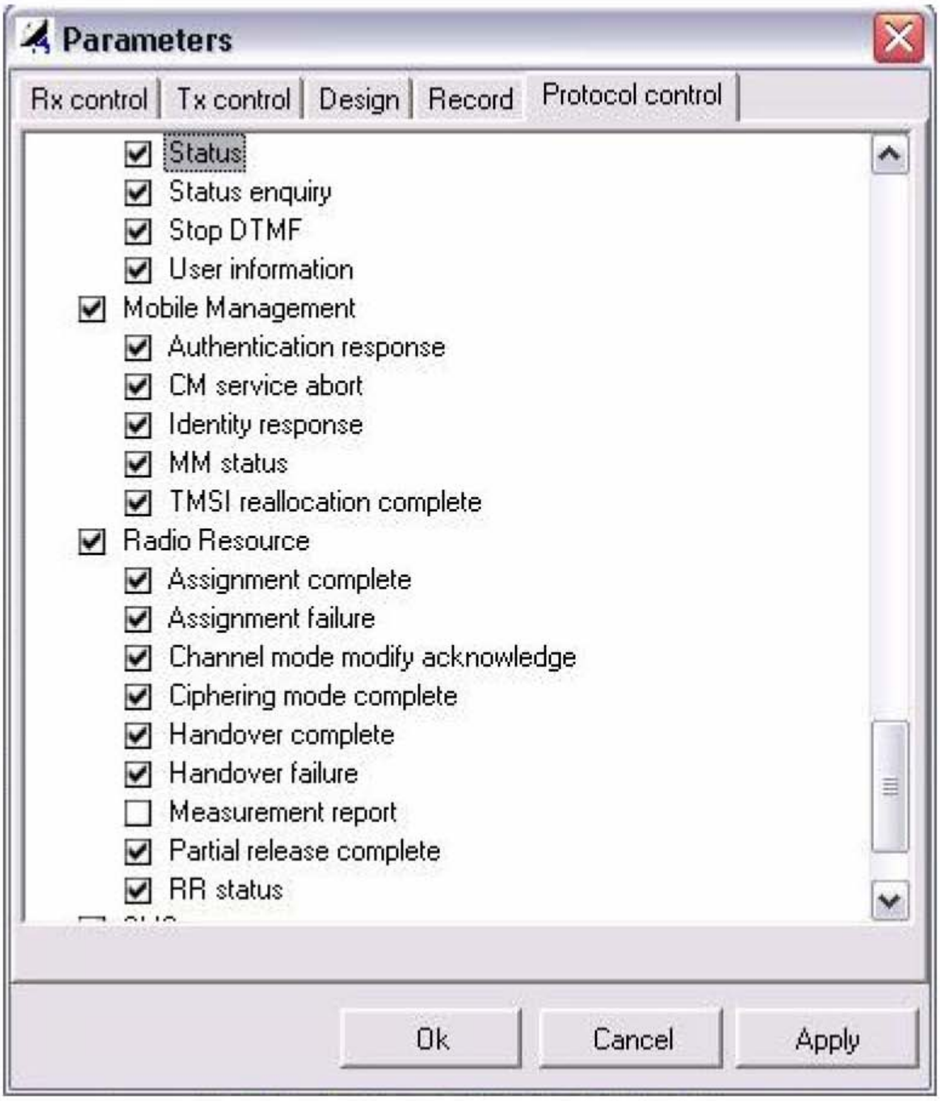
The following parameters can be entered and set for the 4 channel recorder and each of the audio recordings in this dialog window:

- *Speech files* – designation of the folder in which the audio recording will take place
- Speaker auto control – if this function is activated, playing of the audio information on the computer (Notebook) is taking place in parallel to the recording
- *Codec type* – the required recording format (frequency and data format) for the audio information can be set.

> It is recommended to use the setting 8000KHz, 16bit, mono.

- *Minimum free disk space* – setting for how much disk space should remain as reserve on the main disk of the computer (Notebook). Once this minimum space is reached, no further storage of audio data is taking place.

5.5. Protocol control



- ☑ Status
- ☑ Status enquiry
- ☑ Stop DTMF
- ☑ User information

☑ Mobile Management
- ☑ Authentication response
- ☑ CM service abort
- ☑ Identity response
- ☑ MM status
- ☑ TMSI reallocation complete

☑ Radio Resource
- ☑ Assignment complete
- ☑ Assignment failure
- ☑ Channel mode modify acknowledge
- ☑ Ciphering mode complete
- ☑ Handover complete
- ☑ Handover failure
- □ Measurement report
- ☑ Partial release complete
- ☑ RR status

In this dialog window, the operator undertakes settings that are necessary to fulfil the monitoring task. In order not to strain the protocol window and not to make it too confusing, only the most necessary information should be displayed. Every additional detail to be displayed slows down the operation of the FALCON.

