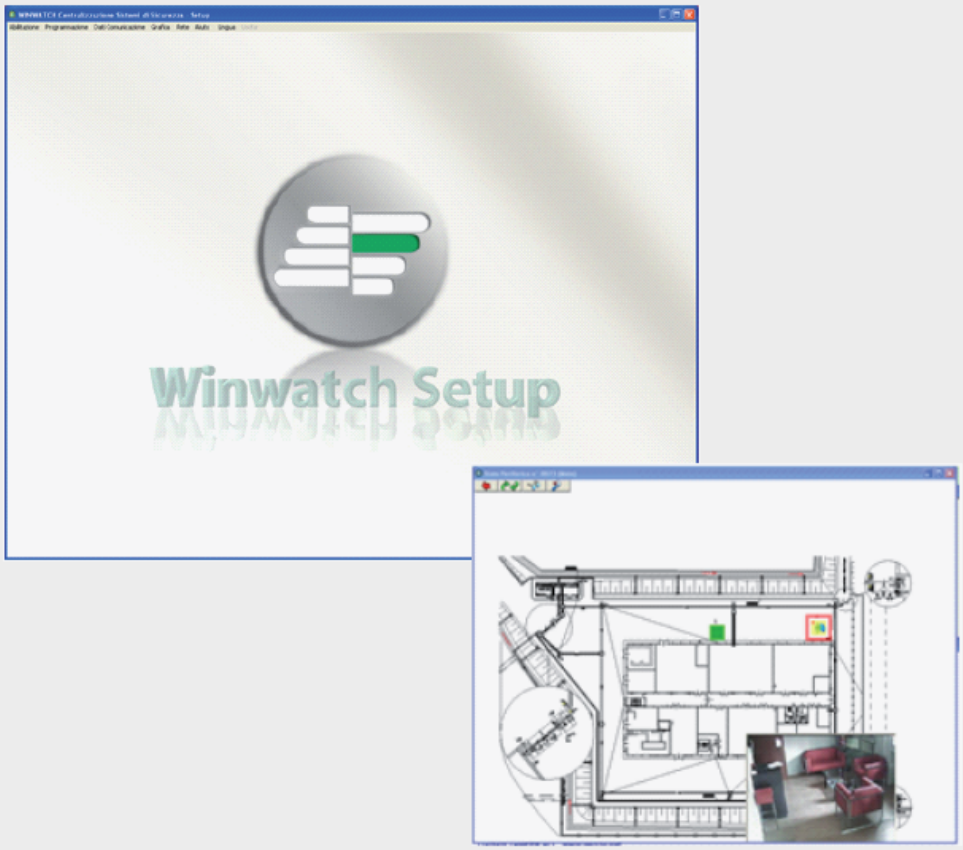
TELEDATA

WINWATCH Supervision Software

for Fire Alarm & Burglar Alarm & CCTV Stations



INSTALLATION & OPERATION **MANUAL**

Rev. 2 / 2012

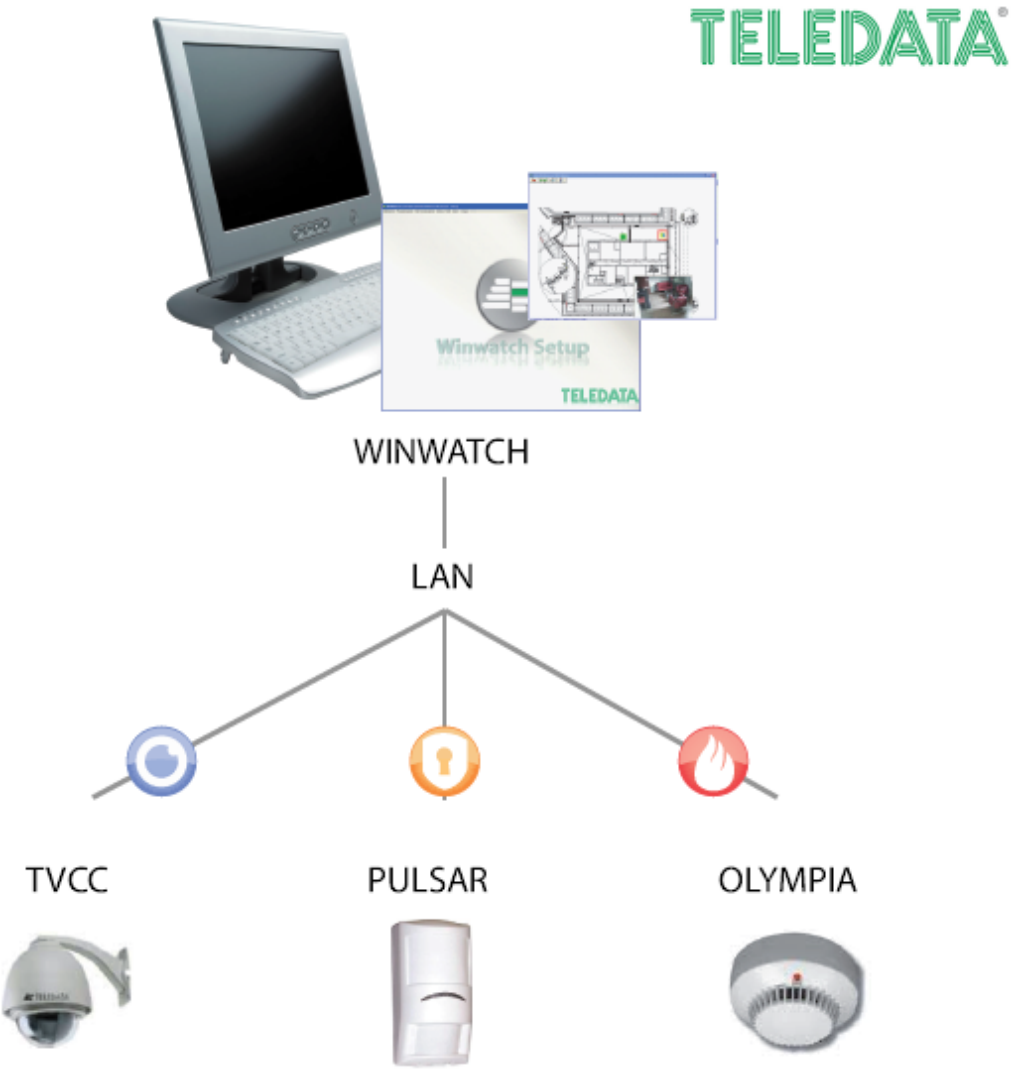
INDEX

1. Introduction

1.1 The Winwatch system

1.1.1 General

The Winwatch software, designed to run in a Windows environment (XP, 2000, Vista, Seven), supervises *Teledata*'s fire alarm and burglar alarm control untis through a remote computer (server). Moreover, the software can: manage *Teledata* CCTV stations starting from a remote location, can be integrated with the software *Serchio* for managing the *Teledata* access control control units, and to be interfaced to all burglar alarm and access control stations via the CEI ABI 79/5 79/6 protocol. All the system can be managed by active multilevel graphical maps.



The *Winwatch* control stations potentiality allows a remote vision of environments where security, safety, reliability and flexibility of the control system becomes fundamental, like important airport and banks centre.

1.1.2 Minimum system requirements

For a better functionality of the software *Winwatch,* there are suggested three different types of minimum configurations depending on the complexity of the system.

- With the minimum configuration, it will be possible to manage fire and burglar control units, without graphical maps and DVR or NVR management.
- With the medium configuration, it will be possible to manage fire and burglar control units, graphical maps and DVR management, but no NVR.
- With the maximum configuration, it will be possible to manage fire and burglar control units, graphical maps and DVR/NVR management.

Component	Minimum	Medium	Maximum
Processor	2Ghz single core	2Ghz dual core	3Ghz quad core
RAM	512Mb	1/2Gb	2/4Gb
Hard Disk	40Gb	100Gb	200Gb
Video card	1 monitor output	2/3 monitor outputs	3 monitor outputs
Operative system	Windows XP	Windows XP/7 32bit	Windows 7 64bit
LAN card	10/100Mb	10/100Mb	100/1000Mb
Connected units	16	32	64+

The suggested configurations are not mandatory. It is suggested to evaluate the computer performances depending on the complexity of the system. For more details please contact *Teledata*'s technical assistance.

1.1.3 Control stations supported

The following control units can be monitored directly by the Winwatch system without a further need of software customization:

- All *Teledata* burglar alarm control units (*Pulsar*, *Minipulsar, Sentinel, Sirius, Argo*…);
- All *Teledata* CCTV digital video recorders (*Phantom*, *Videospy*, *Stargate*, *Nettuno, SteelEye, NetEye*…);
- IP Cameras *Teledata, ACTI* and *ONVIF*
- Videoservers *Teledata* e *ONVIF*
- *Vicon* and *Comerson* CCTV video recorders;
- All *Teledata* fire alarm control units (*Eolo*, *Olympia* with *OlyNet* management);
- *Notifier* fire alarm stations (models AM6000 and AM2000).
- Universal field interface *Teledata* (*Minipulsar/U*)

Through possible software customizations, the *Winwatch* system can support other models of burglar alarm, fire alarm and CCTV control units, on condition that:

- the control unit is prepared to be managed remotely;
- it is possible to interfaced to the control unit via RS232 / RS485 /LAN;
- the protocol used by its manufacturer can be accessed.

1.1.4 Communication line between central units and monitoring station

The communication between the monitoring station and the central units monitored by the *Winwatch* system can take place through one or more of the following links:

LAN network

It is the optimum solution for almost all control units: it requires installation of a network hub or switch; but it is universal, fast, and it can be easily integrated.

Dedicated serial line (RS485 / RS232).

In general, it is installed on low-cost lines only, for economic reasons. Remote control of the control units is managed according to the *polling-select* principle.

If the system includes a high number of devices, it is recommended to subdivide them into several loops (up to 30-40 devices per loop), and to use the multi- serial ports (with possibility to manage up to 8 serial ports).

As this communication line is not fast, this line is not suitable for video applications.

Switched Line (PSTN / GSM).

Because of the low communication speed and of the cost of the call, it is strongly not recommended to use the switched line as main line, unless you are using it for particularly simple applications.

If the switched line is used as a backup line, the communication occurs only in case of malfunction of the main line.

1.1.5 Server, client and backup management

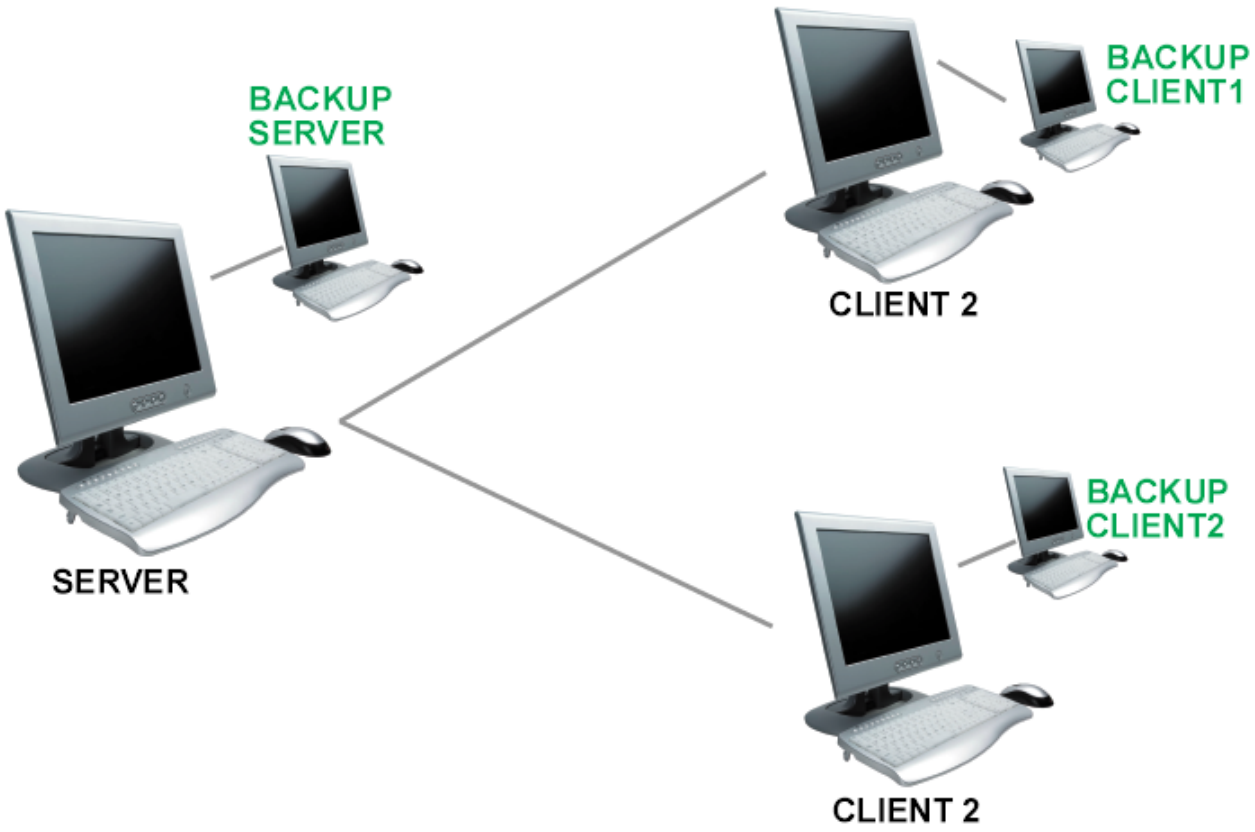
The *Winwatch* system can be centralized on a single server PC, to which up to 40 client PCs can be connected for managing the system with the same performance as the server.

A second PC, configured as a server, can be connected to the server PC. That will automatically take its place in case of bad functionality (hot back-up) to restore the connection with the field.

Also to each client unit it is possible to connect a backup unit, which will be activated only if the main unit fails.

The following figure is an example of a monitoring system consisting of a server and two clients, each provided with a backup PC which takes over if the PC that it is connected to has a bad functionality.

It is necessary that all the PCs are connected via LAN and that the server shares with everybody the folder where the software *Winwatch* is installed..



1.1.6 Multi-monitor management

The software *Winwatch*, is able to manage simultaneously up to 3 monitor connected to a single PC, that become 4 in case of installation of another *Teledata* software pack dedicates for access control, *Serchio,*.

To make the most of a multi monitor system it is necessary to install inside the PC a grahic card with more than one independent output. In case of 2/3 monitor configuration, it is possible to use USB/VGA converter. In case of a maximum configuration with 4 monitors, it is necessary to use QUAD video cards such a: *Matrox Millennium G200*

The different configuration are shown below, from the minimum to the maximum:

Minimum configuration with two monitors

1) Main monitor on the left: management of the log events and communication status.
2) Second monitor on the right: graphical maps management or eventual *Serchio* software pack.

1) Main monitor on the right: management of the log events and communication status.
2) Second monitor on the left: video camera realtime and playback management.

Suggested configuration with three monitors

1) Main monitor in the middle: management of the log events and communication status.
2) Second monitor on the left: camera realtime and playback management
3) Third monitor on the right: graphical maps management or eventual Serchio software pack.

Maximum configuration with four monitors

4) Main monitor in the middle: management of the log events and communication status.
5) Second monitor on the left: camera realtime and playback management
6) Third monitor on the right: graphical maps management
1) Fourth monitor: *Serchio* software management.

1.1.7 Protection through password

The *Winwatch* software allows creating different user profiles, each of which is enabled to modify only some sorts of parameters and to call only given functions.

A different password is assigned to every user, and will be able to modify the authorizations / restrictions of lower-level users.

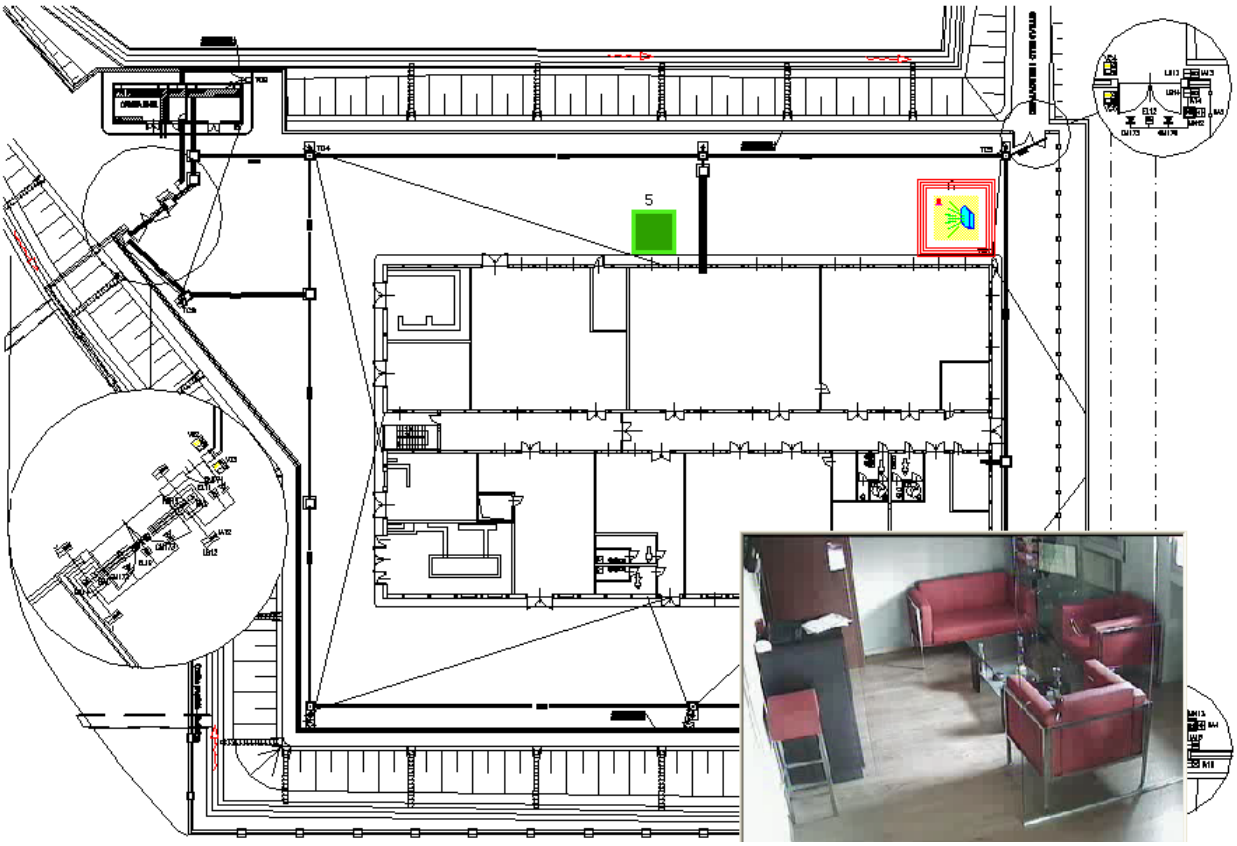
In this way, different user classes are established, that can execute specific operations, without the risk of less skilled users handling particular commands or functions.

1.1.8 Software interface

A multi-level mapping system allows identifying the location of the control units, of the geographic areas or group of devices (one for each control unit) and of the peripheral devices (for each geographic area / group of devices).

The sensors are identified graphically, depending on their type. A short phrase can be associated to each of them to describe their function.

The system is able to display in real time up to 16 graphical maps of the total of control units configured.



1.2 About this manual

1.2.1 Symbols used

The notes shown with this symbol (image on the side) are suggestions for a better use of the software, or advices for a proper programming of the control unit.

The warnings shown with the symbol (image on the side) are importante for correct use of the software. You must keep to them with the greatest care.

1.2.2 Organization of the contents

The manual is composed of different sections, each of which can be called from the list of contents of the document, in PDF version. Every section covers a different aspect of a system based on *Winwatch* software.

The various sections contain hypertext references (active in the PDF version) which allow switching from subject to other correlated subjects. These references are always expressed in **reference** paragraph form.

The manual doesn't cover all programming aspects of the control units. For more information or clarifications, please refer to the instruction manual of the control unit that you are programming.

1.2.3 Manual compatibility

For the compatibility between this manual and the software version installed, please check out the following table.

Manual	Software Version	
Rev. 0	Before	v.12.0.0.22
Rev. 1	From	v.12.0.0.26
Rev. 2	From	v.12.0.0.35

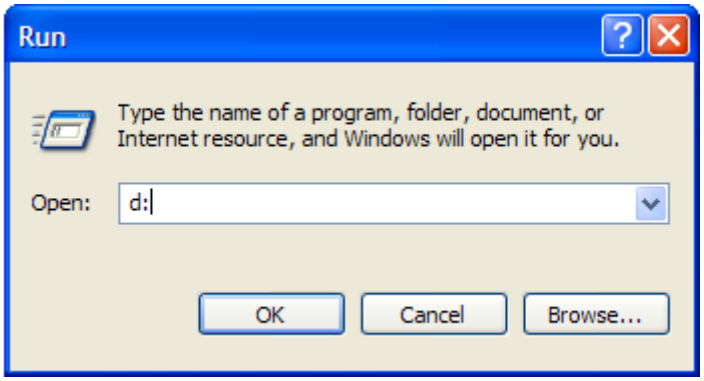
It is suggested to verify that the version of the *Winwatch* software installed is updated, so that it is possible to be compatible with all the functions described in the manual.

2. Installing the software

2.1 Procedure

Installation of the *Winwatch* and *Winwatch Setup* softwares occurs simultaneously. Please refer to the following procedure:

- Insert the CD which is delivered as outfit with the software in the CD reader of the computer where you wish to install the software.
- Open the “resource management” application, and display the CD content.



- Run the *Setup* application.
- Follow the instructions contained in the dialogue windows that succeed until installation is completed.
- Install all the requested extra software packs, confirming all the default parameters.
- Restart the computer.

2.2 Conclusion

At the end of the procedure, the system will have the following software items installed:

- *Winwatch Setup* for the system configuration;
- *Winwatch* for the monitoring of the system.

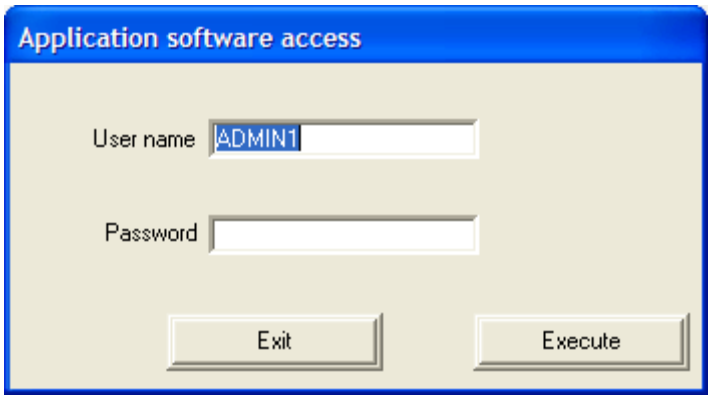
3. Configuring the communication system

Starting from this section, the manual explains how to use the *Winwatch Setup* and *Winwatch* software. Refer to this manual for any doubt or clarification.

It is not possible to anticipate all the software's malfunctions and the consequences resulting from wrong settings. The software has to be used by experienced personnel, informed on the potentials and functions of the system components that is going to be programmed.

3.1 Starting Winwatch Setup

From the operating system applications' menu, start the *Winwatch setup* application from: *Start → Programs → Teledata Security → Setup*.



Click on *Entrance* (figure above) and enter the user name and password in the window that has appeared on the screen (figure on side). The user names and passwords which are set by default in the system are :

- user name: *ADMIN1*
  password: *ADMIN1*
- user name: *ADMIN2*
  password: *ADMIN2*

Press key **Execute**.

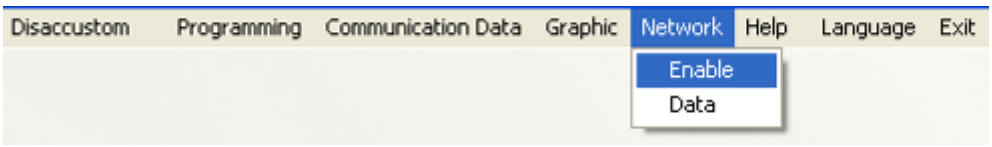
To change the password or add more users with different access levels and different passwords, refer to paragraph 12.2.

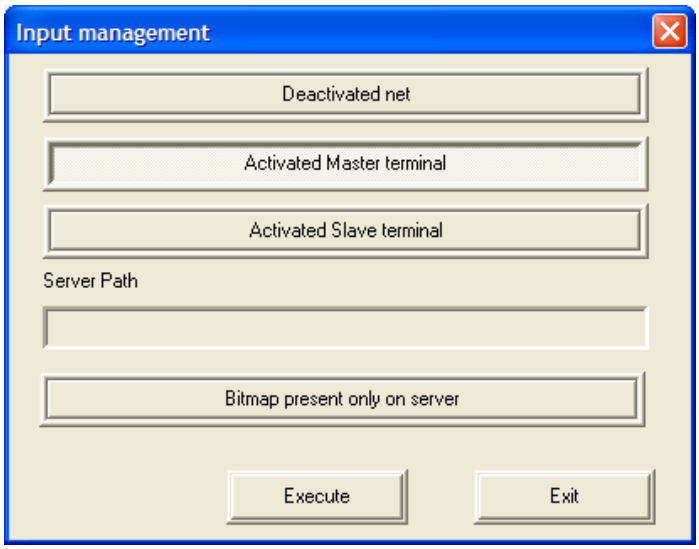
To close the *Winwatch Setup* application and return to the operating system, select *Exit* at top right.