5.5.1. Parameters of Choice

1. *Comman Control Channel Messages* – Messages in the general control channel.
   1.1. *Call* – Search for a subscriber in the network. The message is sent in the Paging Channel and can contain the identification of 1-5 subscribers.
   1.2. *Immediate Assignment* – Request of the network to the mobile phone to establish a connection. The parameters for the dedicated channel for the conversation are transferred (TDMA, Slot and information about Hopping).
2. *Establishment Connection* – Group of commands to establish the connection.
3. *Dedicated channel* – Command to dedicate the channels.

- 3.1. *Mobile Management (MM)* – Commands to continue to maintain the mobility of the mobile phone; Message about the current location.
- 3.2. *Call Control (CC)* – Commands to establish a connection between two subscribers. Each connection has its own number.
- 3.3. *Radio Resource (RR)* – Commands through the channels, through the organisation of the exchange of data.
- 3.4. *Supplementary Service (SS)* – Commands to use services provided by the network operator.
- 3.5. *Short Message Service (SMS)* – Commands for the exchange of short messages.

4. *Reverse Dedicated Channel* – Commands for the dedicated reverse channel (Uplink).
   - 4.1. *Mobile Management (MM)* – same contents as 3.1.
   - 4.2. *Call Control (CC)* – same contents as 3.2.
   - 4.3. *Radio Resources (RR)* – same contents as 3.3
   - 4.4. *Supplementary Service (SS)* – same contents as 3.4.
   - 4.5. *Short Message Service (SMS)* – same contents as 3.5.
5. *System Messages* – System messages in the GSM-network.
6. *Test Messages*

The operator gets to this dialog window through the main menu “SETS”, item “Recorder Sets” and the tool button .

6. Additional Information to GSM-Network

6.1. General

In the GSM Standard the

- IMSI – International Mobile Subscriber Identity
- TMSI – Temporary Mobile Subscriber Identity

are transmitted through the air in the GSM-network. The subscriber is identified within the GSM-network through these numbers.
To monitor the conversation of a subscriber, it is necessary to have/obtain the IMSI or the TMSI.

With the FALCON-Mobile, a specially modified mobile phone that can be delivered as an option with the FALCON system, it is possible to obtain the IMSI or the TMSI of a subscriber to be monitored.

6.2. Details for IMSI

The IMSI is a subscriber number for the use of GSM-networks, which is unique, being handed out only once worldwide for identification. This IMSI contains the code VCC and MNC (Mobile Network Code). The IMSI is stored on the SIM-Card and cannot be changed. In parallel, the IMSI is filed with the Network Operator in the HLR (Home Location Register). In case the subscriber does not use his mobile phone in the own country GSM-network, this means he is in Roaming, then the IMSI will be filed in the VLR (Visitor Location Register).
The IMSI consists of a 15-digit combination of numbers, whereas the first 3 digits show the MCC (Mobile Country Code), and the 2 following digits show the MNC (Mobile Network Code). The remaining 10 digits make up a fixed code for the subscriber in the GSM-network.

6.3. Details for TMSI

The TMSI consists of a letter/number combination that does not carry a particular content. The TMSI is also filed in the HLR and VLR. The change of the TMSI in the GSM-network is carried out on the basis of the procedure "TMSI Reallocation" or by change of location of the mobile phone "Location Updating".

6.3.1. Main methods of changing the TMSI by the Network Operator

The TMSI can be changed by the network operator during:

- every new connection establishment, independent of whether it is an incoming or an outgoing call (TMSI Reallocation)
- changing of the TMSI during the procedure 'Location Updating'. The change can come into effect periodically or after hours/weeks.
- Periodic change of the TMSI during the procedure 'TMSI Reallocation' and/or 'Location Updating'.

6.4. Messages in the Control Channel of the base station (CCCH)

The exchange of control signals and signals of synchronisation take place in the CCCH. This channel is the general channel for all mobile phones in the radio cell of the base station. The mobile phone can hence only occupy this channel for a very short period of time, in order to clarify with the network, on which other dedicated channel the conversation can take place. Due to this, the commands in the CCCH are very short:

1. Call – The network searches the radio cell, in which the subscriber can be reached. This message is sent in the paging channel.

2. Immediate assignment – the network instructs the mobile phone to establish a connection. Every establishment of connection in the network starts with this command. The dedicated channel (ARFCN) as well as the TDMA-Slot or the information for organisation of frequency hopping is displayed. As parameter for the time synchronisation, the distance between the base station and mobile phone is used. For the transmission of this parameter the AGCH (Access Grant Channel) is used.

6.5. Message for establishment of connection between mobile phone and base station (Establishment Connection)

1. The following commands can be transferred /transmitted during establishment of a connection:
2. Call Establishment – Call of a mobile phone with display of identification of the subscriber and the type of phone he is using (Mobile Station Classmark)
3. Emergency Establishment – Emergency call on the emergency phone numbers (e.g. 999), Identification of the subscriber and the type of phone he is using (Mobile Station Classmark)
4. SMS Establishment – SMS sent from the mobile phone; identification of the subscriber (IMSI or TMSI) and the Mobile Station Classmark
5. SS Establishment – connection for the provision of services by the provider (call divert, blocking of incoming calls etc.)
6. Registration – Commands for registration of the mobile phone in the network. Upon request of the network, the mobile phone transmits the IMSI of the subscriber.
7. Power On Registration – registration of the mobile phone within the network when it is switched on
8. Normal Registration - normal registration of the mobile phone within the network
9. Periodic Registration – periodic registration of the mobile phone within the network
10. Power Off registration – registration of the mobile phone within the network when it is switched off
11. Paging response – the mobile phone informs the network of its presence within the network
12. IMSI Detach Indication – the mobile phone informs the network when the service is no longer required e.g. when the SIM Card is changed without switching the mobile phone off.

6.6. Messages in the Dedicated Channel

The following messages can be displayed in the up and down link:

1. Radio Resource – Group of commands like for example channels, organisation of the data transfer in the general channels
2. Additional Assignment – with this command a further channel is dedicated for a second subscriber
3. Assignment Command – this command describes the configuration of the new traffic channel, if the currently used channel shall be changed.
4. Start Ciphering – this command enables/starts the encryption of the channel and the mobile phone must also switch on the encryption module. The type of encryption is displayed
5. Handover Command – this command instructs the mobile phone to switch to the dedicated channel (traffic channel). The dedicated channel and the TDMA-Slot, and possibly also the starting of hopping is displayed
6. Physical Information – the mobile phone receives this command to stop the data transfer in the dedicated channel
7. Channel Release – this command enforces the return / release of the dedicated channel
8. Paging Request – command of the base station to the mobile phone for search and identification of IMSI, TMSI

9. Classmark Enquiry – Command to the mobile phone to provide/send the classmark parameters
10. Short Messaging Service – command to send SMS. The transfer takes place through UNICODE in Latin letters.

The Falcon System can also decode SMS in other types of letters/formats if these types are installed on the computer (laptop)

1. Call Control (CC) – command for call control
2. Release – command to cut the connection, return of the channel
3. Location Updating Request – Message of the mobile phone to the network to inform of change of location
4. Authentication Request – command of the network to the mobile phone to provide authentication: use of KI and of A3 Algorithm
5. TMSI Reallocation Command- command of the network to the mobile phone with regard to switching off or changing or changing of the TMSI

7. Technical Data

	GSM 900	GSM 1800
Reception channels	8 (4 Duplex channels)	
Target numbers	up to 1000	
Identification	through IMSI, TMSI, IMEI, Classmark, Telephone number, Distance	
Frequency range of Downlink (BTS→MS)	935 ... 960 MHz	1805 ... 1880 MHz
Frequency range of Uplink (MS→BTS)	890 ... 915 MHz	1710 ... 1785 MHz
Channel spacing	200 kHz	
Number of channel	124	375
Frequency deviation	45 MHz	95 MHz
Frequency stability	± 0,03 ppm	
Receiver type	double-super heterodyne, asynchrony	
Receiver sensitivity	-105 dbm	
Antenna impedance	50 Ω	
Time of frequency change in Hopping mode	< 500 µs	
Dynamics range	> 75dB	
Volume range	25 dB	
Demodulator	GMSK, asynchrony	
Speech codex	RPE/LTP: FR, EFR	
Channel structure	TDMA/FDMA	
System software	Windows 98/2000	
Audio format	standard Wave-format	
Power supply	220 VAC, 50 Hz; 110 VAC, 60 Hz or external battery 12 V DC	
Operating temperature range	+ 5 °C ... 40 °C -20 °C ... + 50 °C (without condensation)	

Model No: 580 200 0001

8. Scope of delivery

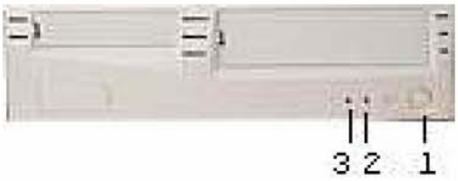
- Main unit *FALCON*
- Control unit (Notebook)
- USB-connecting cable
- Power supply cable 230VAC
- Power supply cable12 VDC
- 2 pcs. Dual-band antenna (magnetic mount)
- User manual
- Transport case

option:

- FALCON mobile
- Mobile telephone with software “NETMON
- Dualband-Yagi-antenna
- Module for remote control via LAN, PSTN, ISDN

9. Appendix

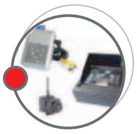
9.1. Frontsite



pic. 1: Frontsite

1	Power On/off
2	LED On/Off
3	LED Power

GOVERNMENTAL SECURITY SOLUTIONS



If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de