3.2 Enabling and configuring the LAN network

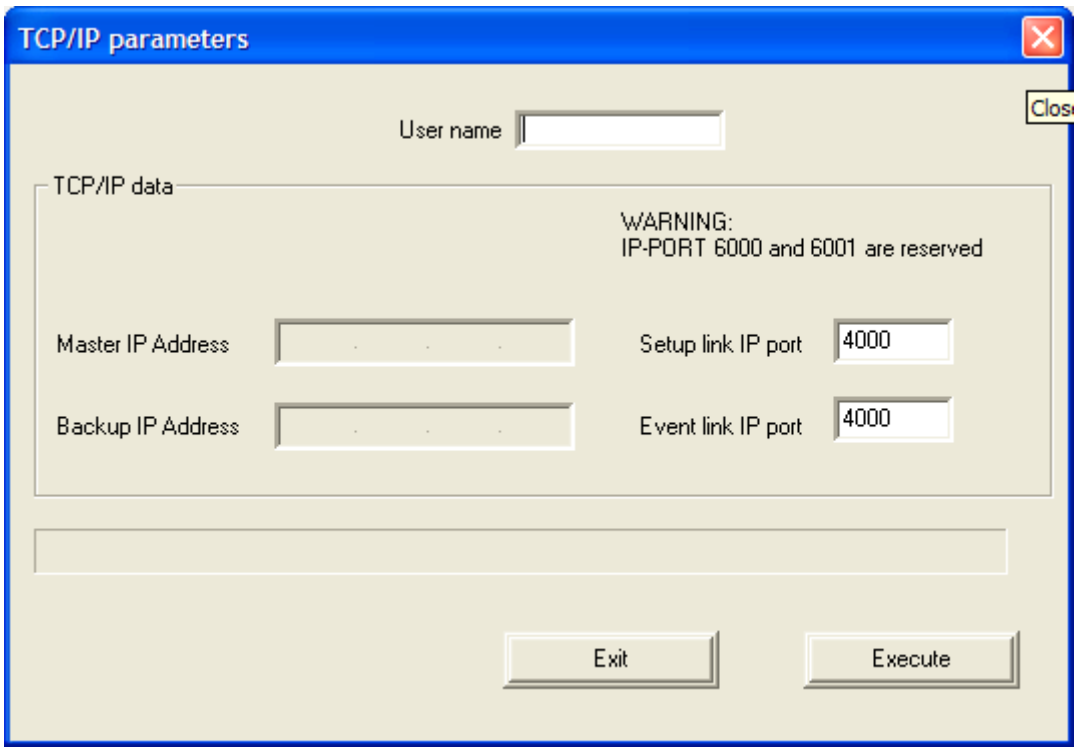
If a LAN network is used to communicate between the monitoring station and the control units, make sure that the network is enabled correctly.

Click on *Network* → *Enable*.





- Press **Deactivated net**, if you are configuring a monitoring system made of only a concentrator PC, without client stations.
- Press **Activated Master Terminal**, if you are configuring a server station. In this case it is necessary to share the root directory with read/write possibility..*Winwatch32* with the client stations
- Press **Activated Slave Terminal**, if you are configuring a client station. In the window that appears on the screen, select the *Winwatch.exe* file located in the shared f on the Master PC (following figure).



Also check the status of the last button:

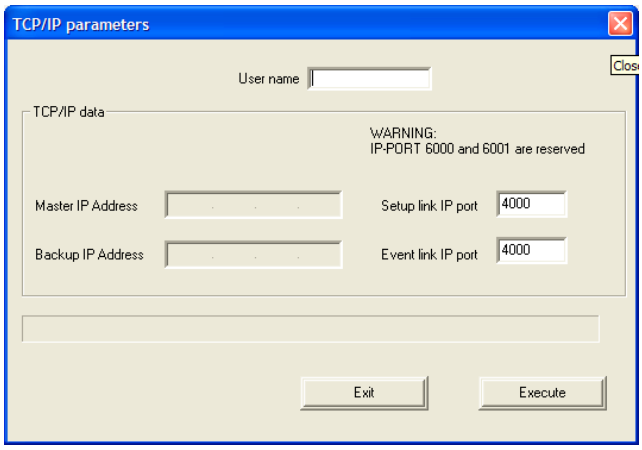
- If released (*Bitmaps present on the server only*), it is possible to display the maps on the server station only and not on the client stations connected to it.
- If pressed (*Bitmaps present on clients too*), it is possible to manage the maps on the server and on the client connected to it.

It makes sense to deactivate the function only if you don't have the necessary licence to activate the maps on all the terminals.

Press key **Execute** to close the window and save the settings; press **Exit** to quit without saving.

3.2.1 Setting the LAN network parameters

Click on *Network* → *Data* and set the parameters as follows:



- Insert in the field *User name* the name of the system that will be viewed in the peripheral tree of *Winwatch32* (free field);
- If the station in use is a server, insert in the field *Setup link IP port* the first IP port used to acquire data from the network.
- Insert in field *Event link IP port* the last port for data acquisition, according to the following scheme:
  - If NO client type stations are connected to the station in use, enter the same value as is set in field *Setup link IP port*.
  - If one or more client type stations are connected to the station in use, enter the result of formula **IP + 2*N-1** where IP is the value as set for parameter *Setup link IP port* and N is the number of connected clients.

For example, if you set *Setup link IP port* = 4000 and = *Event link IP port* = 4005, the quantity of connected servers is 3. In fact: 4005 = 4000 + 2*3 -1.

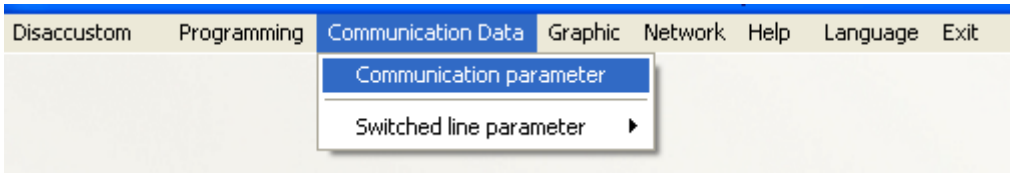
- If the station in use is a client type, insert the IP address of the server in the field *Master IP Address.*
- Insert in the field *Setup link IP port* the first available port of the server, and in the field *Event link IP port* insert the same address as *Setup link IP port* increased by 1.

If in the system there is more than one client station, it is necessary to have unique ports per client. Following the example shown before, the second client will have *Setup link IP port* set at 4002 and *Event link IP port* at 4003, and so on.

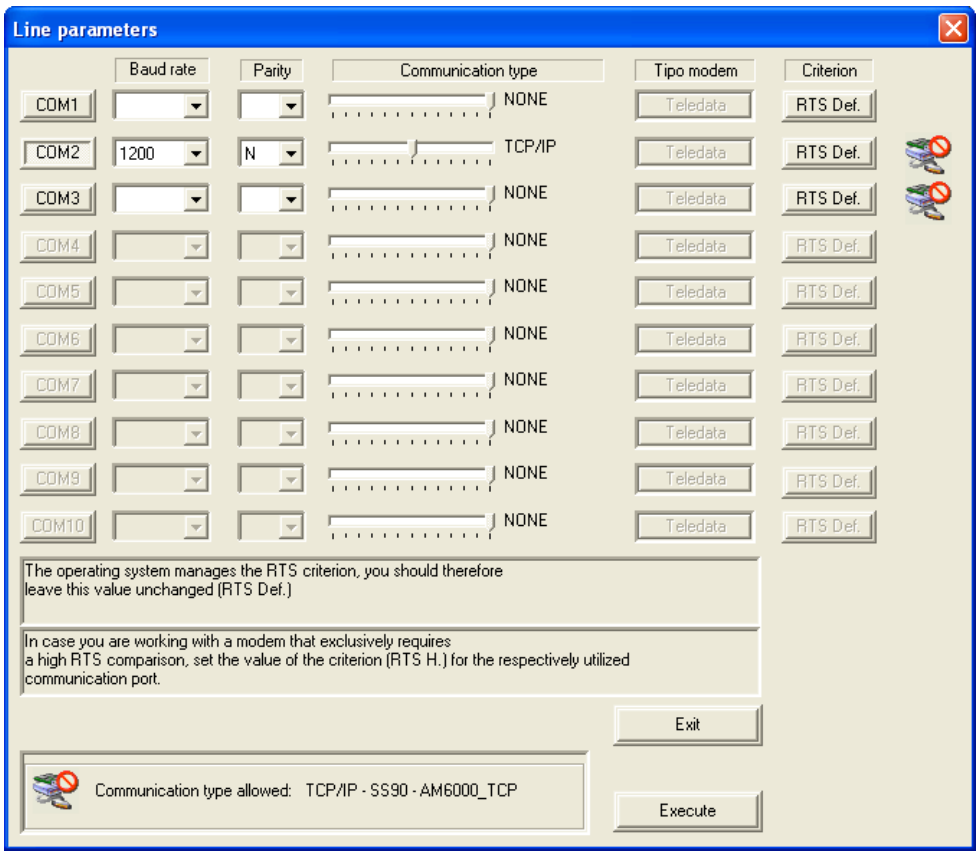
- If there is a backup computer connected to the used station, insert it's IP address in the field *Backup IP Address*;

3.3 Setting the communication lines

Select *Communication data* → *Communication parameter*.



A window, as in the following figure, pops up.



Press the buttons on the left side (COM1…10) to enable a new communication link. Up to 10 different communication links can be enabled.

To set the parameters, please refer to the following paragraphs:

- For *Teledata* control units, paragraph **3.3.1**;
- For *Notifier* control units, paragraph **3.3.2**;
- For other lines, paragraph **3.3.3**.

Once the settings are entered, press key **Execute** to close the window and save the set-points; press **Exit** to quit without saving.

3.3.1 Teledata control units

If *Teledata* control units are going to be monitored, for each communication line you should set the *Baud rate* that is set in the unit, *Parity* to N, and select the type of line:

- *Dedicated*: RS232 or RS485 serial line;
- *Switched*: Analogue line (PSTN);
- *TCP/IP*: LAN network (in this case, ignore the field *Baud rate*).

3.3.2 Notifier control units

If *Notifier* control units are going to be monitored, for each communication line you should set *Baud rate* to 9600, *Parity* to E, and select the type of line between the following:

- *AM600*: RS232 serial link;
- *TCP/IP AM600*: LAN network (in this case, ignore the field *Baud rate*).

3.3.3 Other links

To set any of the following communication line, please ask *Teledata*'s technical support.

- *TVCC COM.*: *Comerson* CCTV video recorder;
- *TVCC VIC.*: *Vicon* CCTV video recorder;
- *IDEFIX(COMM.)*: *Teledata Idefix* burglar alarm control unit (obsolete);
- *TD183*: *Teledata*'s I/O board (obsolete).

The *SS90* and *VIRTUAL CAN.* communication linke are obsolete and are no longer supported by *Teledata*.

3.4 Modem configuration

3.4.1 Modem type and RTS criteria

If you select the switched line, in the *Communication data* → *Communication parameters* window it will be necessary to select, in column *Modem Type*, if a *Teledata* modem or a third-party modem is being used.

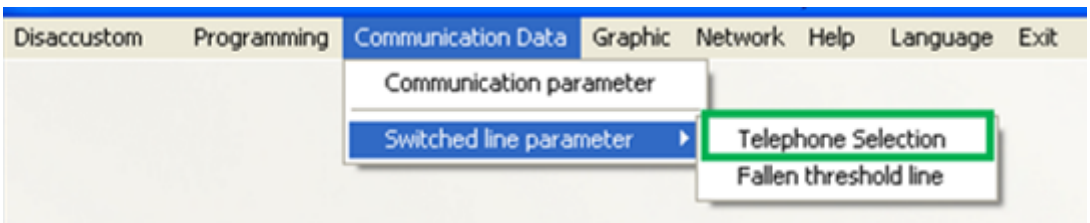
If the modem used operates with the RTS criteria always high, press key **RTS Def.** → so that writing *RTS. H* appears.

For more information about the RTS criteria, please refer to the modem user manual.

Press key **Execute** to apply the settings and return to the main menu.

3.4.2 Type of telephone selection

Select *Communication data* →*Switched-Line Parameters* → *Telephone Selection*.



Select the telephonic line type:

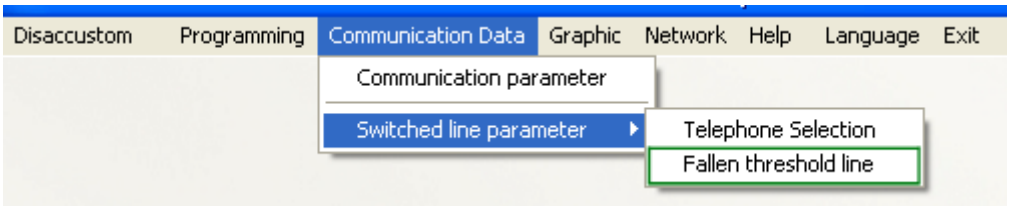
- *DTMF*: multi-frequency (selection valid for the last generation modems)
- *Pulse*: Pulse modem (for old generation modems)

For more information refer to the modem manual.

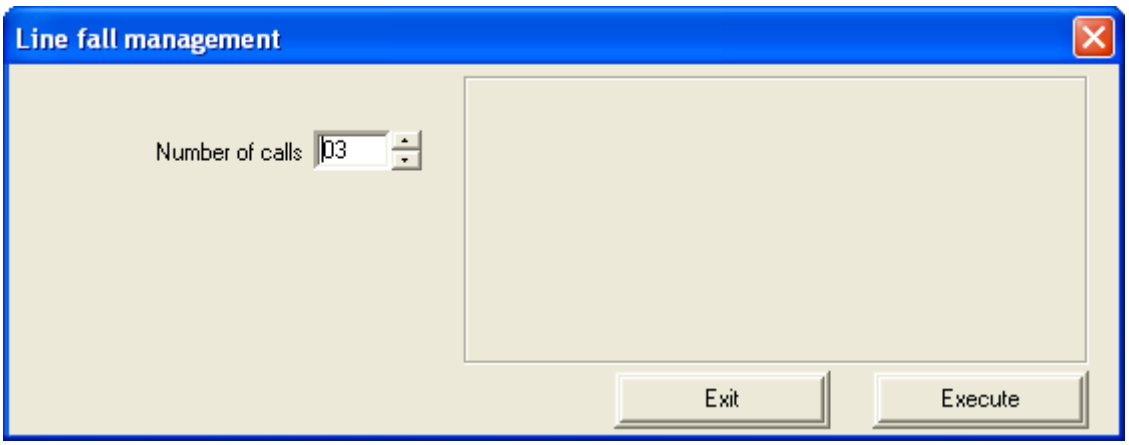
Press **Execute** button to apply the setting and return to the main menu.

3.4.3 Fallen line threshold

Select *Communication data* → *Switched-Line Parameter* → *Fallen threshold line*.



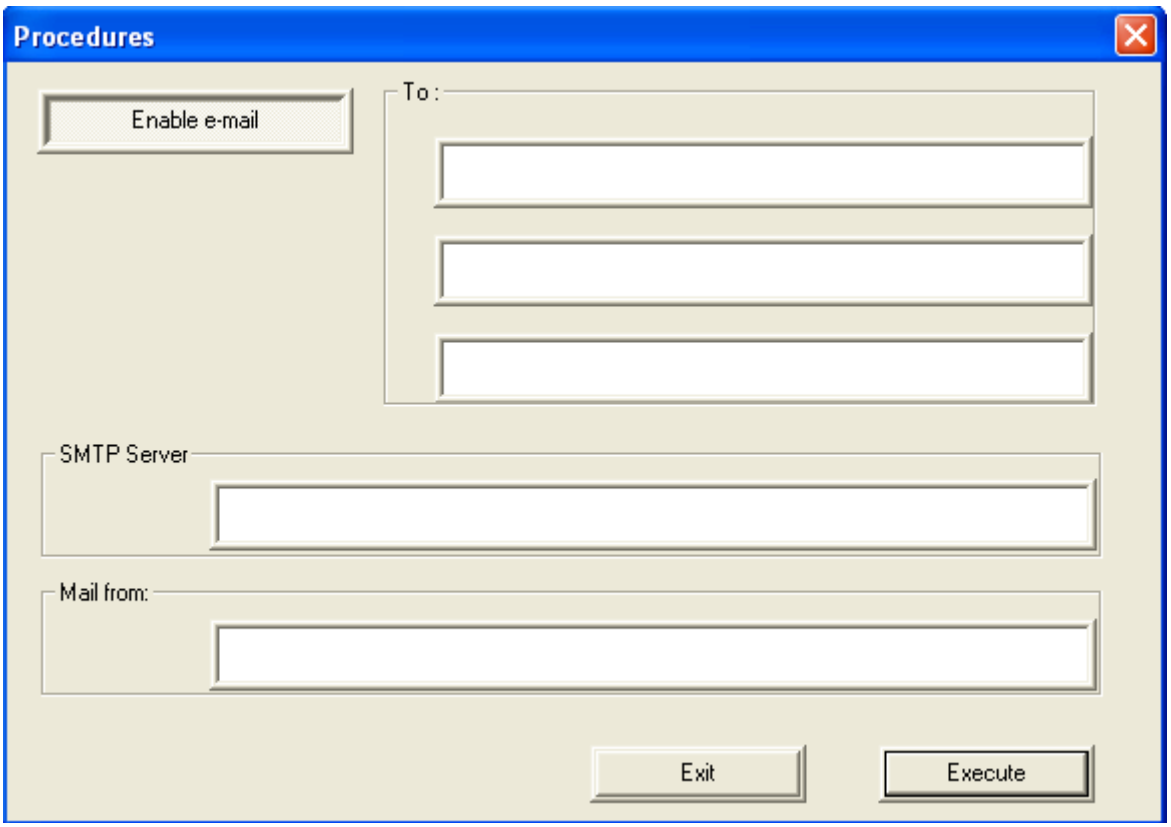
In the window that appears (figure below) set in field *Number of calls* the number of call attempts after which the system signals the fallen line. Once the fault has been signalled, the system waits for a certain time before making a new call attempt, like set in the window at paragraph 9.3.



Press key **Execute** to make the set-points effective and return to the main menu.

3.5 Configuring notification of alarms via E-mail

From the main menu, select *Programming* → *E-Mail Configuration*. In the window that appears (figure below) it is possible to enter up to three e-mail addresses which will receive the alarm messages.



First of all, press key **Enable e-mail** to activate the function.

If the E-mail management is not enabled, the icon will appear in window *Command Icons*.

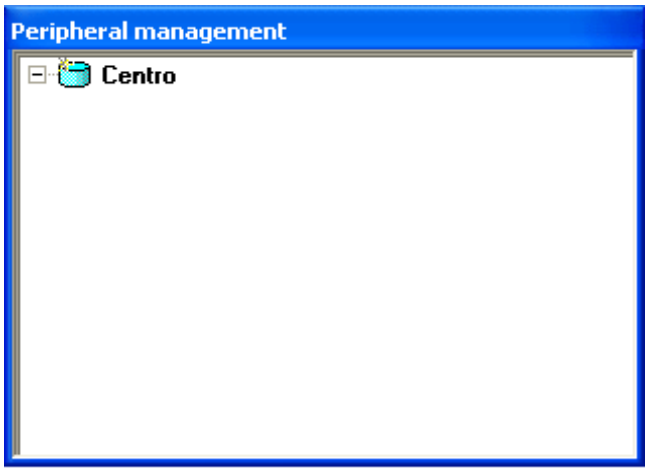
Enter the addresses (up to of 3 addresses) in the *To*: fields and insert the name of the SMTP server through which the messages are sent.

Insert in the *Mail from* field a valid e-mail address where the replies will be sent: in this way, when one of the addressees receives an alarm notification e-mail, il will be possible to answer to the so specified e-mail address.

Press key **Execute** to make the set-points effective and return to the main menu.

4. Configuring the control units

4.1 Adding the control units

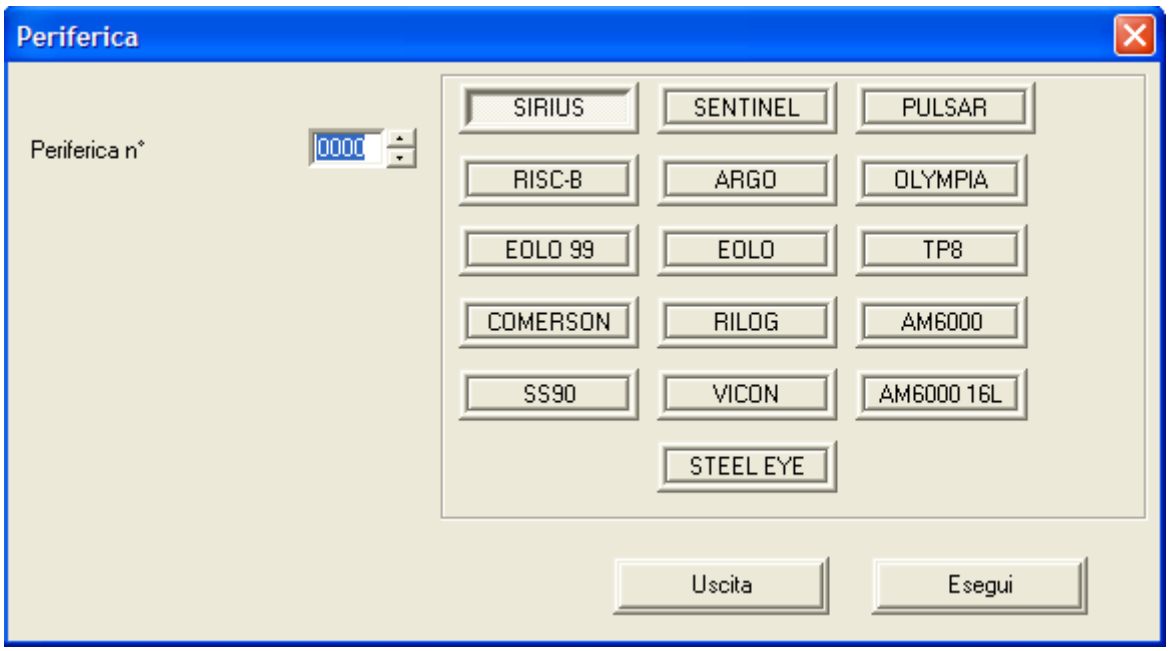


Once the control units are connected to the monitoring station and configured the connection parameters, you should add the control units in the system and configure them one by one, so that they are properly recognized by the software.

Select *Programming* → *System Configuration*.

The window that appears (figure on side) indicates the list of the configured control units; obviously initially the list is empty.

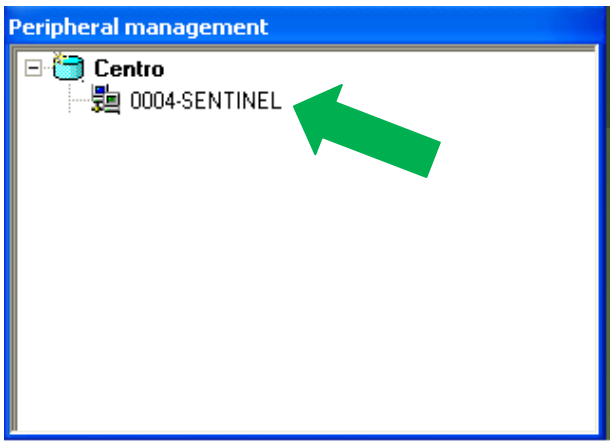
To add a new control unit, double click on *Centre*; the following window pops up.



In field *Peripheral n°* select the number of the control unit. This parameter has to me unique for each control unit.

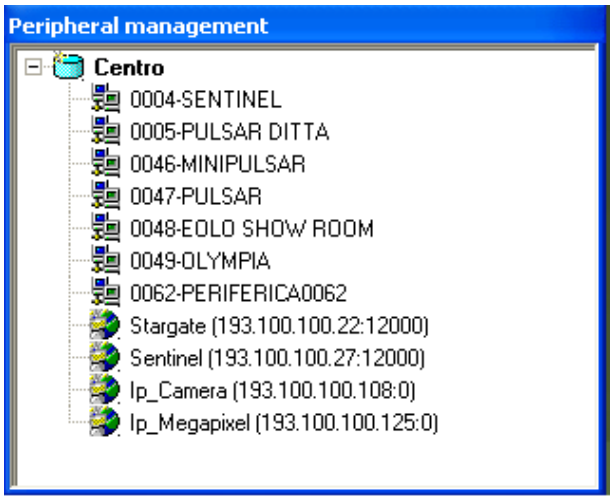
For every control unit, this parameter must be set in the same way on *Winwatch* software and on the control unit. On the control unit setup, this parameter is usually found in programming page *Centralized* → *Address*. For more information, please refer to the control unit user manual.

Select the model of control unit and press **Execute**. Repeat the same adding procedure for all the control units that need to be monitored.



To delete a control unit already added in the system, do a right click with the mouse on the control unit's icon in window *Peripheral management* (menu *Programming* → *System Configuration*) and select *Remove*.

By deleting a control unit all the set parameters will be erased too. To reactivate it again it will be necessary to reprogram it from the beginning.



The list of the control units added in the system is shown in the window *Peripheral management*.

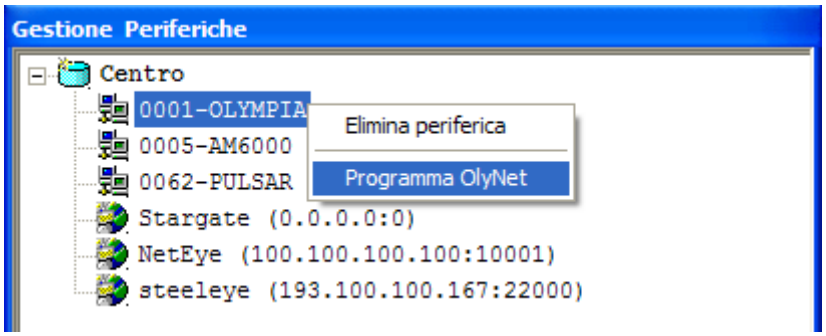
The icon aside the name varies according to the sort of station:

- this icon identifies burglar and fire alarm control units;
- this icon identifies the CCTV control units (added from the menu *Setup DVR-NVR*, paragraph 4.3).

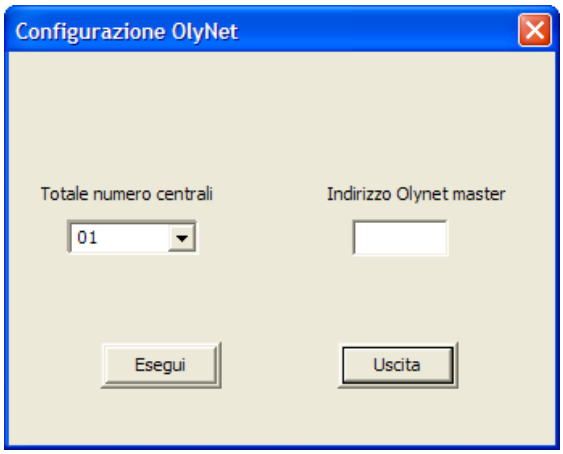
Sentinel and *SteelEye* model control unit appear twice in the list, as they carry out both functions of CCTV and burglar detection.

4.1.1 Programming *OlyNet* system

If an added *Olympia* fire control unit is connected to an *OlyNet* system with other control units of the same model it is possible to monitor all of them with *Winwatch* software.



To add an *Olympia* on *OlyNet* network, do a right mouse click on the *Olympia* control unit that is connected directly to the monitoring station (see image above), and click on the menu *Configure Olynet.*



In such way, set these parameters.

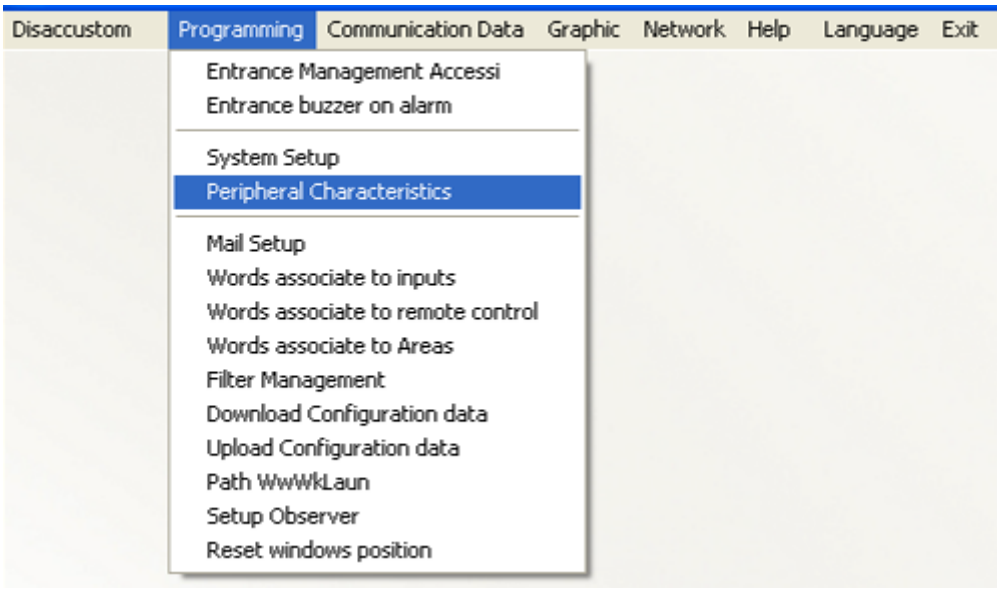
- Set the total of control units connected in *OlyNet network* (including also the control unit connected directly via LAN) through the drop down menu (for a maximum of 32 control units).
- Set the *OlyNet* address taken by the control unit connected directly via LAN, parameter that has to be set also in the control unit's programming (please refer to *Olympia* operator manual).

The *Winwatch* system will assign automatically the unique peripheral addresses (paragraph **4.1**) to all the new control units.

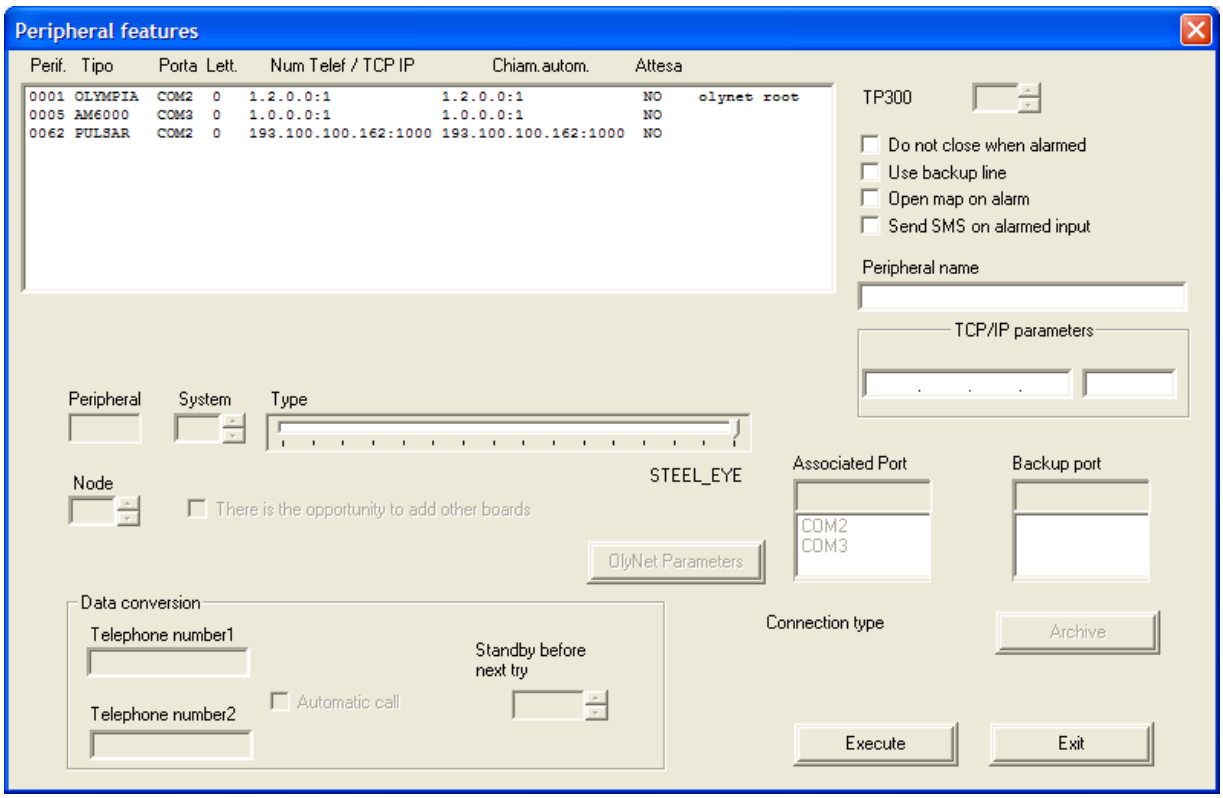
For more information about the behavior and the management of the *OlyNet* network please refer to *Olympia* operator manual.

4.2 Fire / burglar alarm control unit setting

From the main menu, select *Programming* → *Peripheral Characteristics*.



At the top left in the window now appearing (figure below) shows the list of all the control units added in the system with their progressive number and IP address. The unit number is displayed also at bottom left, in the field *Peripheral*.



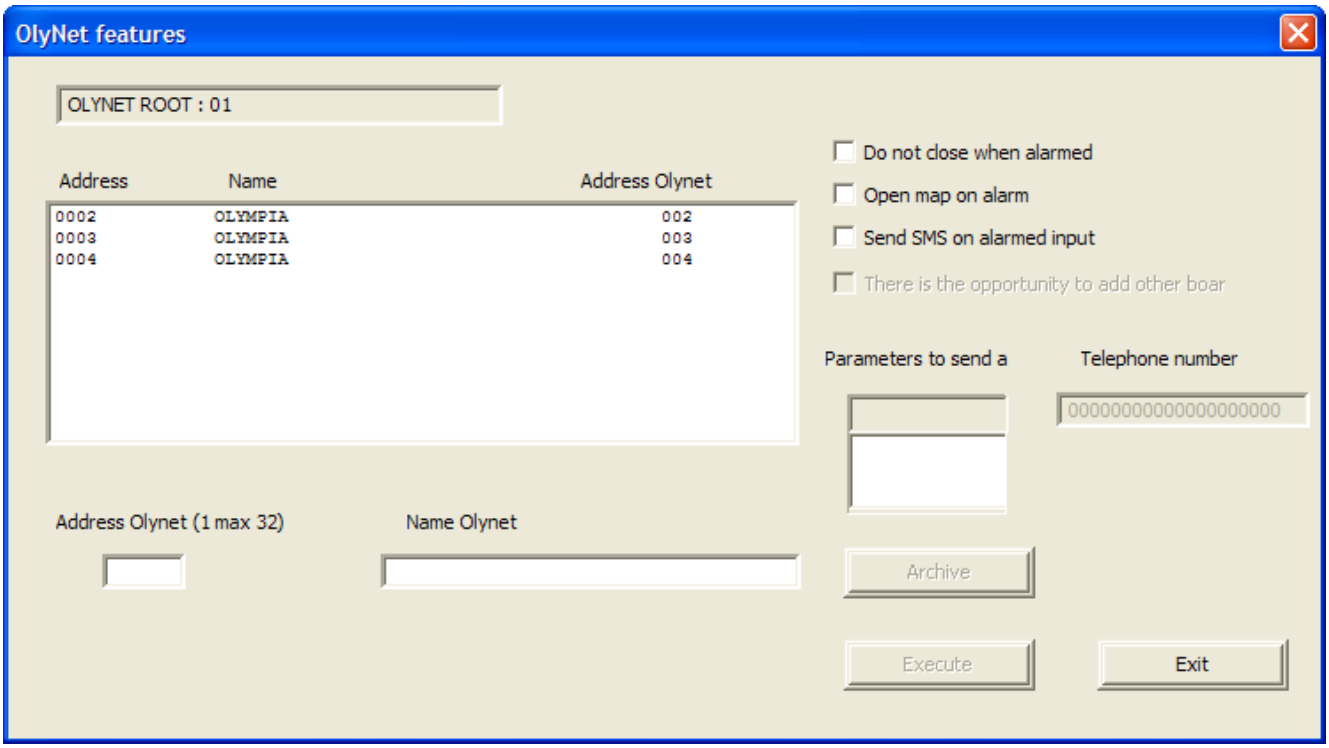
Do a left mouse click the on the name of the control unit to be programmed; Set the following parameters depending on the system requirements:

- Slide the arrow of field *Type* until the correct model of the selected control unit is displayed. If the type of control unit is changed, the configuration previously set will be deleted. (Function not mandatory)
- Set the control unit's name in field *Peripheral Name*.
- In field *Associated Port* select the communication port between monitoring station and control unit, as indicated in paragraph **3.3**:
  - If the communication port is configured as LAN, insert the IP address and IP port in field *TCP/IP Parameters*.
  - If the communication port is configured as switched / PSTN, enter in field *Telephone number2* the phone number to be composed for communicating with the selected control unit.
- If the use of a switched line has been set in the display page of connections (**3.3**), enable option *Use Backup Line* and select the corresponding connection port in the *Backup Port* field.
- Set in the *TP300* field the number of TP300 readers connected to the selected control unit. (Obsolete)
- Select the options of interest in the fields at top right:
  - *Do not close when alarmed*: if selected, avoids the user from closing the software *Winwatch* until all the alarms in queue are acknowledged;

- *Open map on alarm*: if selected, in case of occurrence of an alarm and the presence of that zone on map, automatically the map containing the peripheral device that generated the alarm will appear;
- *Send SMS on alarmed input*: if selected, in case of alarm an SMS is sent to the phone number programmed in field *Telephone number2*.

If the SMS are not enabled, icon is displayed in the *Command Icons* window.

- Only for *Olympia* control units, select option *Use Expansion Card* if the control units is prepared to add an expansion card inside.
- Only for *Olympia* control units, if an *OlyNet* network has been programmed (paragraph 4.1.1) it will be necessary to set the parameters described before also for all the other control units by pressing the button *OlyNet Parameters*.

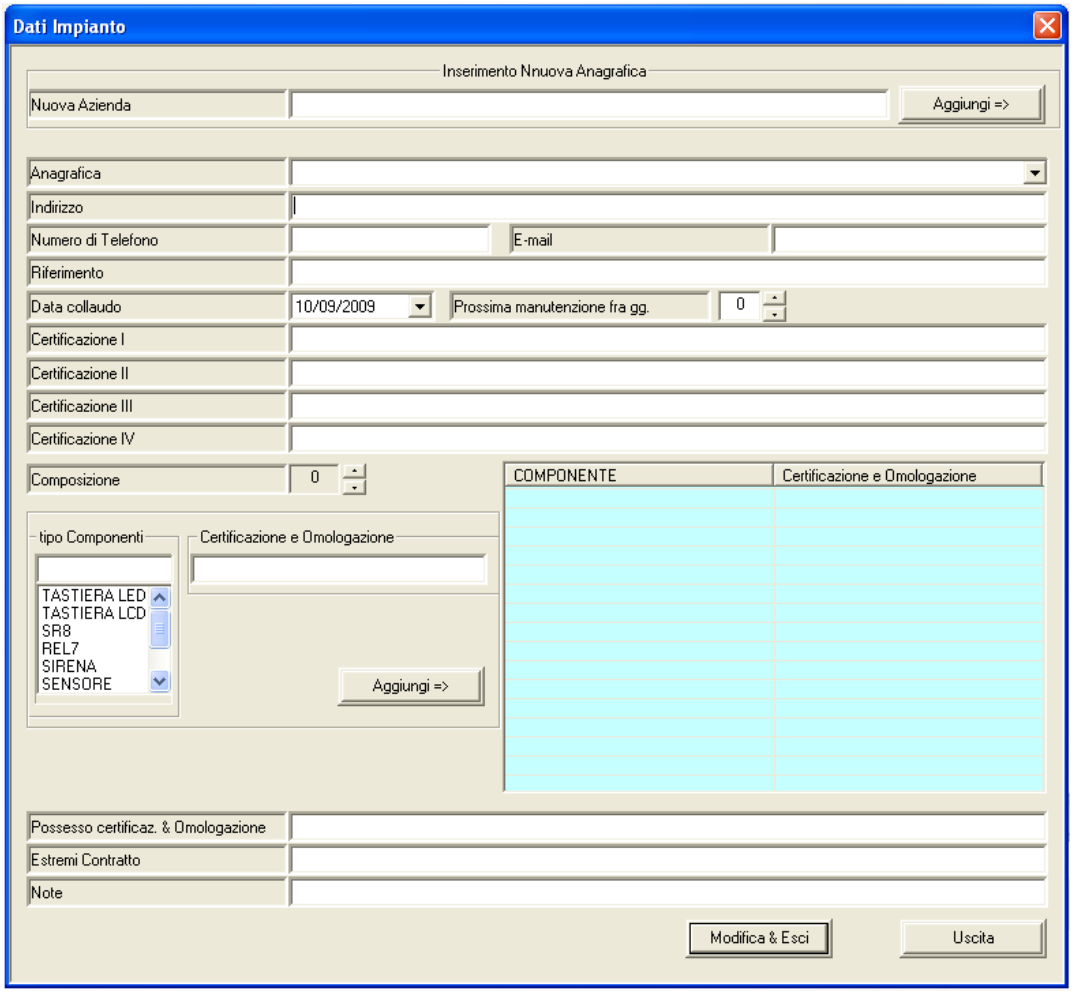


- Click the control unit to program.
- Give a name to the control unit in field *Name OlyNet.*
- Set the map management and SMS parameters (if needed).
- Press the button **Execute** to save the settings; repeat the same procedure for all the control units. Press **Exit** to close this window.

Once back to *Peripheral Characteristics* menu, press key **Execute** to save the settings.

4.2.1 Control panel registry record form

Press key *Archive*; a window as hereafter appears.

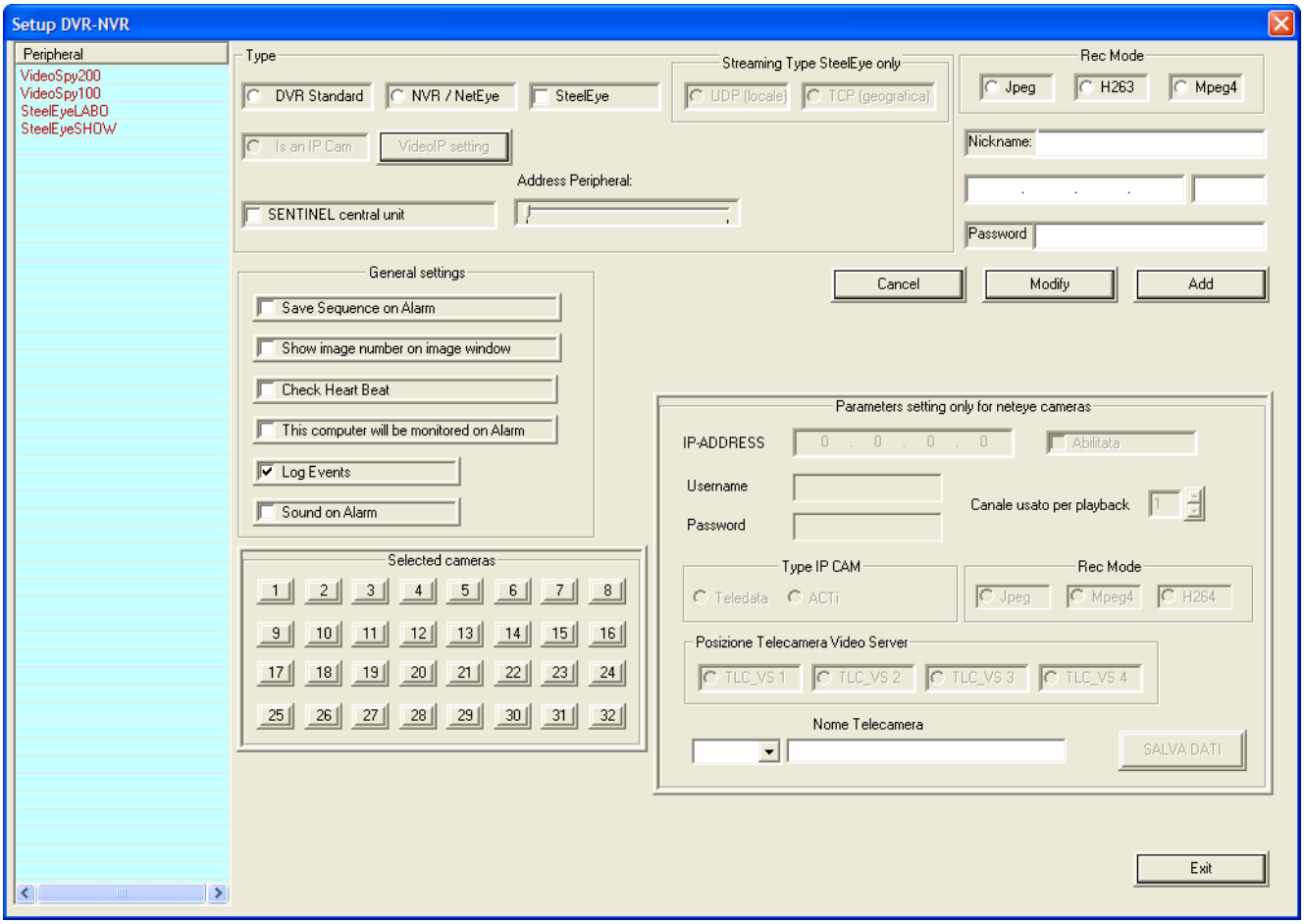


Fill the form according to the control unit's configuration and maintenance condition.

This page is only a record for the installer / maintainer of the system. How it is filled in has no practical effect on the system. The operators of the software will be able to view this mask from the menu *Peripheral Information.*

4.3 CCTV control units settings

Select from main menu *Programming* → *Setup DVR/NVR*.



The window appearing allows to add and configure CCTV station.

4.3.1 Inserting a new station

Below is the procedure to add a new video control unit to the system:

- Digit the station name in field *Nickname*.
- Select the video recorder model (*DVR Standard*, *NVR*, *SteelEye*, *IP CAM*)
- Press key **Add**: the control unit will appear in the *Peripheral* list.

Once a video peripheral is added, it will not possible to change the type. It will be necessary to delete it and reconfigure it from the beginning.

4.3.2 Configuring an added video control unit

If you are programming a DVR model *Stargate, Phantom* and *VideoSpy*, proceed as follows:

- Select the control unit name in the *Peripheral* list.
- If the control unit is protected by password, insert it in field *Password*.
- Insert the IP address and port in the field below *Nickname.*
- Activate the video channels that that need to be monitored with the software from the *Selected cameras* box.
- Select the type of *Rec Mode* set also in the DVR, viewable in the launcher.

To configure correctly all the remaining parameters, it is suggested to refer to the user manual of the single control units.

- Press button **Modify** to save the settings.
- Press button **Exit** to exit to main menu.

If you are programming a DVR model *Sentinel* or *SteelEye*, proceed as follows:

- Select the control unit name in the *Peripheral* list.
- Select *SENTINEL Central unit* option (if it is a model *Sentinel*)
- Select *Is a SteelEye* option (if it is a model *SteelEye*)
- Move the arrow in field *Address Peripheral* to select the address of the peripheral (the control units must have been added previously also in the menu *Programming* → *System configuration*)

For a correct functionality of *Sentinel* and *SteelEye* control units, set the peripheral address the same as the one inserted in the menu *Programming* → *System configuration*.

- If the station is protected by password, insert it in field *Password*.
- Insert the IP address and port in the field below *Nickname.*
- Activate the video channels that need to be monitored with the software from the *Selected cameras* box.
- Select the type of *Rec Mode* set also in the DVR, viewable in the launcher.

To configure correctly all the remaining parameters, it is suggested to refer to the user manual of the single control units.

- Press button **Modify** to save the settings.
- Press button **Exit** to exit to main menu.

If you are programming an NVR model *NetEye*, it will be necessary to set not only the video recorder, but also all the IP cameras connected. Differently from a DVR system with analogue cameras, the real time of an IP camera connected to a *NetEye* will be direct, without passing through the NVR. The *NetEye* IP parameters will be necessary only for camera playback. To program an NVR model *NetEye* proceed as follows:

- Select the control unit name in the *Peripheral* list.
- If the control unit is protected by password, insert it in field *Password*.
- Insert the IP address and port in the field below *Nickname.*
- Activate the video channels that need to be monitored with the software from the *Selected cameras* box.
- For each IP camera connected to *NetEye* it is necessary to set the IP address of the camera, user name and password, channel used for playback, type and *Rec Mode* from the *Enable channel to perform playback* box.
- To switch to the next IP camera, use the arrows above the *Enable channel to perform playback* box.

To configure correctly all the remaining parameters, it is suggested to refer to the user manual of the single control units.

- Press button **Modify** to save the settings.
- Press button **Exit** to exit to main menu.

If you are programming a *Video server* (added as an NVR), proceed as follows:

- Select the control unit name in the *Peripheral* list.
- If the control unit is protected by password, insert it in field *Password*.
- Activate the video channels of the cameras that need to be monitored with the software from the *Selected cameras* box. (maximum 4 cameras celectable)
- Set the IP address of the activated cameras the IP address of the video server, and set uniquely the *Camera position* for all the activated channels.
- Set the type of *IP Cam* to *Teledata.*

To configure correctly all the remaining parameters, it is suggested to refer to the user manual of the single control units.

- Press button **Modify** to save the settings.
- Press button **Exit** to exit to main menu.

5. Maps programming

5.1 Planning the map system

The *Winwatch* application isn't mandatory to have maps to work. The use of maps is particularly useful for displaying graphically the position of the linked control units (burglar detection / fire detection / CCTV) and of the devices interfaced to it (for example burglar detection sensors, fire alarm buttons, video cameras, etc.) through a system of multi-level maps.

The main map (level 0) represents the system in general, showing the position of the control units. Several level 1 maps can be associated to it, which represent for example (but not necessarily) the detail of the system managed by that control unit. Several level 2 maps can be associated to each level 1 map, and they represent for example (but not necessarily) the zones associated to an individual control unit.

The organization of multi-level maps is free and not mandatory; the only map that requires to be configured is the main map.

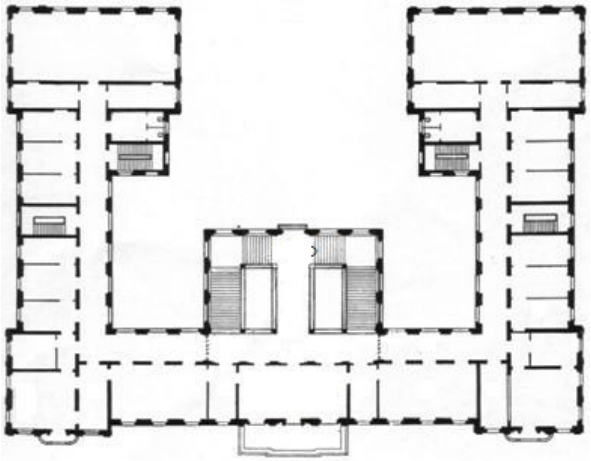
Below are shown two different examples of organization of the mapping levels for systems of different complexity.

5.1.1 Simple or medium complexity system

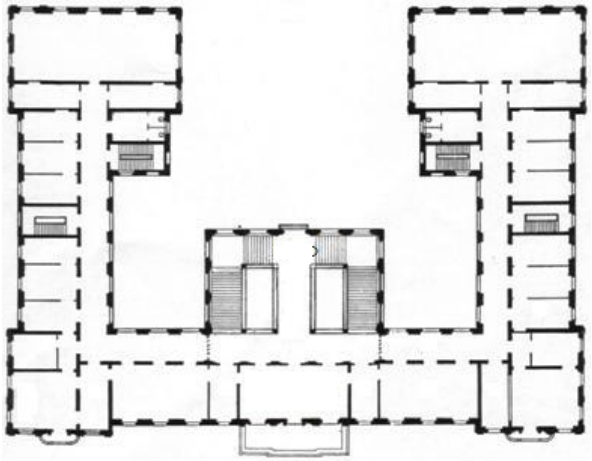
Assuming that the system is a complex system, for example a multi floor buinding, where every floor has several rooms.

The main map consists of the front of the building, which contains a view of all the floors (in our case 3). Each floor is associated to a level 1 map that represents the plan of one floor (ground floor, first floor, second floor).

Main map



Level 1 map (ground floor)



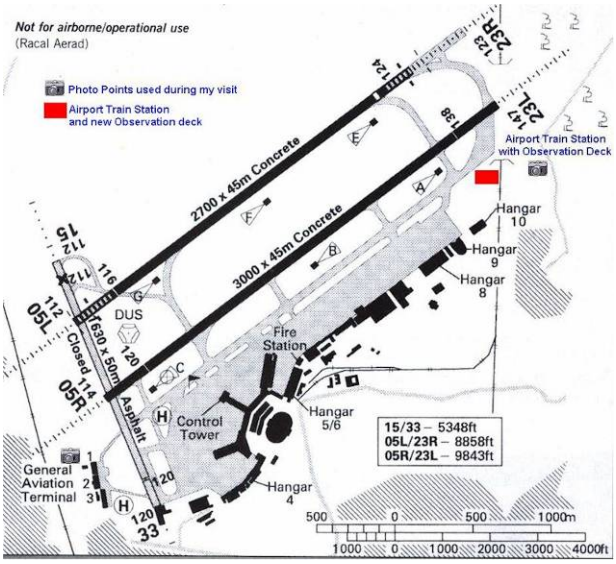
Level 1 map (first floor)

5.1.2 Complex system with groups and sub-maps

Assuming that the system is applied to control an international airport, consisting of more terminals, each having more floors.

In this case, the main map is the airport plan, which several level 1 maps are linked to it, each of which covers a different area of the airport: terminals, car parks, etc. Every area is disposed on more that one floor, each of which is shown on a level 2 map.

Main map



Level 1 map: terminal 1 **Map level 2: first floor of terminal 1**

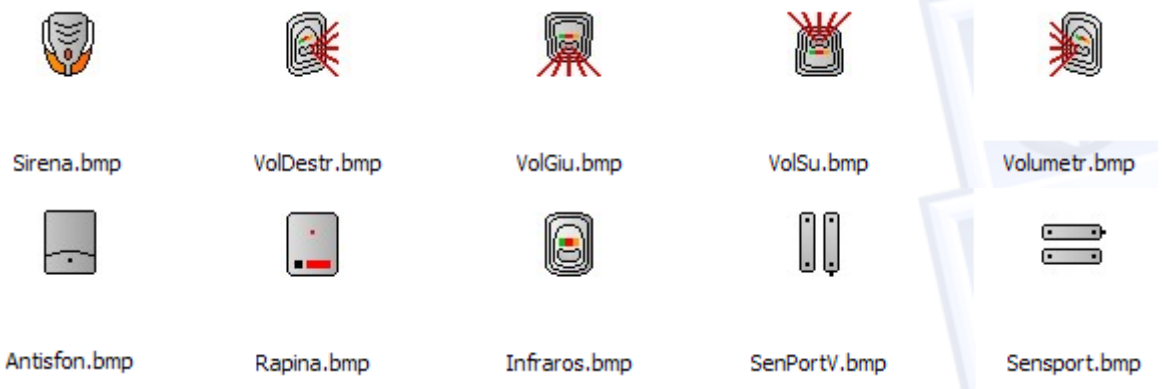
5.2 Peripheral devices symbols management

5.2.1 Symbols library

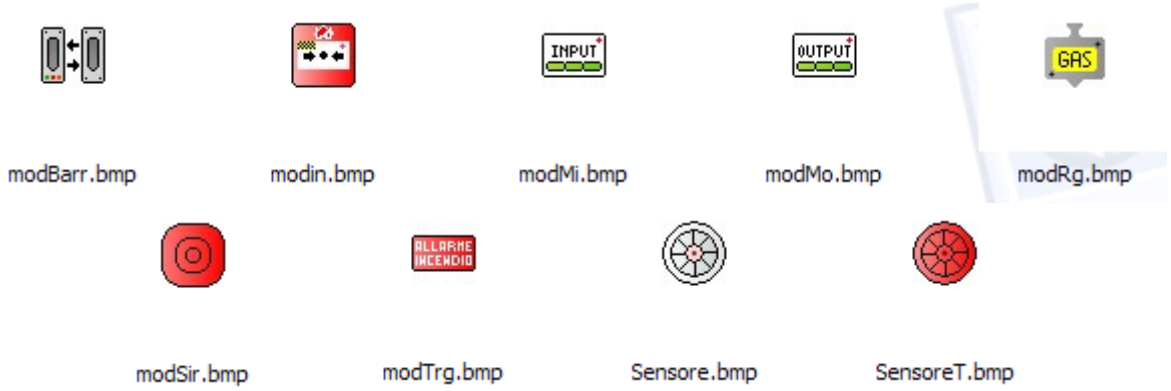
The software contains a library of predefined symbols linked to the various peripheral devices which are connected to the burglar and fire alarm control units:

- 10 symbols for the burglar alarm peripheral devices;
- 9 symbols for the fire alarm peripheral devices.

5.2.1.1 Burglar alarm peripheral devices



5.2.1.2 Fire alarm peripheral devices



5.2.2 Creating and modifying symbols

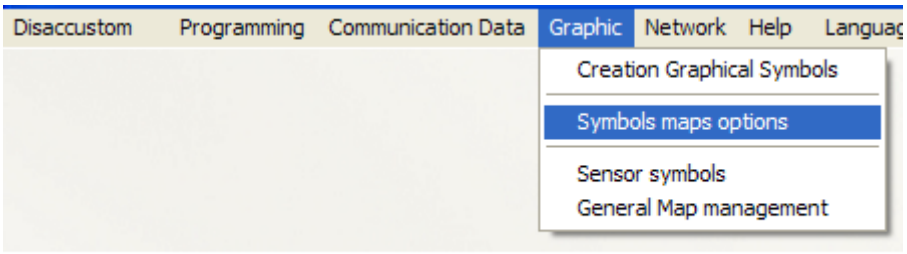
To create symbols, use the option *Graphics* → *Creating Graphic Symbols*. Once a symbol has been created, it will be added into the library stored in directory *…\winwatch32\Simbolisensori*.

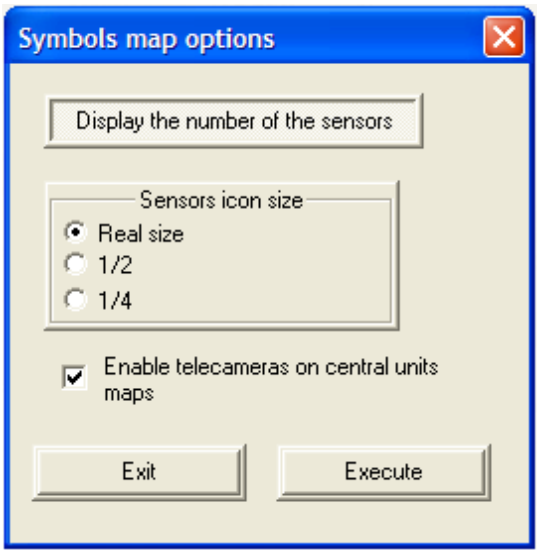
To modify existing symbols, use an image editor software (like for example *MS Paint* or *Adobe Illustrator*) and save the images in BMP format, with resolution 32×32 pixel and maximum size 10Kb.

Symbols can be created and modified by using any editor; once the operation is completed, enter the symbols in directory *…\winwatch32\Simbolisensori*.

5.2.3 Symbol map options

Select *Graphics* → *Symbols map options*.



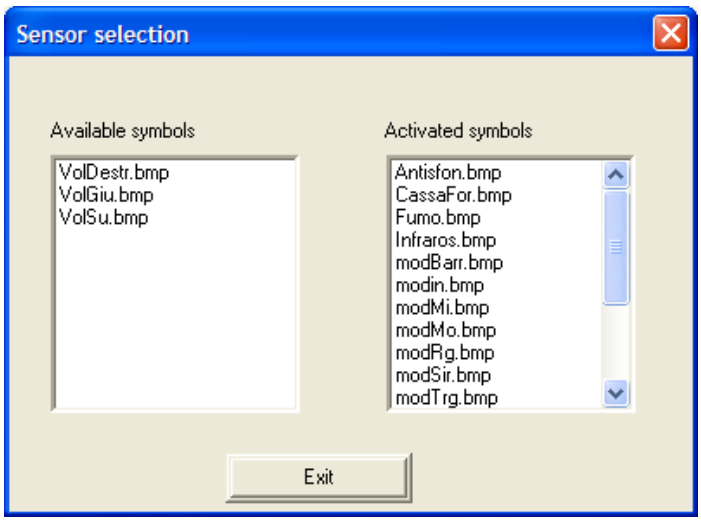


In the window appearing on the screen (figure on the side) enter the following settings:

- Press key *Display the number of sensors* if you wish that, in correspondence of every sensor, a number indicates the referred input;
- Select, in box *Sensor icon size* the size of the icons viewed that represent the sensors on the maps;
- If you wish to insert the cameras on the maps of the control units, select the option *Enable telecameras on central units maps*.

5.2.4 Symbols activation

The system allows to activate up to 16 sensor symbols from the library. To do so, click on *Graphics* → *Sensor selection*.



The window now appearing shows two lists:

- Available symbols (left column)
- Activated symbols (right column)

To activate a symbol, double click on the name of the symbol in the *Available Symbols* list; the symbol name will appear in the *Activated Symbols* list.

To deactivate a symbol that was activated previously, double click on the symbol name in the *Activated Symbols* list: it will disappear from the list.

5.3 Main map management

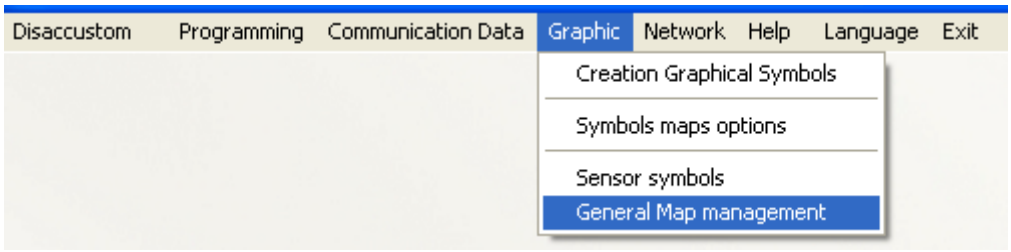
5.3.1 Creating the main map

It is possible to use any software capable of generating an image in BMP format; once the map has been created, it is necessary to save it under name *Mmap.bmp* in directory *..\winwatch32\winwatch*.

Once the control units are configured, they will be laid on the main map. Then it will be possible to associate a level 1 map to each control unit (paragraph **5.4.1**).

5.3.2 Modifying the main map

Once all stations have been entered in the system, select *Graphics* → *General Map management*.



The main map is displayed; all station icons are located at top left.

For laying out the station icons wherever desirable, proceed as follows:

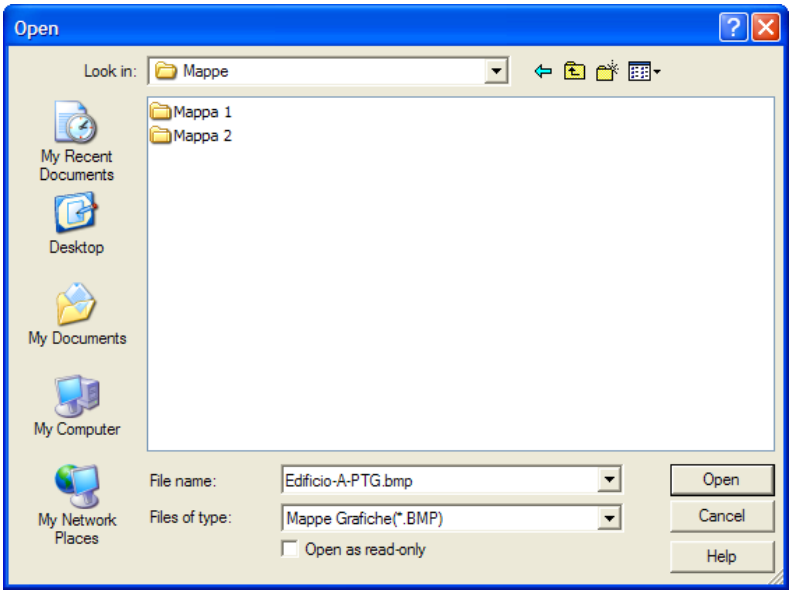
- Double click on the icon of the station to be relocated.
- Put the mouse pointer where you intend to locate the peripheral device; double click again.

5.4 Management of level 1 and level 2 maps

5.4.1 Control unit map (level 1)

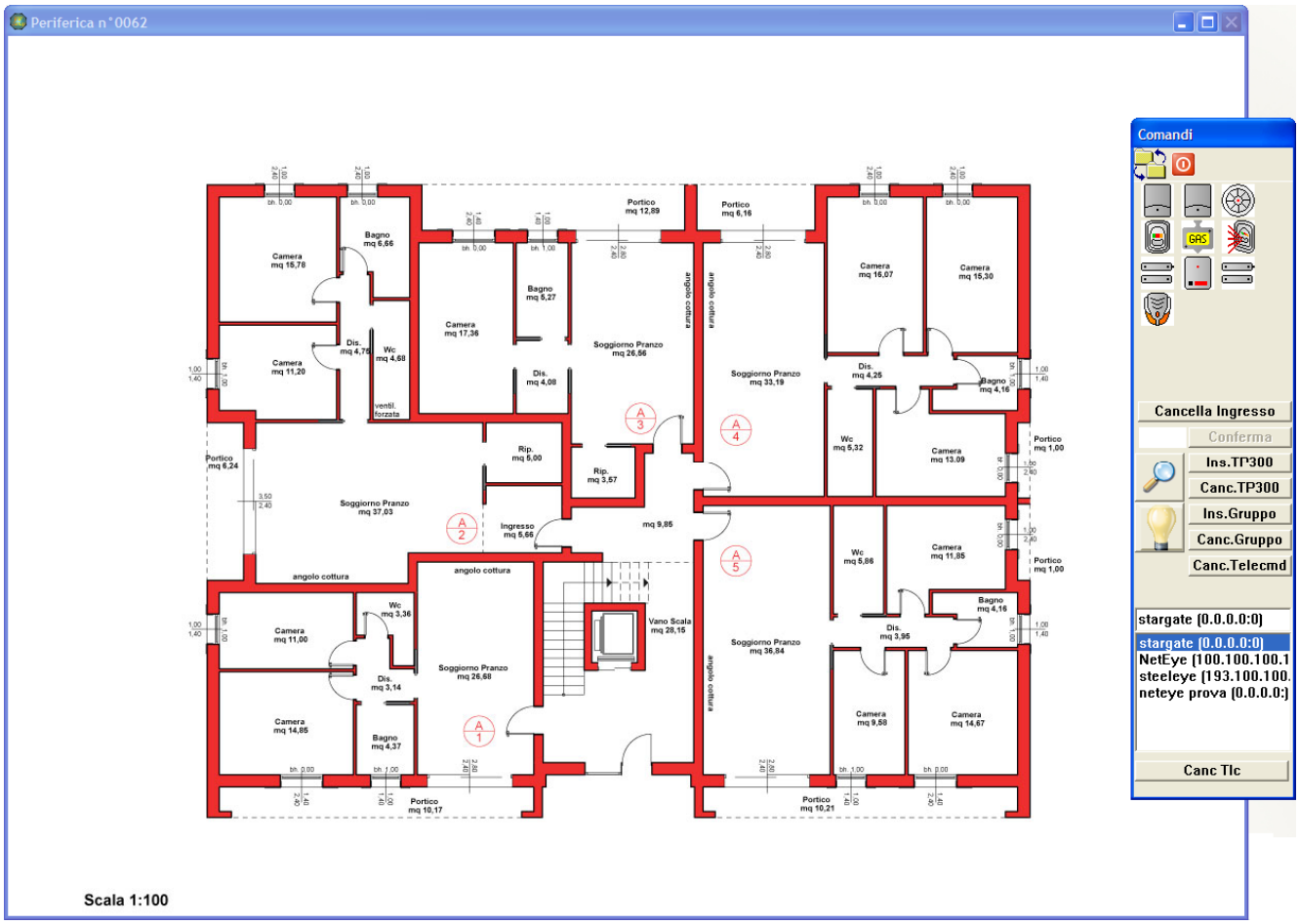
To every control unit it is possible to link a map (control unit map) which shows all the devices connected to it (sensors, cameras, etc.). To do so, create the map with a suitable application and save it in directory *…\winwatch32\maps*. In .bmp file format. It is possible to organize the maps in sub-directories, if necessary.

To select the map, double click on the control units icon in window *Peripheral management* (menu *Programming* → *System Configuration*).



Select the level 1 map that will be linked to the selected control unit and press **Open**.

Once opened, the control unit's map can be subdivided, if needed, into groups to generate level 2 maps (paragraph 5.4.7).



Instead, if it is necessary to use only the control unit map (without sub-levels), then it is possible to lay out the devices symbols in the control unit map.

Each device has to be located on the control unit map (level 1) or on the map of a group of peripheral devices (level 2, paragraph 5.4.7), even if this is not mandatory for the complete functionality of the system.

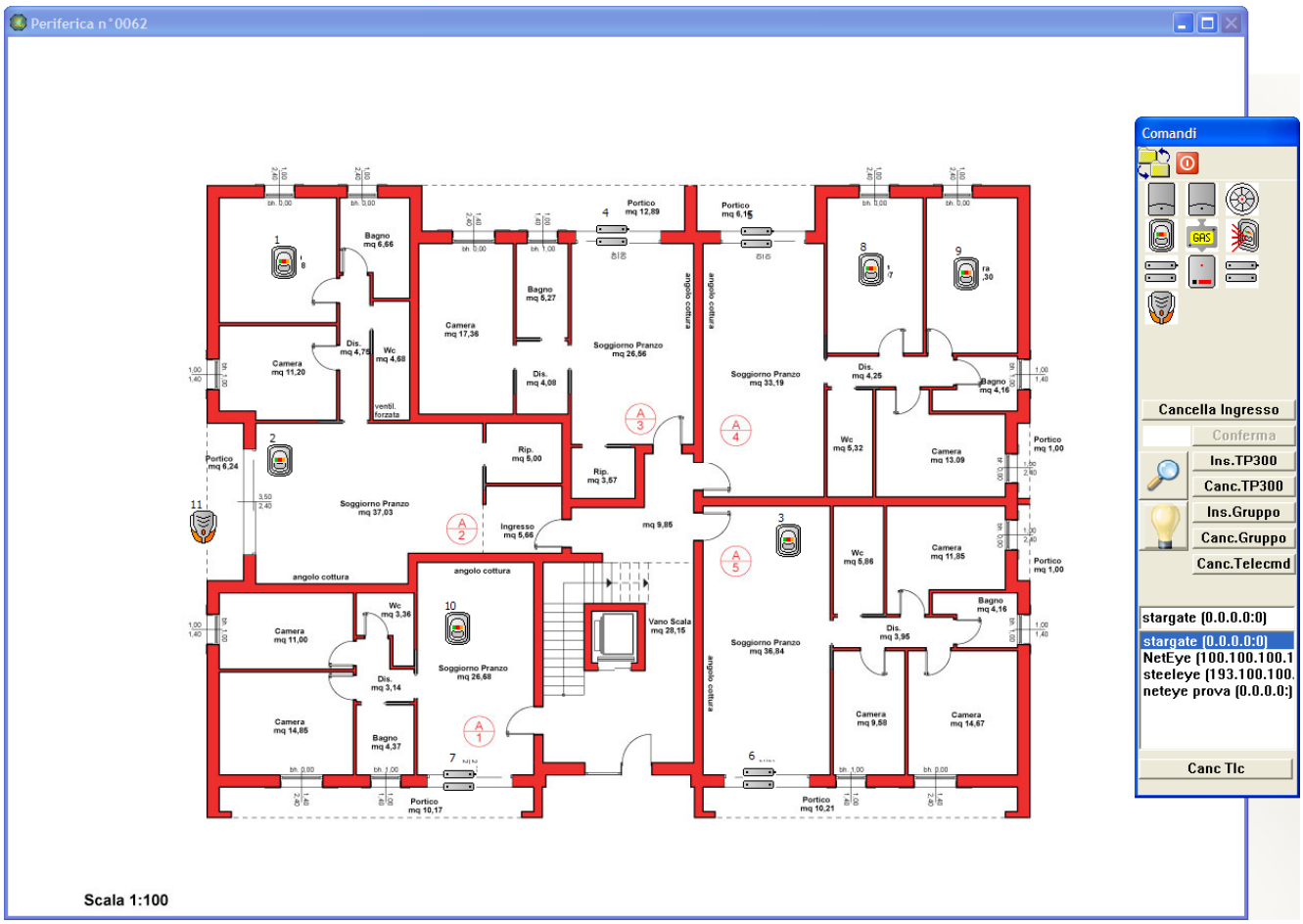
5.4.2 Adding / Deleting burglar detection symbols

Once opened the map, proceed as follows:

- Select the interested sensor symbol in window *Controls* (figure on the left);
- Position the mouse pointer into the spot of the map where you wish to add the sensor and double left click with the mouse.
- Enter the control unit's input/zone number that has been added in the white field next to the *Confirm* button.
- Press **Confirm**.
- Repeat the same operation for the inputs that need to be monitored.

To delete a burglar detection sensor, proceed as follows:

- Enter the number of the sensor to delete in the white field next to the *Confirm* key.
- Press key **Cancel input**
- Press **Confirm**.



In the example of the figure above, 6 volumetric sensors marked with symbol , 4 magnetic contacts marked with symbol and a siren marked with symbol have been added, numbered from 1 to 11

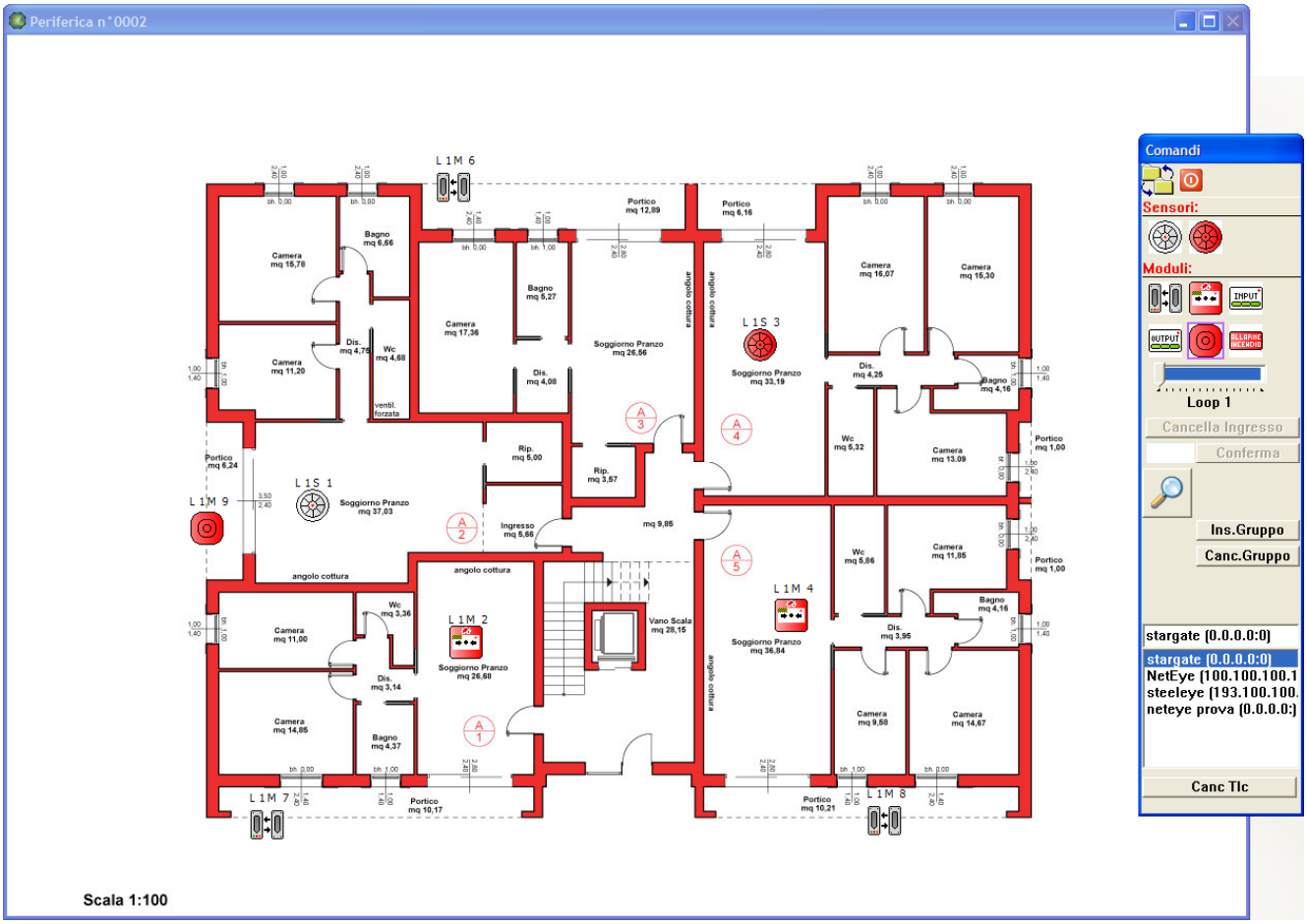
5.4.3 Adding / Deleting fire related symbols

Once having opened the map, proceed as follows:

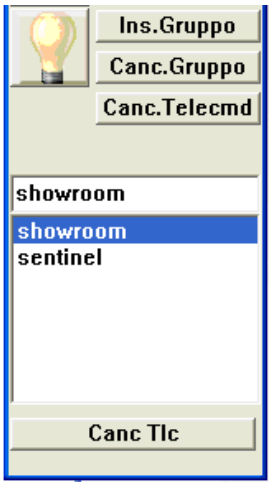
- Select the loop where the sensor/module is connected;
- Select the interessed sensor / module symbol in window *Controls* (right hand side in the figure below);
- Position the mouse pointer into the spot of the map where you wish to add the sensor/module and double left click with the mouse.
- Enter the sensor/module number in the white field next to the *Confirm* key.
- Press **Confirm**.
- Repeat the same operation for the inputs that need to be monitored.

To delete a fire detection sensor/module, proceed as follows:

- Right mouse click on the symbol to be removed;
- Select **Remove & Quit**.



5.4.4 Adding / Deleting video cameras



It is possible to add cameras on burglar and fire detection control unit's maps. To add a camera, proceed as follows:

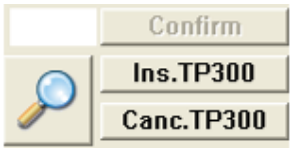
- Select the name of the DVR in the window below. the example in the figure shows two systems: *showroom* and *sentinel*.
- Position the mouse pointer into the spot of the map where you wish to add camera and double left click with the mouse.
- Enter, in the white field next to the *Confirm* key, the number of camera input that is added.
- Press key **Confirm**.
- Repeat the same operation for the inputs that need to be monitored.

To delete a video camera, proceed as follows:

- Select the name of the CCTV control unit in the window below.
- Press key **Canc Tlc**.
- Enter the number of the camera to deleted.
- Press key **Confirm**.

5.4.5 Adding / Deleting TP300 sensors

The procedure to add a TP300 access control reader is as follows:



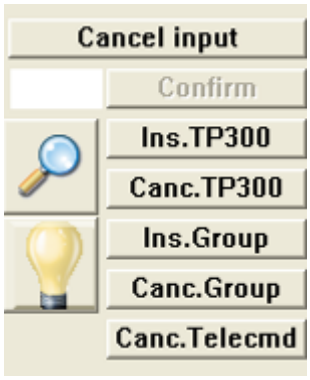
- Press key **Ins. TP300**.
- Position the mouse pointer into the point of the map where you wish to add the reader and double left click with the mouse.
- Enter the number of the TP300 reader in the white field next to the *Confirm* key.
- Press key **Confirm**.
- Repeat the same operation for all the needed readers.

Every TP300 reader must be numbered, and the total number of TP300 readers must be set in the system (paragraph 4.3.1).

To delete a reader, proceed as follows:

- Press key **Canc. TP300**;
- Enter the number of the TP300 to deleted in the white field next to the *Confirm* key.
- Press key **Confirm**.

5.4.6 Adding / Deleting a remote control



Add a relay uses as remote control, proceed as follows:

- Press the  key.
- Position the mouse pointer into the spot of the map where you wish to add the remote control and double left click with the mouse.
- Enter the number of the relay in the white field next to the *Confirm* key.
- Press key **Confirm**.
- Repeat the same operation for all the needed relay.

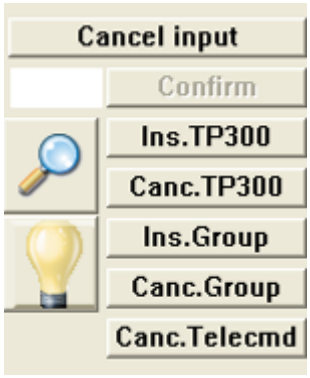
To delete a remote control relay, proceed as follows:

- Press key **Canc. Telecmd**
- Enter the number of the remote control relay to delete in the white field next to the *Confirm* key.
- Press key **Confirm**.

5.4.7 Creating maps for groups of sensors (level 2)

Instead of positioning the symbols of the peripheral devices on the control unit map (level 1), it is possible to subdivide the peripheral devices into two or more groups, associate a map to each of them, and distribute the symbols in the maps of the groups (level 2).

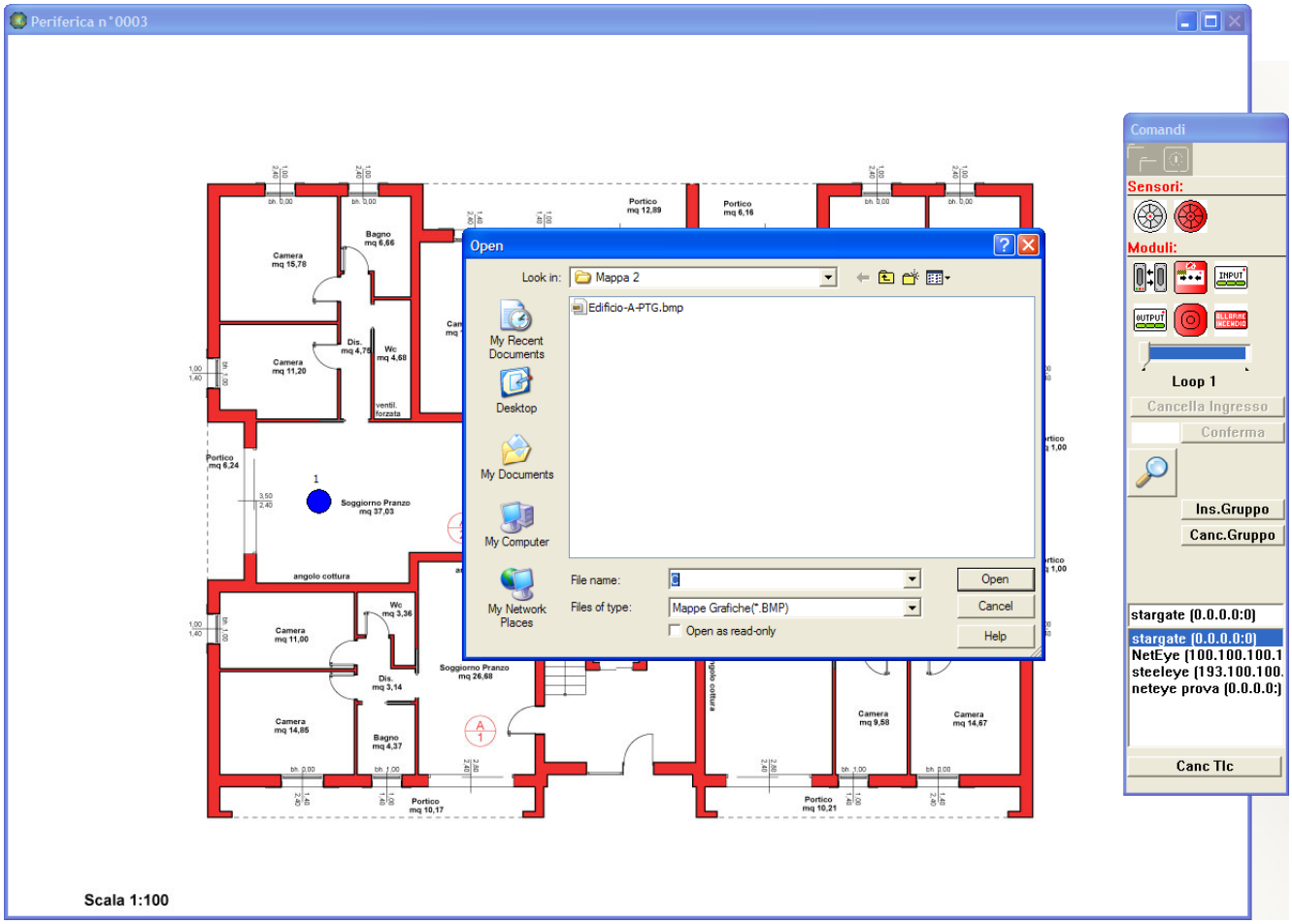
To add a group in the control unit map, proceed as follows:



- Press **Ins. Group** in window *Controls*.
- Position the mouse pointer into the spot of the map where you wish to add the group and double left click with the mouse.
- Enter the number of the group in the white field next to the *Confirm* key.
- Press key **Confirm**.
- Repeat the same operation for all the needed groups.

A blue spot appears to indicate the group, with the selected number.

It is suggested to continue a progressive numeration. The group number has to be unique for each control unit map.



To link a map to the added groups, double click on the blue spot and select the file of the map in .bmp file format.

At this point, it will be possible to add the peripheral devices as indicated in the previous paragraphs.

5.4.8 Browsing through the maps

To browse through the maps, use the following keys:

 Change the map's image

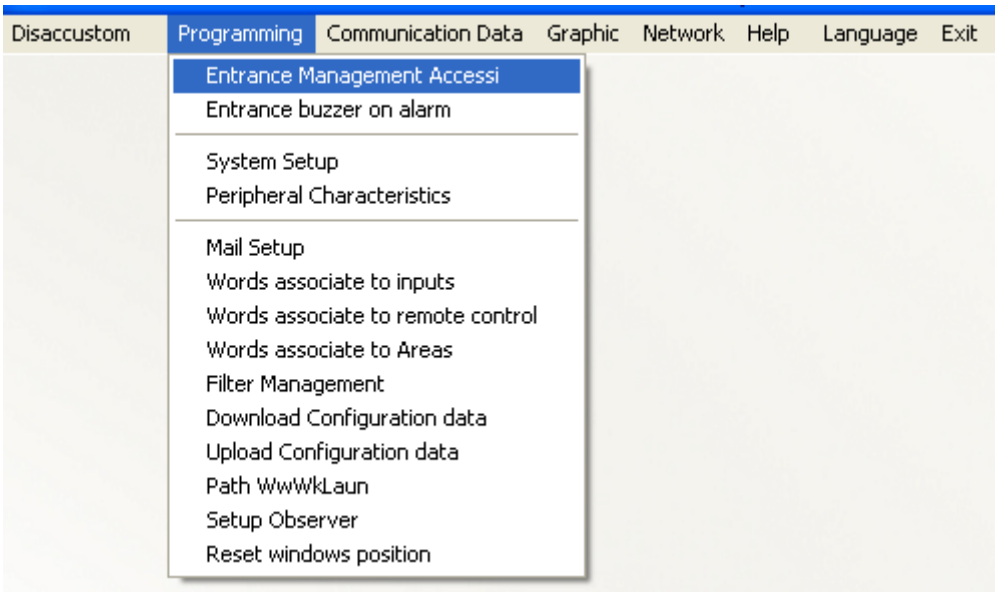
 Return to the higher level map

 Exit the maps setup

6. Special settings

6.1 Access control management

Select *Programming* → *Enable Management Accessi*.

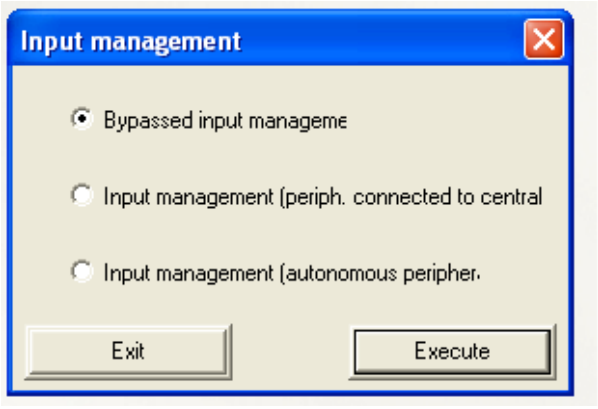


This setting is for the integration between the software *Winwatch* (dedicated for monitoring burglar, fire alarm and CCTV control units) and the software *Serchio* (dedicated for programming and monitoring access control units).

The *Serchio* software is available in two versions:

- *Serchio Standard*, supported until 2009 by *Teledata*, and integrated into the *Winwatch* software as an option;
- *Serchio 2009*, which replaced the *Serchio Standard* software and which cannot be integrated direct into the *Winwatch* software.

If the *Winwatch* version installed in the computer in use integrates the *Serchio Standard* software (installed in directory C:\winwatch32\Serchio), it is possible to select one of the following options in the pop-up window (figure below):



- *Input management (periph. Connected to centrals)*, if the system has at least one access control unit which is connected to peripheral devices that monitor the accesses;
- *Input management (autonomous periph.)* if the access monitoring peripheral devices are installed directly to the computer in use.

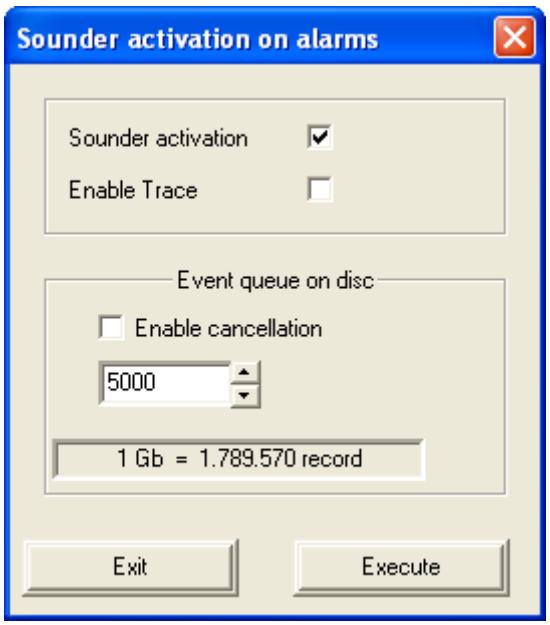
Vice versa, if the *Winwatch* version installed in the computer in use is not integrated with the *Serchio Standard* application, select option *Bypassed input management*.

In this case, any access control unit in the system must be managed by the *Serchio 2009* application (if installed in the computer in use).

Press key **Execute** to make the set-points effective and return to the main menu.

6.2 Enable advanced functions

Select *Programming* → *Sounder activation on alarms*; the following screen appears.



In this page it is possible to enable some special functions, as explained in the following paragraphs. Once the settings are entered, press key **Execute** to close the window and save; press **Exit** to quit without saving.

6.2.1 Buzzer activation

Select option *Sounder activation* if you wish to activate the buzzer when an alarm is received by a control unit.

6.2.2 Events erasure

For saving space on the hard disk of the computer in use, it is possible to delete the older stored events when their list reaches an N quantity of events: the N parameter can be set. To do so, proceed as follows:

- Select option *Enable deletion*;
- In the field underneath, select the number of events upon reaching which the older ones are deleted.

For example, if you select 5000, after 5000 events have been generated, all of these will be deleted from the hard disk.

6.2.3 Enable Trace

Select this option only if requested by *Teledata* technical service engineers.

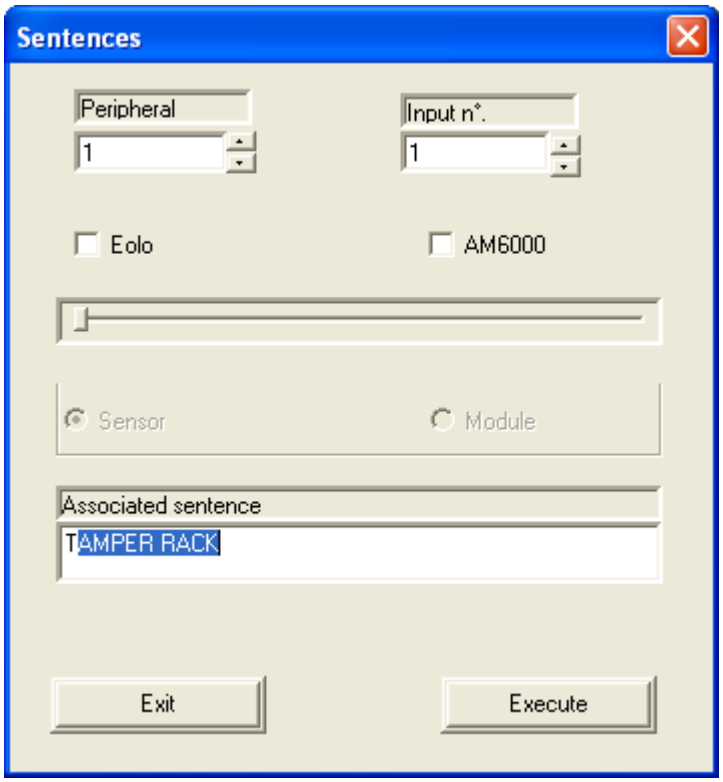
This function generates a log file which will be useful for *Teledata* engineers in finding out the source of faults during system diagnostics.

6.3 Associated sentences

It is possible to associate a short description to inputs (paragraph 6.3.1), to remote controls (paragraph 6.3.2), and to areas (paragraph 6.3.3).

6.3.1 Inputs

Select *Programming* → *Sentences associated to Inputs*.



In the window now appearing, select the control unit number (field *Peripheral*) and the input/zone number (field *Input N°*).

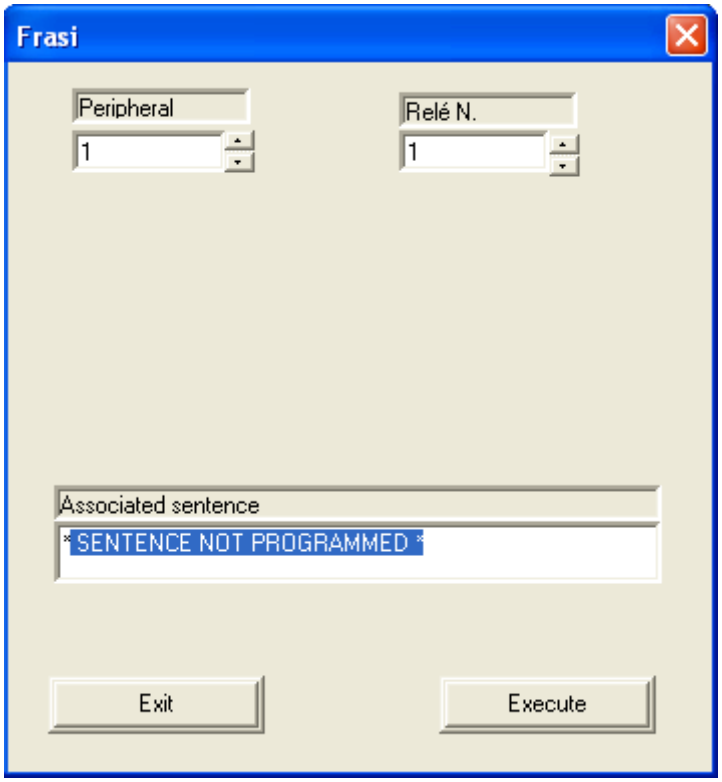
If the control unit is a fire alarm, the option *Eolo* and *AM6000* will select automatically. Select the loop where the device is connected. Declare also is it is a *Sensor* or a *Module*.

Once the input/zone is univocally identified, write a description of the peripheral device in field *Associated sentence*. In this way, as soon as an alarm arrives, the set phrase is shown on the screen (or in the text of the E-mail, paragraph 10.5).

Press key **Execute** to save the phrase and pass to the next input/zone.

Press **Exit** to return to main menu.

6.3.2 Remote controls



Select *Programming → Phrases associated to Remote Controls*.

In the window now appearing, select the control unit number (field *Peripheral*) and the number of the relay which was programmed in the control unit as remote control (field *Relay n°*).

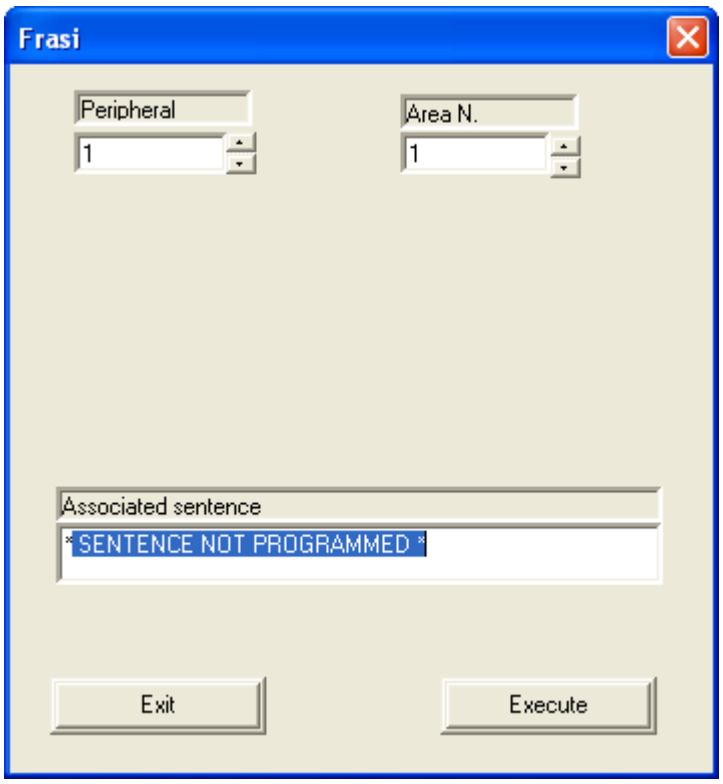
A this point, write a description of the relay in field *Associated sentence*.

In this way, whenever the relay being used as remote control is activated or deactivated, the set phrase is shown on the screen of the computer in use.

Press key **Execute** to save the phrase and pass to the next input/zone.

Press **Exit** to return to main menu.

6.3.3 Areas



Select *Programming → Associated sentences*.

In the window now appearing, select the control unit number (field *Peripheral*) and the area number (field *Area n°*).

At this point, write a description of the area in field *Associated Phrase*.

In this way, whenever an area is armed or disarmed, the set phrase is shown on the screen of the computer in use.

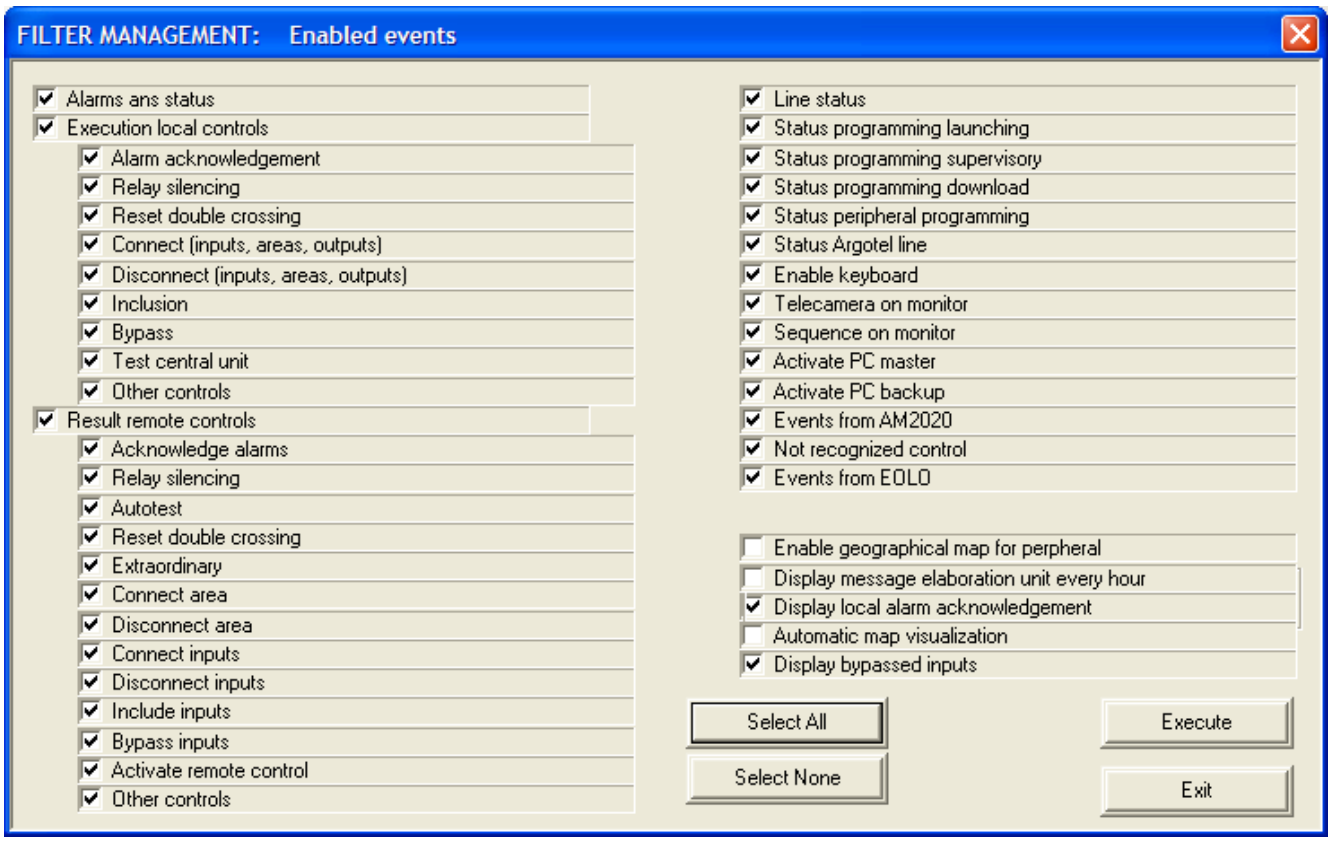
Press key **Execute** to save the phrase and pass to the next input/zone.

Press **Exit** to return to main menu.

6.4 Events window filter

It is possible to select the type of messages that will be displayed in the events window (paragraph 8.2.6); the messages that are not displayed are however stored in the events database.

Select *Programming →Events Window Filter*.



Select the type of messages in sheets *Alarms and Statuses*, *Execution of local commands* and *Outcome of remote controls*.

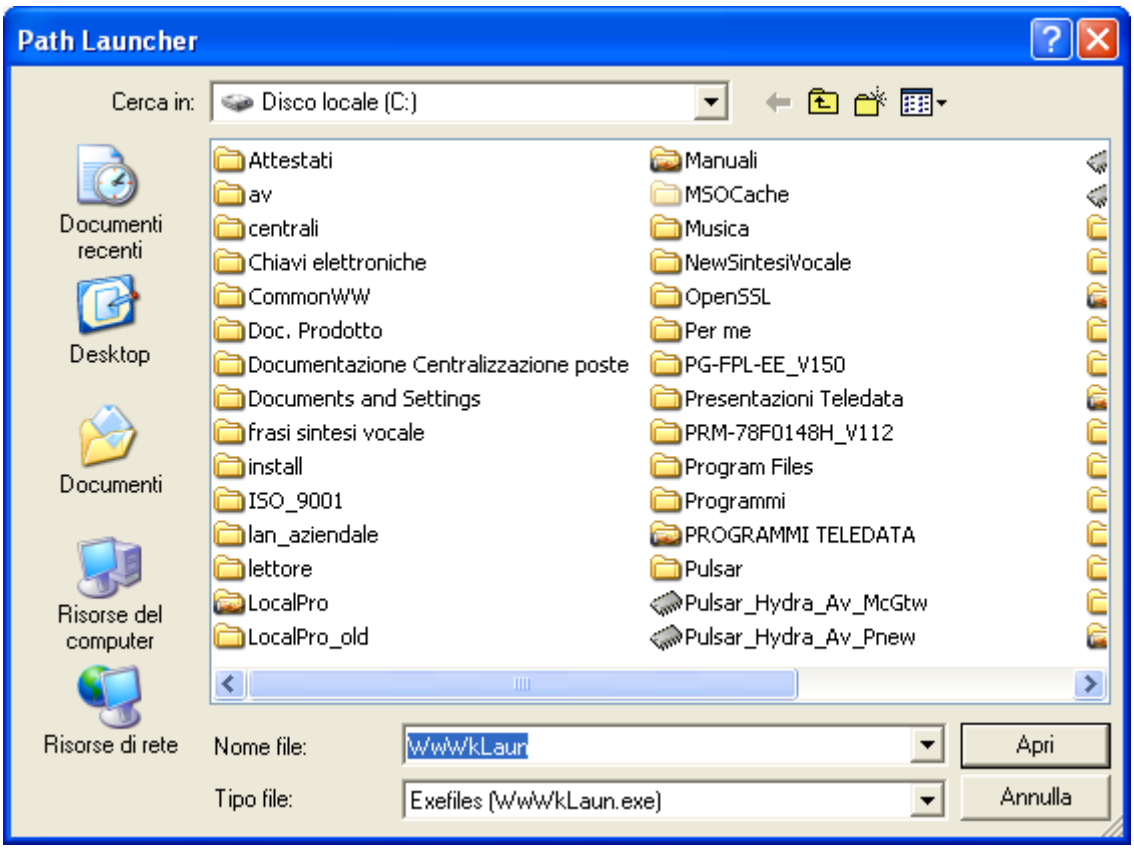
Below right, enable the display options.

Use the buttons *Select All* or *Select none* for a fater setup.

6.5 Configuring a double server

In case the system has two servers (main server and hot backup server, paragraph 1.1.5), it is necessary to share with read and write possibility, the *..\winwatch32* server folder..

Select *Programming → WwWklaun Path*.



In the window appearing, select the position of the *wwwklaun.exe* file, located in the *…\winwatch32* directory, which is shared on the server.

If the main server doesn't function properly, the backup server intervenes that can be used for monitoring the system(more details at paragraph 1.1.5).

6.6 Restoring windows layout

This function positions the windows of the *Winwatch* application back to default position. In this way, the positioning preferences for the windows are lost (paragraph 8.2).

To activate the function, from the main menu select *Programming* → Restore w*indows layout*.

6.7 Language selection

To change the software interface language, select *Language* on the main menu, then choose the desired language among:

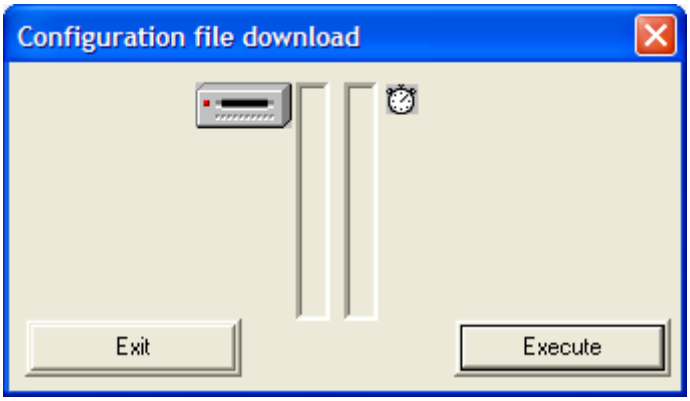
- Italian
- English
- French

7. Setup configuration backup

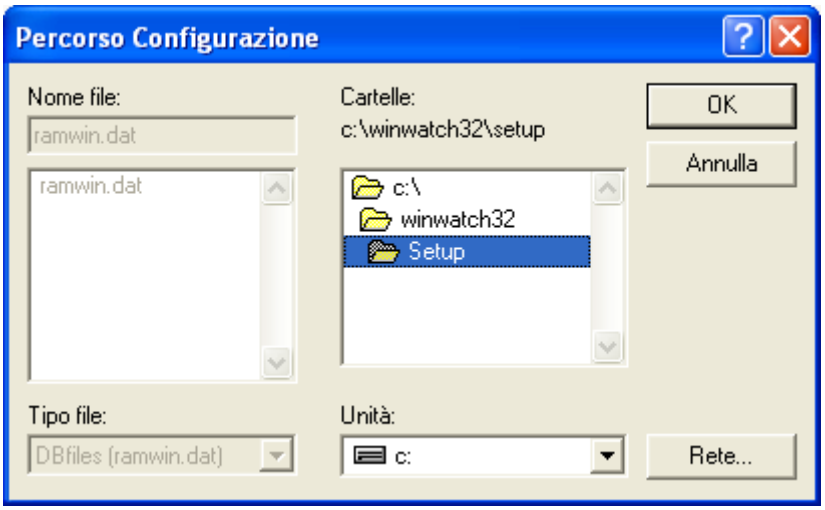
7.1 Creating a backup file

Once all settings have been entered, a backup configuration file can be created, containing such set-points – that is the system configuration – which can be restored in case of emergency.

To do so, from the main menu select *Programming* → *Configuration file download*.



In window *Downloading the configuration files* press key **Execute**.



In window *Configuration Path*, select the directory where you want to save the configuration file containing the current system configuration.

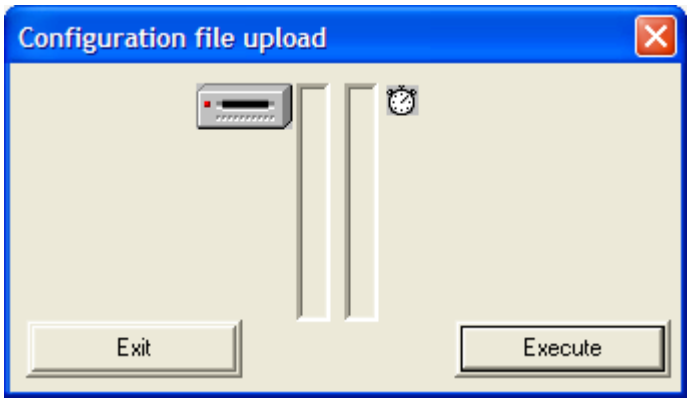
It is suggested, once configuration is finished, to create a backup copy of the entire folder..*Winwatch32* on the hard disk or on to an external device as backup.

7.2 Restoring the backup file

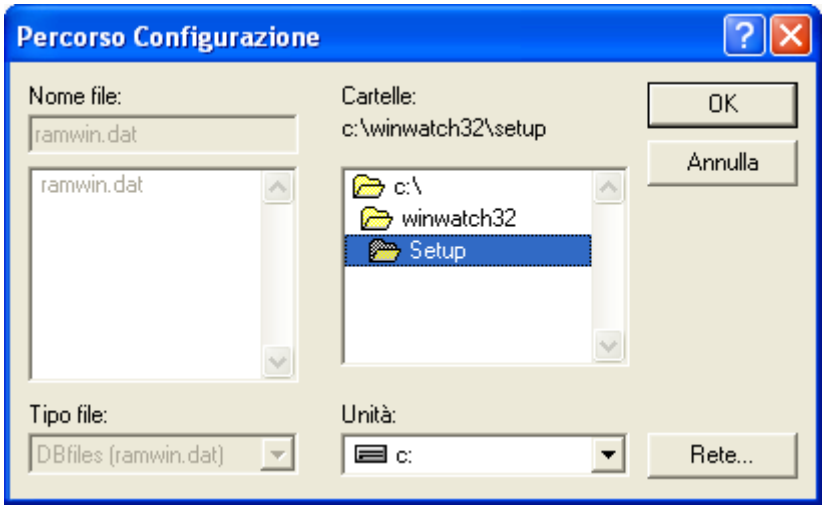
This function allows to upload the settings contained in the configuration file that was produced with the above function (paragraph 7.1).

Once this function is triggered, all the previous setting modifications will be overwritten by the ones in the configuration file.

In the main menu, select *Programming* → *Configuration file Upload*.



Press key **Execute** in the *Configuration File Upload* window.



In the *Configuration Path* window, select the directory containing the configuration file.

If a backup of the ..*Winwatch32* folder was created previously, it is possible to restore the configuration by overwriting the original folder. In this way, the log events will be restored to the backup date.

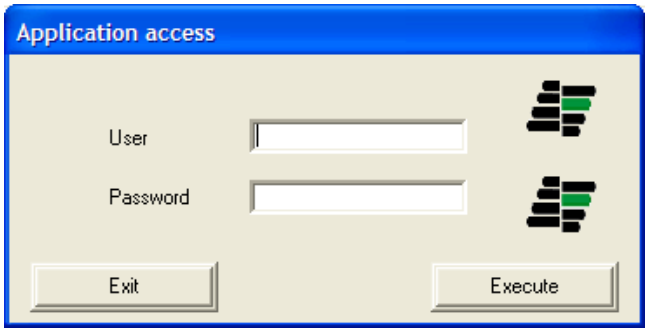
8. Winwatch Interface

8.1 Winwatch Startup

Before starting the *Winwatch* software, make sure you have configured the system correctly by using the *Winwatch Setup* application, as explained in the previous chapters.

Run the *Winwatch* application from the *start* menu of the operating system: *Start* → *Programs* → *Teledata Security* → *Winwatch*.

To enable the use of the software, it's needed to logon: press the key and enter the user name and password in the window appearing on the screen (figure below).



The default user names and passwords are:

- user: *ADMIN1* - password: *ADMIN1*
- user: *ADMIN2* - password: *ADMIN2*

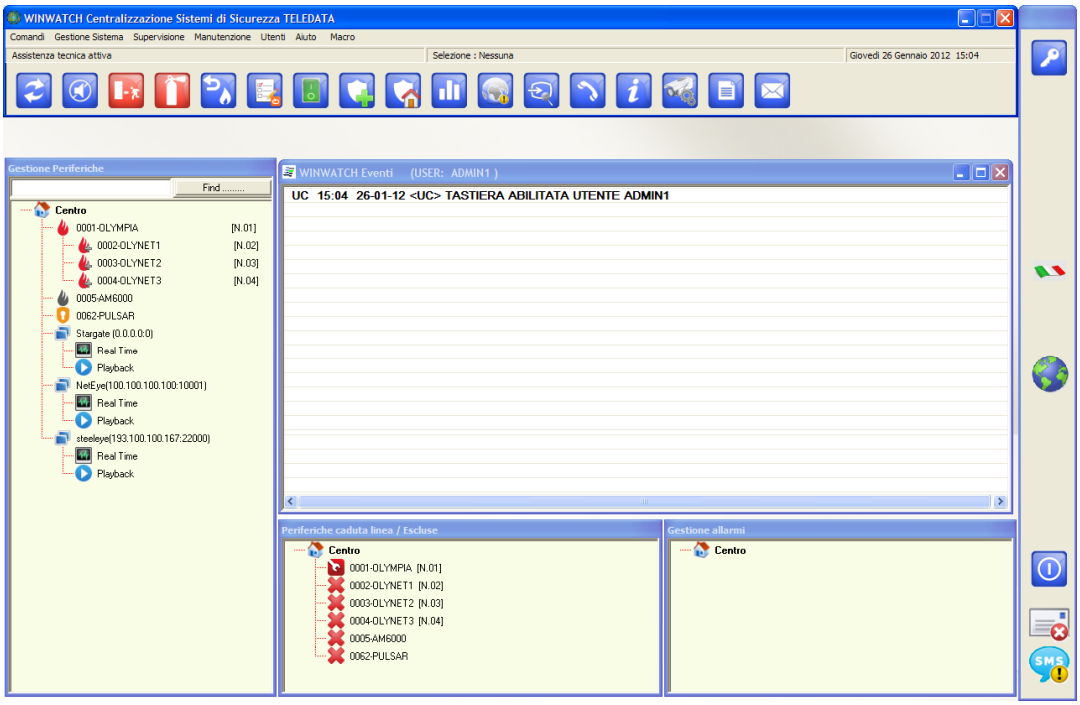
Press key **Execute**.

To change the passwords, refer to paragraph 12.2.4.

To modify or create new users, refer to paragraph 12.2.

8.2 How the windows operate

The software is subdivided into windows, each with its own function.



At the first start up, it is possible that the windows are laid out as shown above. The user can position the freely the masks for an easier use.

The following paragraphs describe the functions of the various windows.

8.2.1 Control icons

This window presents the following function keys:

It enables / disables the user. If disabled, it will not be possible to send commends to the system (paragraph 8.1).

This key, available only with the built-in *Standard Serchio*, reduces the *Serchio Controls* window to icon (paragraph 8.2.7).

This key, available only with the built-in *Standard Serchio,* shows the status of the connection to the access monitoring scanners (paragraph 8.2.8).

Shows the current language, set in the *Winwatch Setup* (paragraph 6.7).

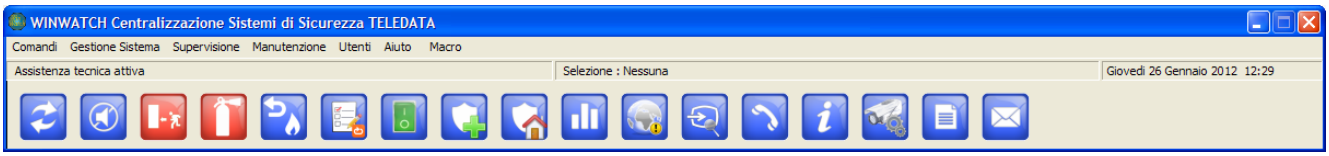
It shows the main map (paragraph 5.3).

It closes the *Winwatch* application and returns to the operating system.

It shows whether the E-mail function is enabled or not (paragraph 10.5).

It shows whether the SMS function is enabled or not (paragraph 10.5).

8.2.2 Commands



With this window it is possible to send commands and open the main functions of the software *Winwatch*. They are distributed over 4 pull-down menus (*Controls*, *System Management*, *Supervision* and *Maintenance*).

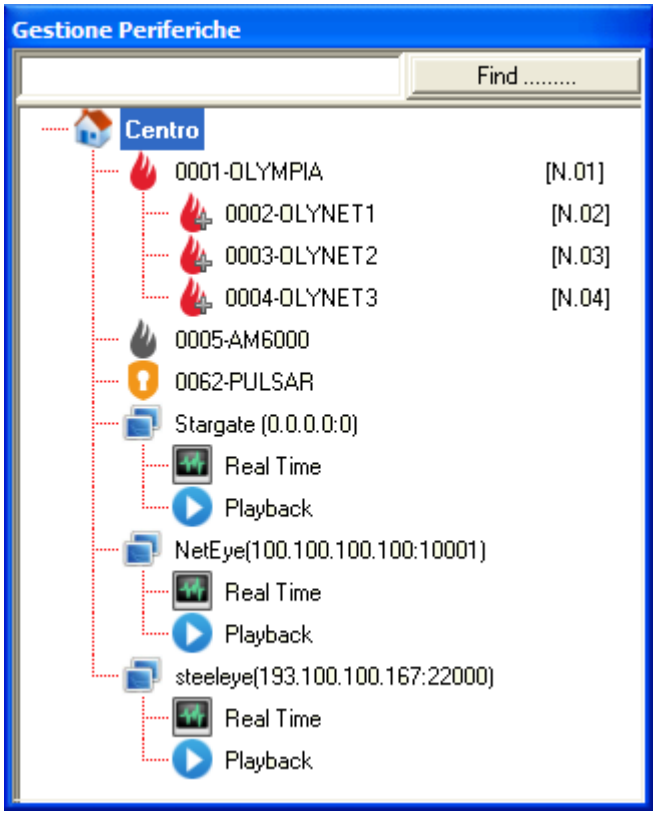
The main commands can be also called through the 16 direct keys.

All the functions that can be called through the control keys can be also called through the pull-down menus.

The following table shows the list of the function keys, each with a short description, the path for calling the same function through the pull-down menu, as well as the reference paragraph for a more in-depth description.

Key	Command	Pull-down menu path	Reference
	Alarms acknowledgment	Command → Alarms acknowledgment	9.5.1
	Relay silencing	Command → Relay silencing	9.5.2
	Evacuation fire	Command → Evacuation fire	9.5.3
	Fire confirm	Command → Confirm fire alarm	9.5.4
	Double crossing / Reset fire central unit	Command → Reset double crossing	9.5.5
	Autotest / Reset fire loops	Command → Selftest peripherial	9.5.6
	Activate relay	Command → Remote controls relay	9.5.7
	Connect / Disconnect inputs	Command → Connect / Disconnect input	9.2.2
	Connect / Disconnect areas	Command → Connect / Disconnect area	9.2.1
	Unit status	Supervision → Look peripherial condition	11.2.1
	Display maps on alarms	Supervision → Look alarms status	11.2.1
	Display disconnected inputs	Supervision → Look disconnected inputs	11.2.2
	Telephone commands	Command → Control on phone line	9.3
	About peripheral	Supervision → Look peripheral informations	11.4.6
	Setup DVR	Supervision → Setup VideoSpy	10.2
	Videospy Alarms / Videospy Logs	Supervision → VideoSpy Alarms	11.4.7
	Send an e-mail to a client	Not present	10.5

8.2.3 Management Peripheral



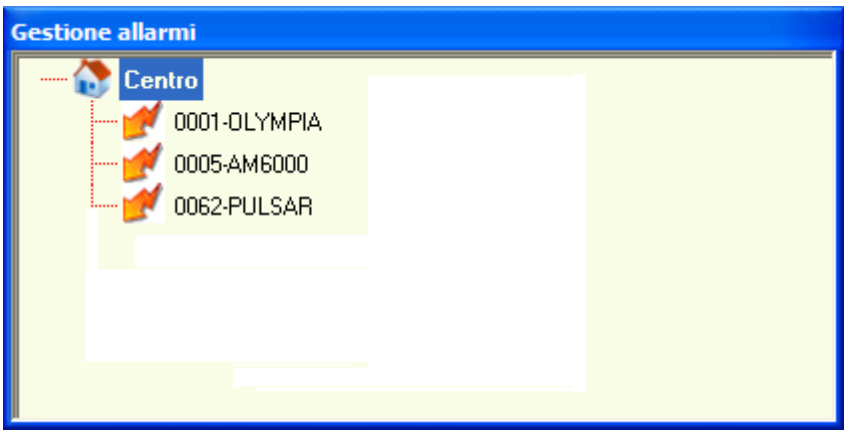
This window shows, with different icons, the control units connected to the system:

The icon next to the name changes according to the type of unit:

- for the fire alarm units;
- for the OlyNet fire alarm units;
- for the Notifier fire alarm units;
- for the burglar alarm units;
- for the CCTV units.

If a command is active (paragraph 9.1.1), by clicking twice on the units name the command is sent to itself.

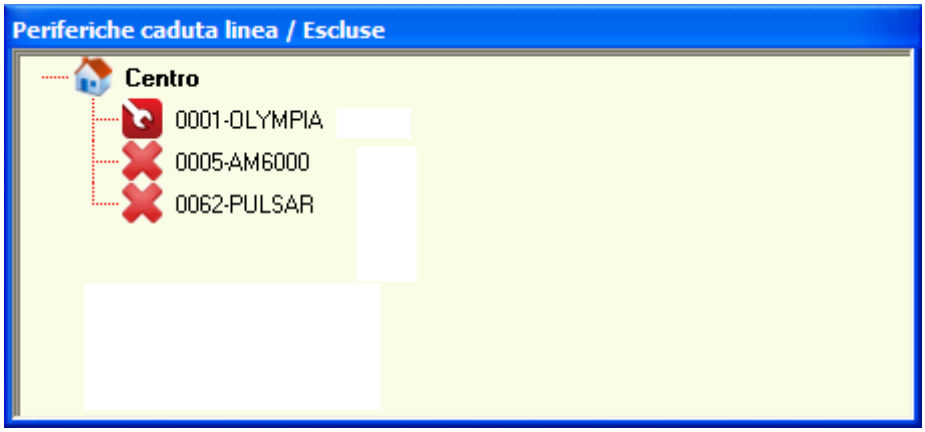
8.2.4 Alarm Management



This window shows the list of units in which an unacknowledged alarm is present. By clicking twice on the station name, the list of all current alarms appears.

Remove as soon as possible the causes for the signalled alarms, and acknowledge them to delete the the alarm signal.

8.2.5 Peripheral devices: power supply failure / off

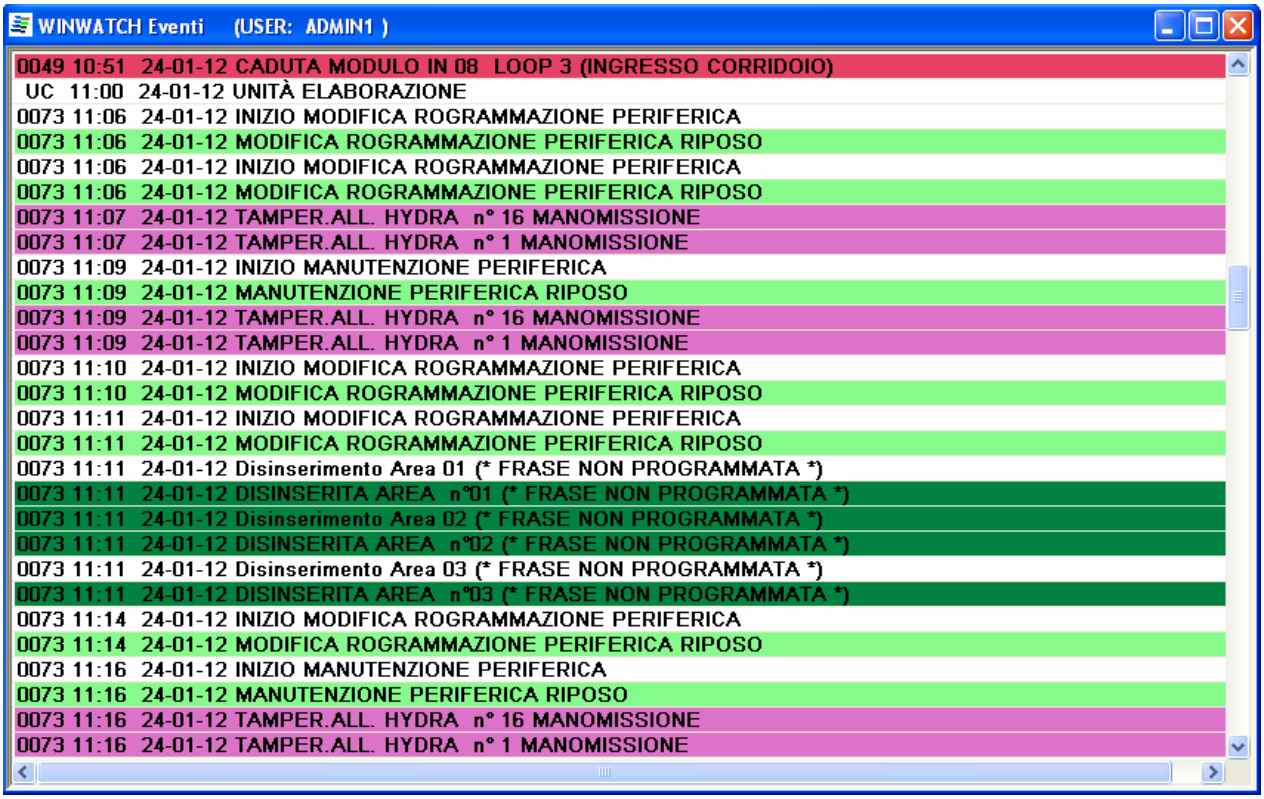


This window shows the unit that have connection problems with the supervision centre and the units that have been excluded by the user:

- Unit excluded (paragraph 10.3)
- Unit TCP/IP non active
- Unit drop line

It is important to remove the cause for the line drop and restore the connection to the supervision centre.

8.2.6 Events window



This window shows the events occurred, the commands sent and the status indications coming from the stations connected to the system.

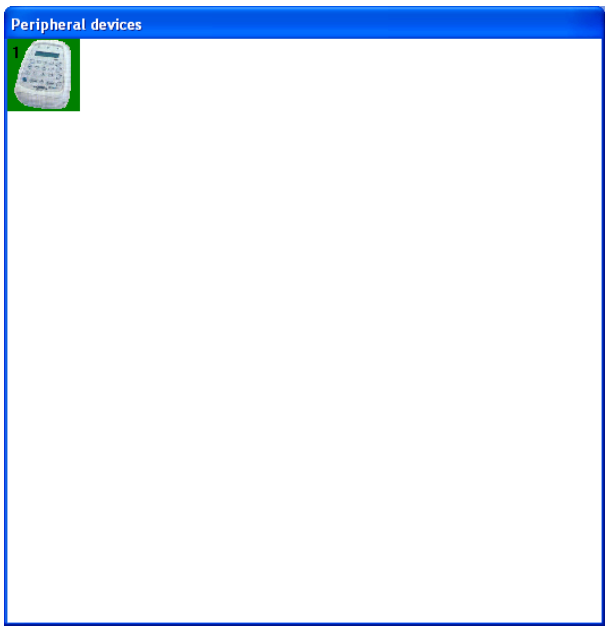
The first column displays the number of the unit involved, followed by the date and time of occurrence of the event, and by the corresponding message.

The events colour is freely programmable (paragraph 12.1.5)

8.2.7 Window of Standard Serchio controls

This window, active only if the *Winwtatch* version with built-in *Standard Serchio* is installed, is used for calling the access monitoring control. For more information, please refer to the *Standard Serchio* software manual.

8.2.8 Linkage status of access control stations



This window shows the status of the access control units. The background colour indicates the status of the reader:

- Dark green: enabled (it accepts the programmed cards only);
- Pale green: always enabled (it accepts any card);
- Red: not enabled

8.3 Changing the layout of windows

The windows can be relocated on the screen in different positions than originally preset. To do so, click the left mouse-key on the blue bar containing the name of the window (for example *Peripheral management*) and drag the window to the desired position.

The layout of windows is stored: upon starting the software, every user will find the windows arranged again at the same point where he/she had left them during the previous session.

To restor the windows to their originally preset location, just call the specific function through the *Winwatch Setup* software (paragraph 6.6).

9. Operative commands

This section of the manual explains how to call the commands and operative functions of the *Teledata* burglar and fire alarm units.

For further information on the operative commands and functions of each unit, refer to itself installation and operative manual.

9.1 Sending a command through the pull-down menu

9.1.1 Command activation

To activate command, or call one of the available functions, select it in the pull-down menu or click the left mouse button on the corresponding function key (if available) in the *Commands* window.
The command remains active until another command is called; in this case, the last called command will be active and displayed at the point indicated in the status bar.

The command is deactivated automatically after a continued non-usage of the system (keyboard disabled) or after a user logout..

9.1.2 Sending a command

Once a command is activated, it can be sent to one or more units.

To do this, double click the left mouse button on the units involved, in window *Peripheral management*.

If the sent command requires more information to be performed, a window will appears where extra information has to be inserted. Otherwise, the command will be activated immediately.

For every command sent, the system always emits a confirmation phrase if the command is correctly performed, or an error if for any reason in was not possible to sent the command itself.

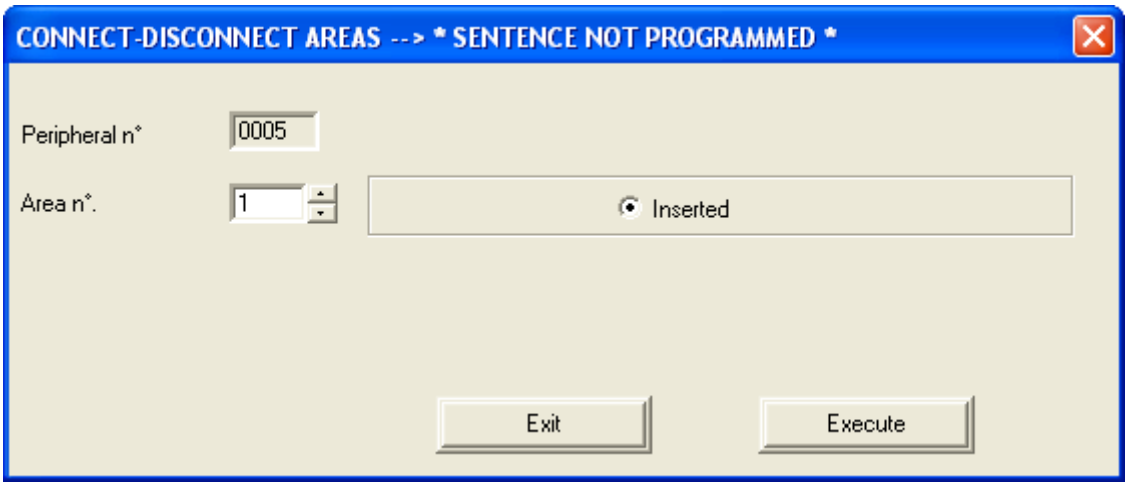
For example, when the alarm acknowledgement is sent to fire alarm unit, the following message appears: *ACKNOWLEDGMENT FAILED: COMMAND NOT AVAILABLE.*

9.2 Detectors and areas

To define the *geographic areas* and for more information about arming, disarming, including and excluding geographic areas and inputs, please refer to the unit's programming manual.

9.2.1 Connect-disconnect areas

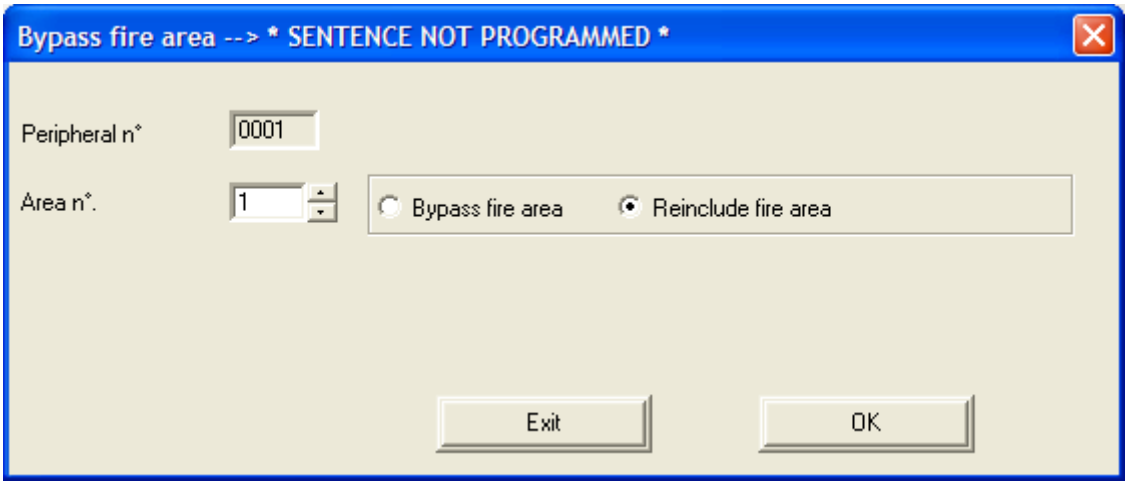
If sent to a burglar unit, this command, called via key allows to arm/disarm the geographic areas defined in the involved unit.



In the window appearing (previous figure), enter the following information:

- By using the arrow keys, set the area number in field *Area n°*.
- Select the desired status: *Not inserted* or *Inserted*.
- Press **Execute**.

If sent to a fire detection unit, this command will allow to exclude/include a geographic area defined in the involved unit.

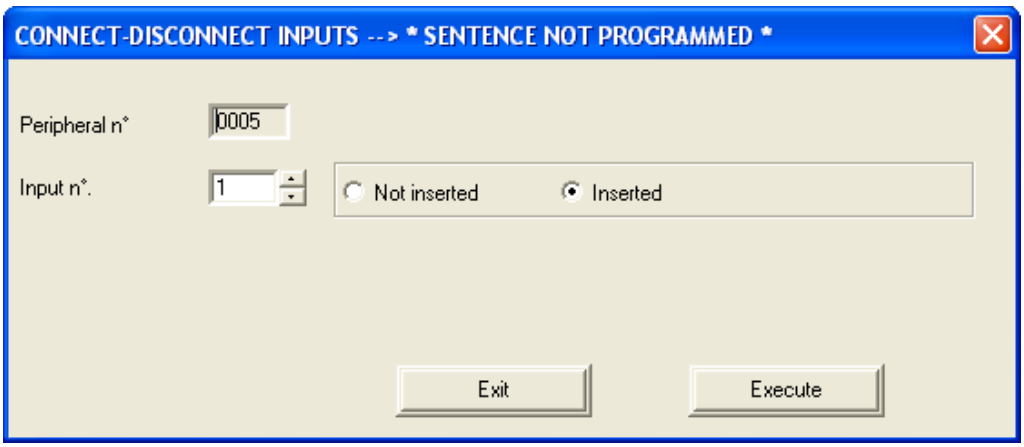


In the window appearing (previous figure), enter the following information:

- By using the arrow keys, set the area number in field *Area n°*.
- Select the desired status: *Bypass* or *Reinclude*.
- Press **Execute**.

9.2.2 Arming and disarming inputs

Feasible only on burglar alarm units, this function, called by pressing the key , allows arming and disarming the individual peripheral devices connected to the involved unit's inputs.



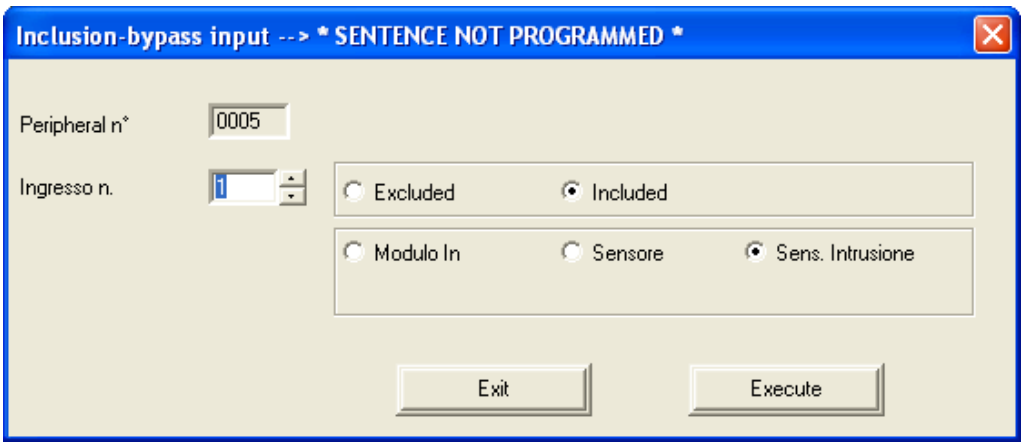
In the window appearing (previous figure), enter the following set-points:

- By using the arrow keys, enter the input number (same as set in the station) of the detector or other peripheral device in field *Input n°.*
- Select the desired status: *Not inserted* or *Inserted*.
- Press **Execute**.

The command is not feasible for fire detection and CCTV units.

9.2.3 Inputs inclusion and exclusion

This command, selectable from pull-down menu *Commands* → *Inclusion/Exclusion of Inputs*, allows to include or exclude burglar inputs and also peripheral fire alarm devices controlled by the selected burglar alarm unit. It also allows to include and exclude detectors and modules of fire detection units.



If activated on a burglar unit, the previous window will appear. Enter the following data:

- Select the number of the peripheral device's input in field *Input n°*.
- Select the desired status: *Excluded* or *Included*.
- Select *Sens. Intrusione* if the detector is a burglar type, select *Modulo In* or *Sensore* if the device is a fire detection type device (expects that in the unit there is installed a dedicated expansion card, called *SFIRE*)
- Press **Execute**.

On burglar units it is possible to exclude fire detectors and modules, that expects that a dedicated expansion card, called *SFIRE* is installed. For more information, refer to the user manual of the unit itself.

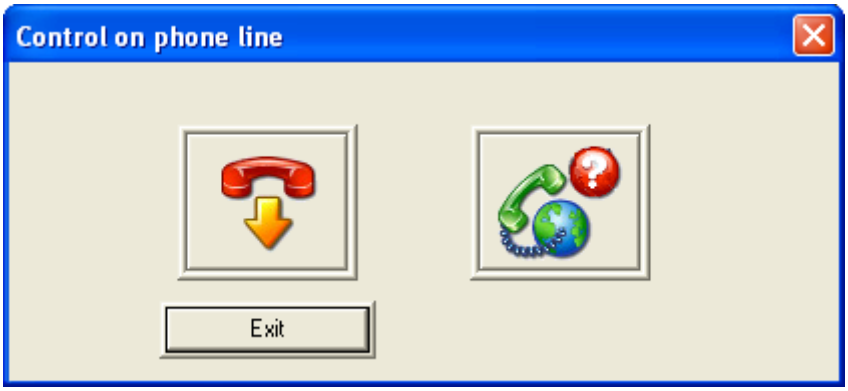
If activated on a fire alarm detection unit, this function allows to exclude or include the individual fire detectors or the modules connected to the various loops.

In the window appearing (previous figure), enter the following set-points:

- Select the number of the detector or of the module in field Element *number*.
- Select the type in sub-window **1**: *Modulo In* (input module), *Modulo Out* (output module) or *Sensore* (fire detector).
- Select the desired status in box **2**: *Excluded* or *Included*.
- Select the test mode in box **3**
  - *Exclusion*: device exclusion/inclusion
  - *Test*: activates the test mode for detector diagnostics.
  - *Walk test*: the device's alarm will be viewed will have no consequences on the system.
- Press **Execute**.

9.3 Control on phone line

This command, called by pressing the key , allows end the current digital telephone conversation with the selected unit or to send the test of the backup line between the monitoring station and the selected unit.



In the page now appearing there are two function keys:

If the LAN line it is not active and a telephone connection is in progress with the unit, it stops the telephone connection.

It sends a test command that deactivates the connection through LAN and forces a test call to the monitoring station.

9.4 Videocamera management

Call the *Commands* → *TVCC Management* function from the pull-down menu, and select one of the following functions:

- *Camera on Monitors*: shows on display the real-time of a a video camera connected to the unit.
- *Activate Sequence*: shows a video sequence set in to the unit.

These functions can be activated only for *Vicon* and *Comerson* CCTV stations.

9.5 Various commands

9.5.1 Alarm acknowledgement

This command, called by key , erases all alarm signals on the monitoring station and on all the burglar units under alarm; as a result of the command, all the detectors that triggered the alarm are reset. It will silence also the audio card/buzzer of the monitoring centre.

This function doesn't remove the physical cause that generated the alarm. Once the detectors are reset, if the alarm persists, a new alarm signal will be sent to the monitoring centre.

9.5.2 Relay de-activation

This command, called by the key  , resets all the relays activated by an alarm to the control unit to witch is sent to. It will silence also the control unit and the remote repeater internal buzzers.

9.5.3 Fire evacuation

This command called by the key  , activates all the sirens/outputs programmed as evacuation in a fire detection control unit.

This command can be sent only to control units model *Olympia* and will be accepted only if the unit has active alarms.

9.5.4 Fire confirm

This command called by the key  , sends a fire confirmation command, after a manual checkout of the fire presence. it will activate all the programmed sirens/outputs.

This command can be sent only to control units model *Eolo* and will be accepted only if the unit has active alarms.

9.5.5 Double crossing reset / Reset fire central unit

This command, called by the key  , has the effect as explained below:

- If sent to a burglar alarm unit, it resets the counter of double crossing alarms on the unit with it is sent to;
- If sent to a fire alarm unit, it performs a general reset: it acknowledges the alarms and restores all the detectors and modules.

9.5.6 Autotest / Reset fire loop lines

This command, called by the key  , has the effect as explained below:

- If sent to a burglar alarm unit, it checks the unit's memory.

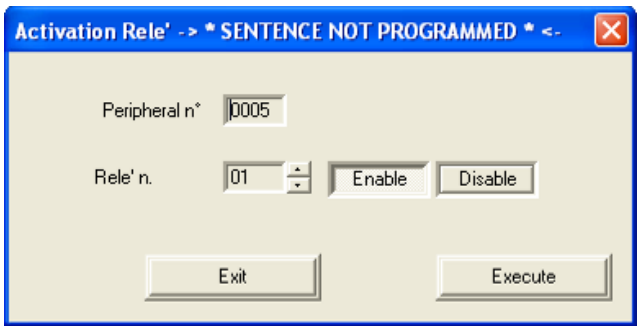
Performing this test is recommended, if it is presumed that the unit doesn't function correctly.

- If sent to a fire alarm unit, all loops are reset: it interrupts and restores for a brief time the communication between the unit and the modules and detectors connected through the various loops.

9.5.7 Activate relay

This control, called by the key  , has different functions, depending on the control unit:

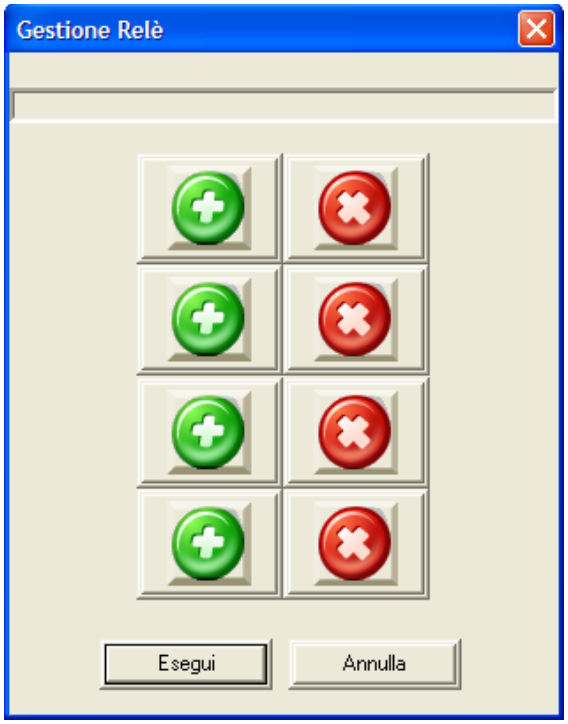
- If the command is sent to a burglar unit, this will allow to activate or deactivate a relay of the unit itself.



In the window appearing enter the following set-points:

- Select the relay number (same as set in the unit) in field *Relay n°*.
- Select the desired status: Enable (activated) or Disable (deactivated).

- If the command is sent to a fire detection unit, it allows to set the status of the internal relay of the unit itself.



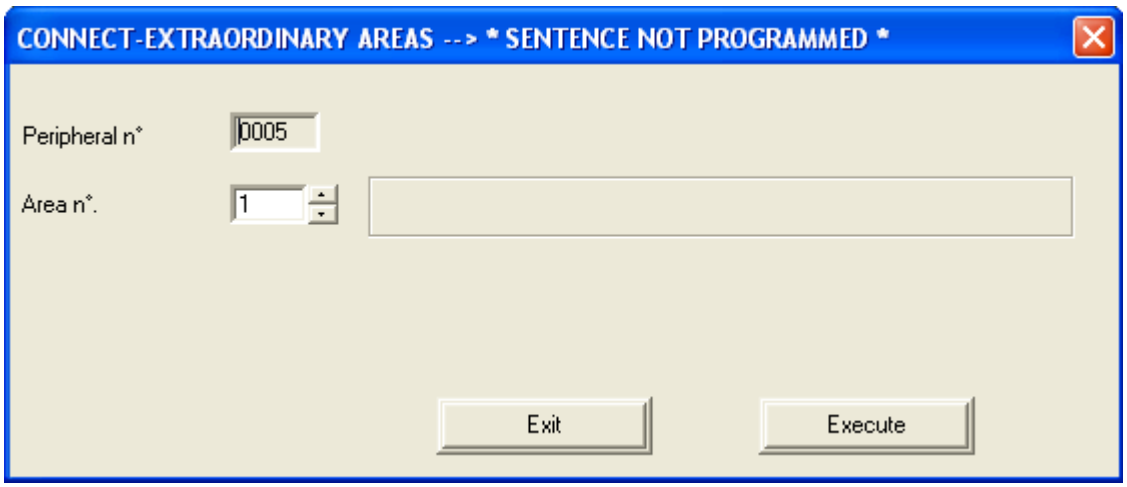
In the window appearing enter the following set-points:

- Selecting the first couple of keys it will be possible to include or exclude the monitored relay n°1 of the unit (usually used for fire signaling).
- Selecting the second couple of keys it will be possible to include or exclude the monitored relay n°2 of the unit (usually used for fire signaling).
- Selecting the third couple of keys it will be possible to include or exclude the siren relay of the unit (usually used for fire signaling).
- Selecting the fourth couple of keys it will be possible to silence or rearm the siren relay of the unit (usually used for fire signaling).

9.5.8 Adding the overtime

This command, selectable from pull-down menu *Commands* → *Connect Straordinario*, delays the automatic arming respect to the set daily bands, of the selected area by 30 or 60 minutes (depending on how the unit is configured)

For more information on the daily bands for arming and disarming areas, on activation and duration of the overtime, please refer to the programming manual of the unit involved.



In the window appearing (previous figure), enter the following set-points:

- Select, in field *Area n°*, the number of the area to which overtime is to be assigned.
- Press **Execute**.

10. Special functions

10.1 Programming the burglar alarm units

To modify the settings of a burglar alarm and a fire detection unit, recall the function *System Management → Programming Peripheral*. The *Winlocal* software is opened for programming the unit.

For more information about programming burglar alarm and fire detection units, please refer to the installation and operation manual of the software *Winlocal* and the operative manuals of the units..

Once programming is completed, you should call function *System Management → Send Peripheral Programming* so that the configuration is sent to the unit.

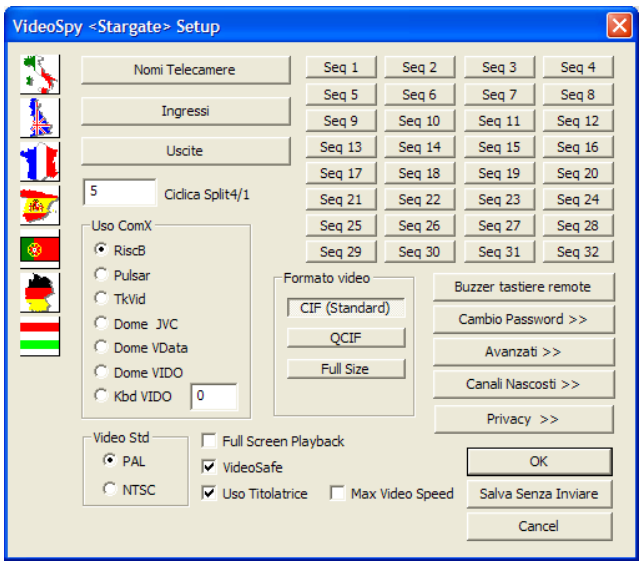
The following functions are available:

- *System Management → Verify Programming*: it checks that there have been no variations between the set configuration and the current one in the unit.
- *System Management → Download Programming*: it downloads to the monitoring centre the configuration set in the unit.
- *System Management → Print Programming*: it displays on screen and prints the configuration of the selected unit.

10.2 Programming the CCTV units

To configure the units *VideoSpy*, *Phantom* and *Stargate* or the cameras names, press the key in the *Commands* window.

The configuration of *Sentinel* units cannot be programmed remotely: use the software delivered with the unit or *Winlocal* software.



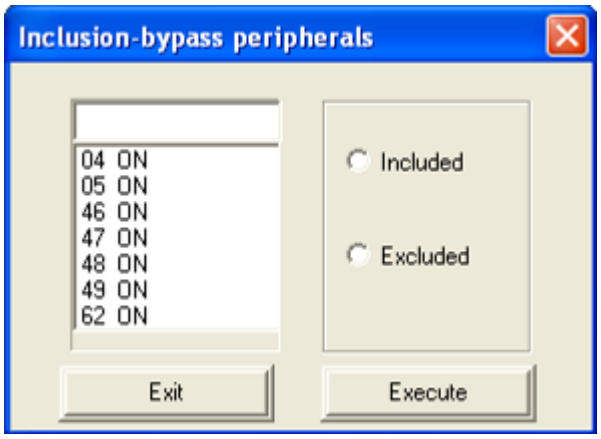
In the window now appearing (previous figure), enter the following set-points:

- Select Nomi Telecamere and modify them.
- Set the other parameters if necessary.
- Press **OK** to exit saving and sending the configuration to the video unit..

Per maggiori informazioni sui singoli parametri presenti nella figura precedente, fare riferimento al manuale di programmazione della periferica stessa.

10.3 Exclusion and inclusion of units

For excepting one or more stations from the entire system, select function *System Management → Inclusion-bypass peripherals.*



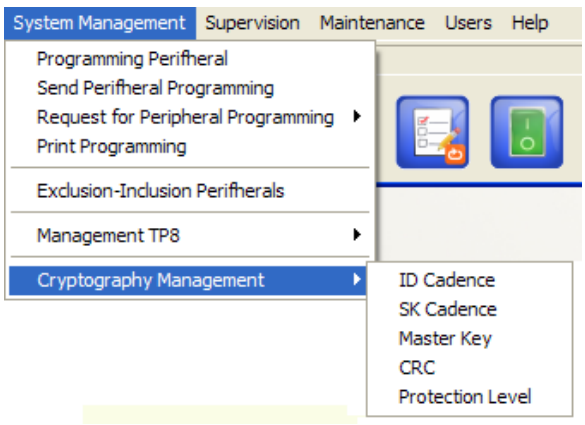
In the window now appearing enter the following set-points:

- Select, the unit number in the list on the left
- Select the desired status: *Included* or *Excluded*.
- Press **Execute**.

Excluding a unit means interrupting the communication between the unit and the monitoring centre. It doesn't deactivate the unit itself, that will continue to work locally in autonomous.

10.4 Cryptography Management

In order to set the parameters for connection with the unit through the CEI/ABI protocol with a cryptography level 2, select function *System Management → Cryptography Management*.



The following functions are available :

- *ID Cadence*: setting the frequency of the identification procedure.
- *Switch Key Cadence*: setting the frequency of switching of the cryptography key.

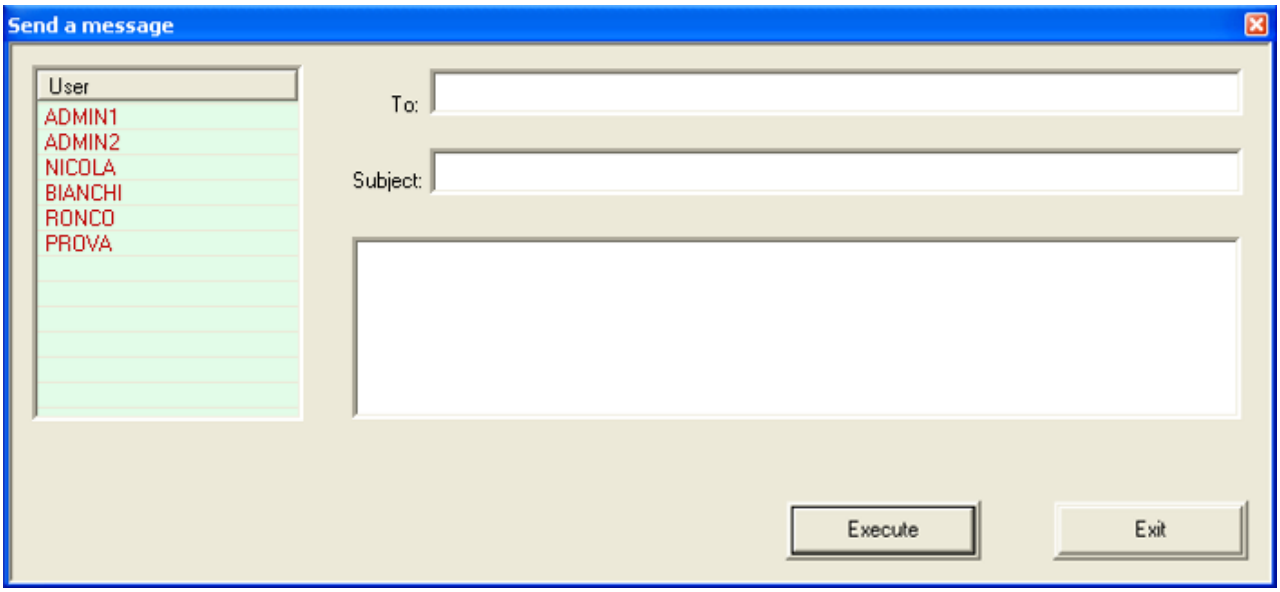
- *Master Key: setting the master key for cryptography.*

Set the same master key on all the units connected to the monitoring centre.

- *CRC configuration*: selection of the calculation method (CRC2 or CRC16).
- *Protection Level configuration*: choose the level protection (in clear, with authentication or cryptographed).

10.5 Sending messages

To send a message to a user or to another unit, press the key.



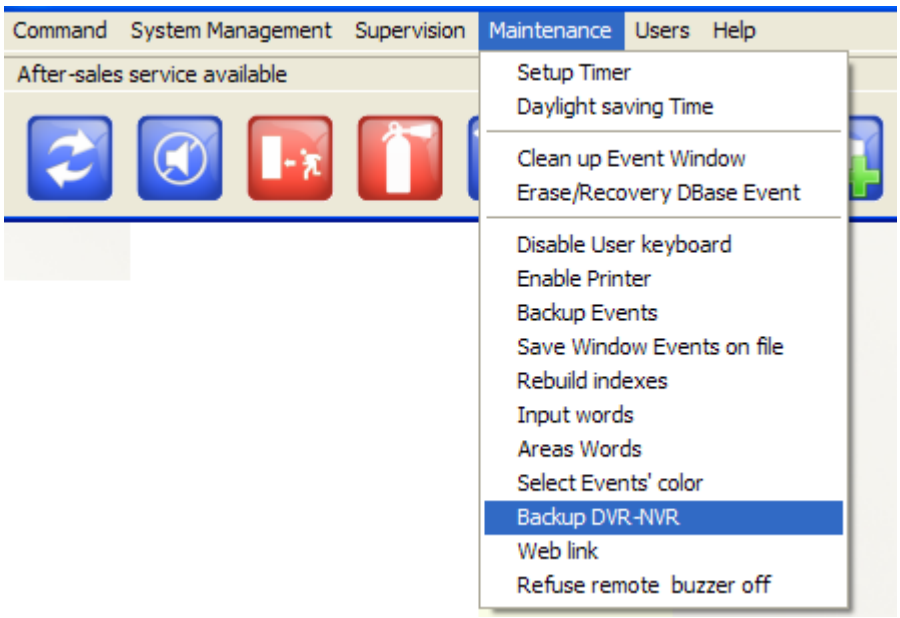
Proceed as follows:

- Double click on the name of the user to whom the message is to be sent (list on the left hand side).
- Write the subject of the message in field *Subject*.
- Write the message text in the field underneath.
- Press **Execute**.

The message will be read by the user at the next login.

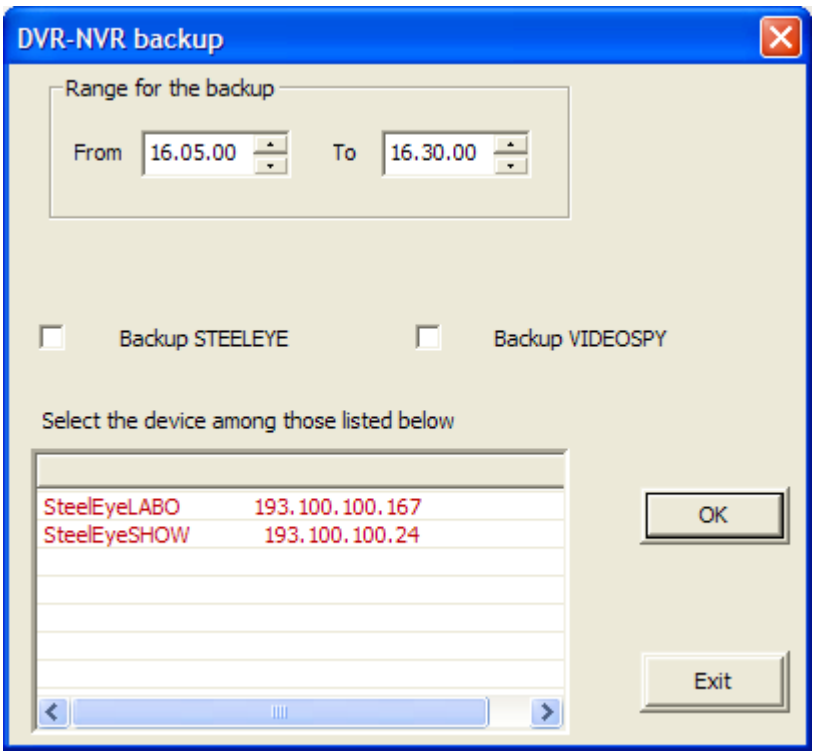
10.6 Backup video recording

It is possible to backup the video recordings of DVR model VideoSpy, Nettuno, Stargate and SteelEye. Recall the function from the pull-down menu *Maintenance → Backup DVR-NVR*

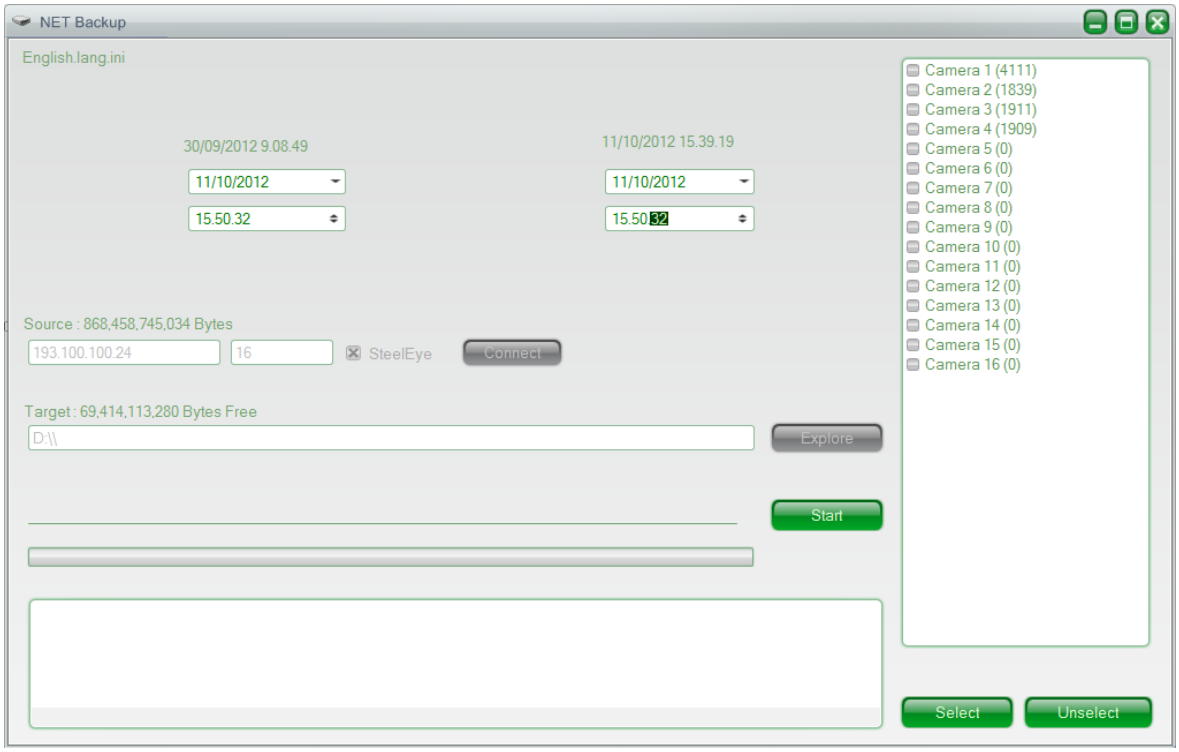


In the window that appears (window below) configure these settengs:

- If the DVR is a **SteelEye** model, check the flag *Backup STEELEYE*, select the desired DVR in the table below, and press **OK**.
- If the DVR is **VideoSpy**, **Nettuno** o **Stargate** model check the flag *Backup VIDEOSPY* and the time range (minimum 5 minutes) where the system will download the images selected in the next step. Press **OK**.



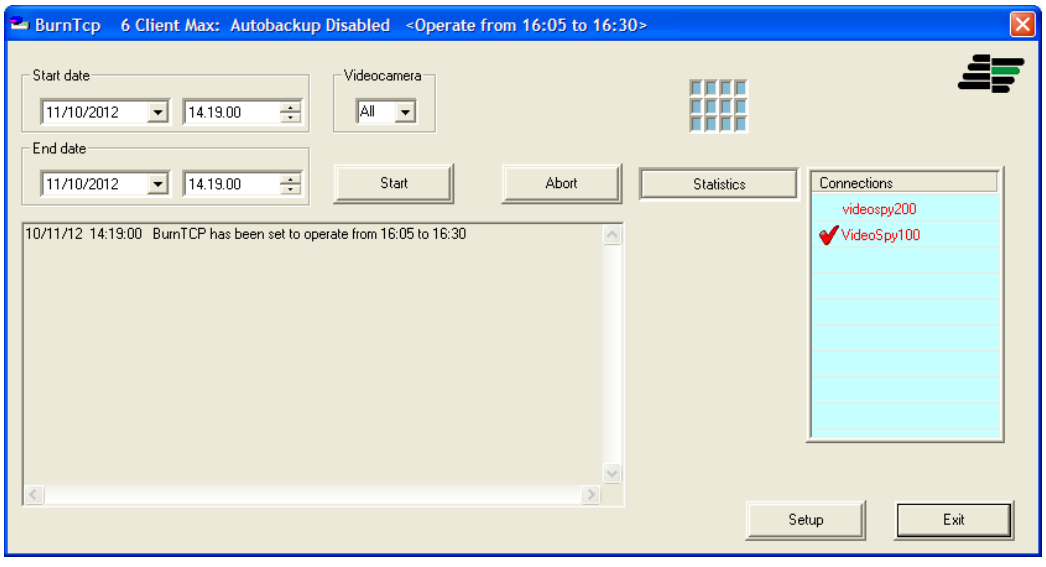
If the video unit is a *SteelEye* model, after confirming the path where the files will be copied, the following window will appear:



Proceed as follows:

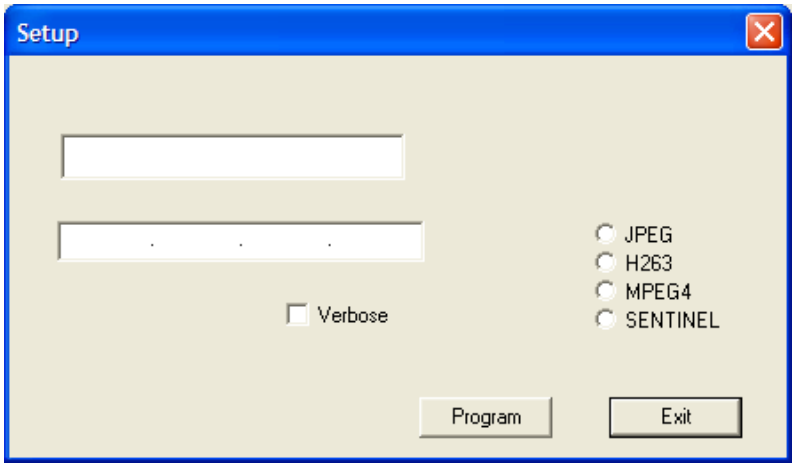
- Double click on the desired cameras. It is possible to backup single cameras or do a multiple selection.
- Select the start (on the left) e fine (on the right) period by inserting the date and time of the necessary recordings..
- Press the key **Start** and wait the conclusion of the backup before exiting.

If the video unit is a *VideoSpy, Nettuno o Stargate* model, after confirming the path where the files will be copied, the following window will appear:



Proceed as follows:

- Click on the key **Setup**.
- Insert the DVRs Name and IP address.
- Set the recording format.
- Press the key **Program.**
- Repeat the operation for all the DVR that require backup.



Returning to the main window of *BurnTCP*, set the start and end date and time of the reqired recordings and select the single camera or all from the pull-down menu..

Double click the interessed video unit. The symbol ✔ qill appear infront of the unit.

For the DVRs *SteelEye* model, the backup will start immediately. For the other DVRs models if the backup was not completed in the programmed range time, the backup will restart automatically as soon as the time is in the range.

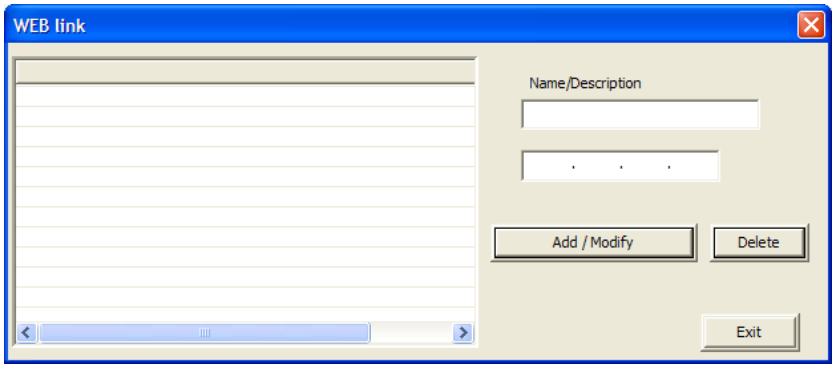
If the backup is not completed in the programmed range time, to ensure that it will restart automatically as soon as the time is in the range, it is important that the software *BurnTCP* is not closed.

10.7 Web link management

It is possible to add in the peripheral list a web link.

This functionality allows to integrate and interact with any LAN device that can have a connection on port 80 thouw internet browser (es. DVR su TCP/IP).

Call the functionality fron the pull-down menu *Manteinance → Weblink Management*



To add a web link proceed as follows:

- Insert a name in the field Name/Description.
- Insert the relative IP address of the device.
- Click on **Add/Modify**.
- Repeat the procedure for all the devices that are required.
- Press the key **Exit.**.

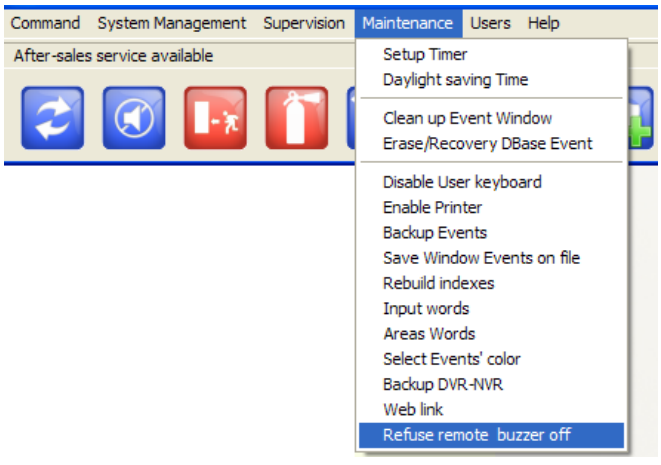
To modify or delete a web link, proceed as follows:

- Click on the device in the list on the left.
- Modify the parameters and click on **Modify**.
- Click on **Delete** to delete definitly the device.

10.8 Buzzer management in server/client systems

In case of systems with server and client, it is possible to manage the buzzers in autonomous o synchronized mode. If set in autonomous mode, each terminal will need to silence their own buzzer. If set as synchronized, the silencing of the buzzers will be generalized for all the system and all the terminals.

To set the buzzer management, call the functionality from the pull-down menu *Manteinance → Refuse remote buzzer off* where, if flagged the buzzer management will be autonomous. Differently, if the function is not flagged, the buzzer management willl be generalized for all the system.



11. Monitoring the system

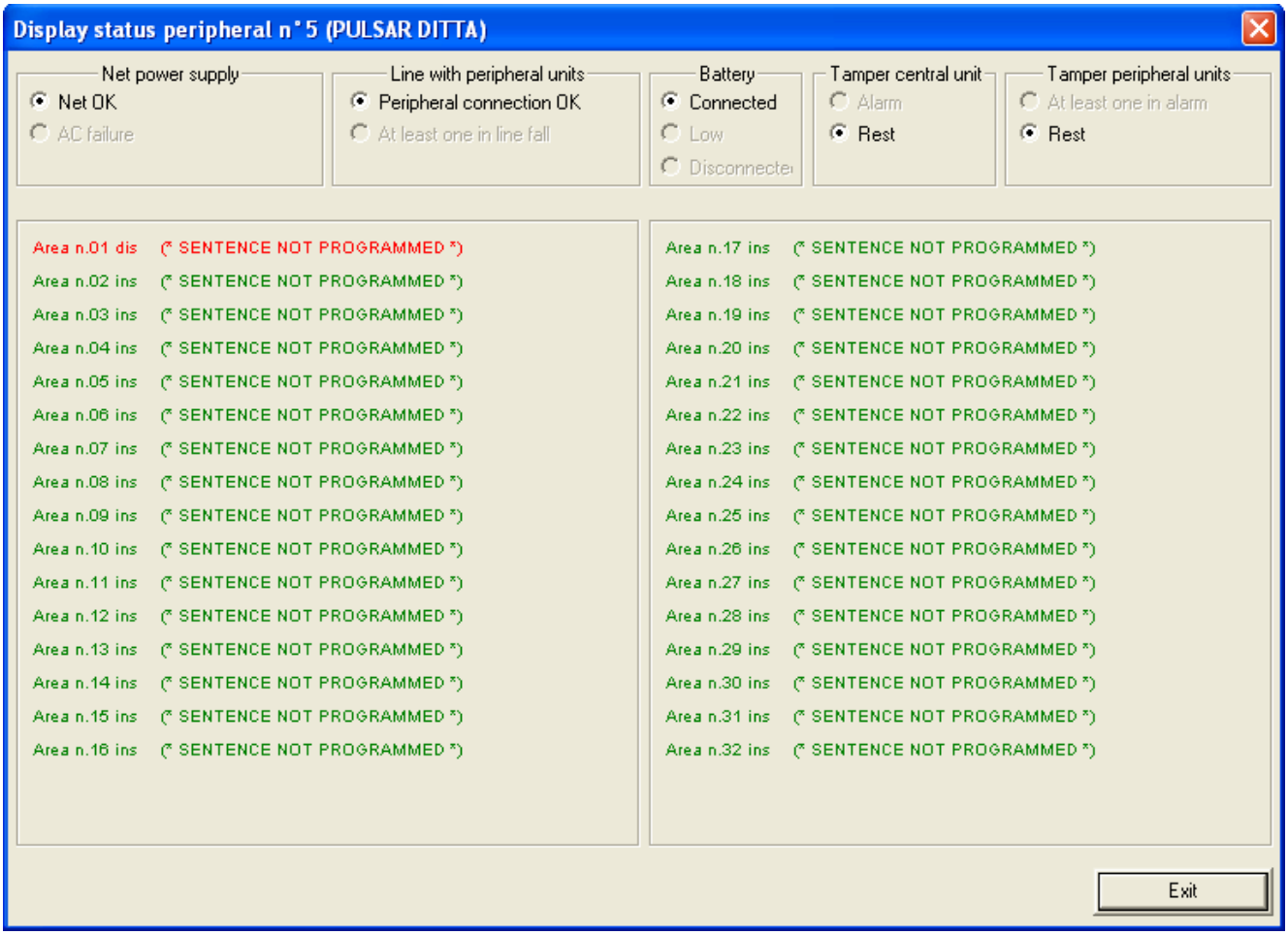
11.1 Introduction

The following paragraphs describe the procedures and monitoring functions of the system by the *Winwatch* software.

11.2 Status of stations, sensors and areas

11.2.1 Peripheral devices status view

Calling the function through the key  the following figure will appears where the statuses of the selected unit are shown.



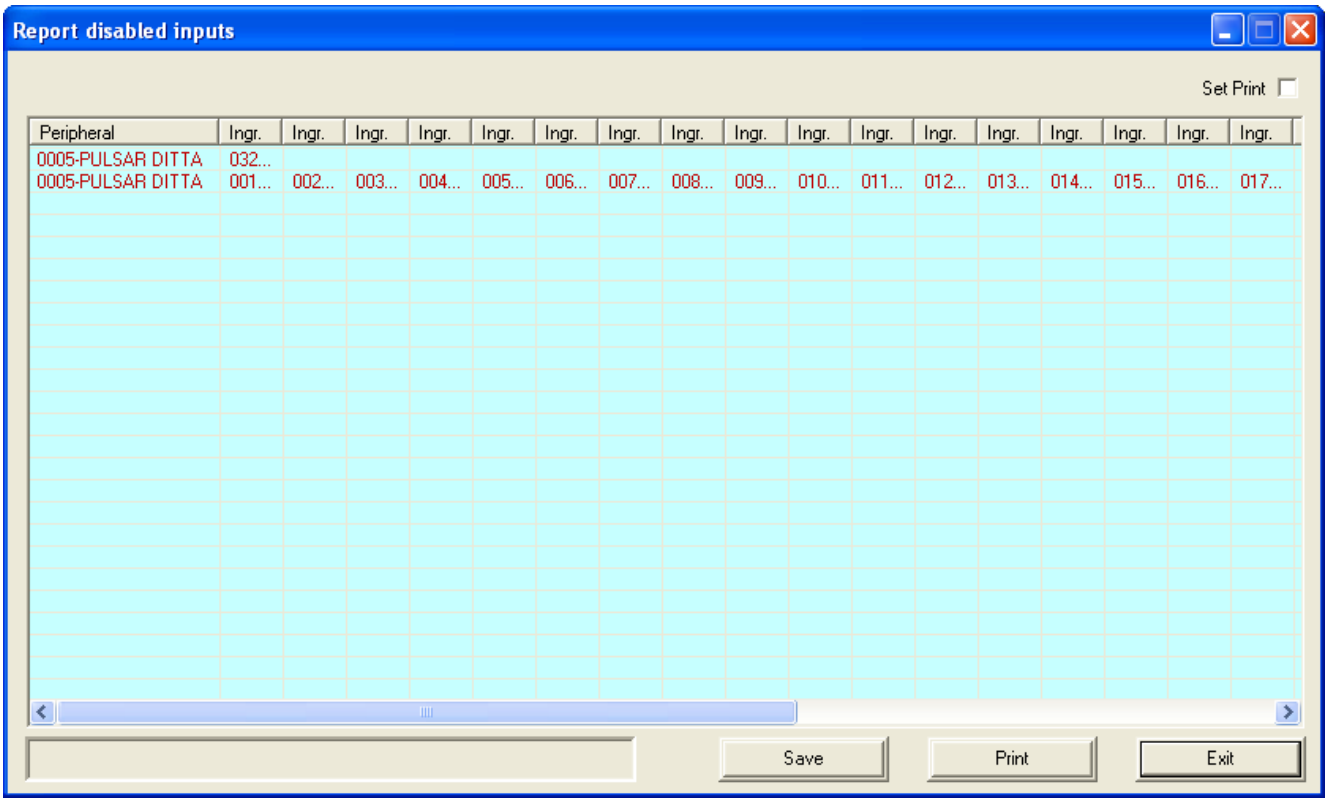
- Status of the areas, where red = off and green = on.
- Connection status with the peripheral devices: all connection OK, or at least a device in bad connection
- Battery condition: connected, low or disconnected.
- Unit tamper status: rest or alarm

- Peripheral devices tamper status: rest or at least a device in alarm.

This window shows all the possible areas, non only the selected ones. The command will be accepted only by burglar alarm units.

11.2.2 Display disconnected inputs

Press the key to view the status of disconnected inputs.



The appearing window (figure above) shows all the disconnected inputs of the selected unit.

11.2.3 Look excluded inputs

Select function *Supervision* → *Look Excluded Inputs*.

The window appearing (like figure above) shows all the excluded inputs of the selected unit.

11.2.4 Look global excluded inputs

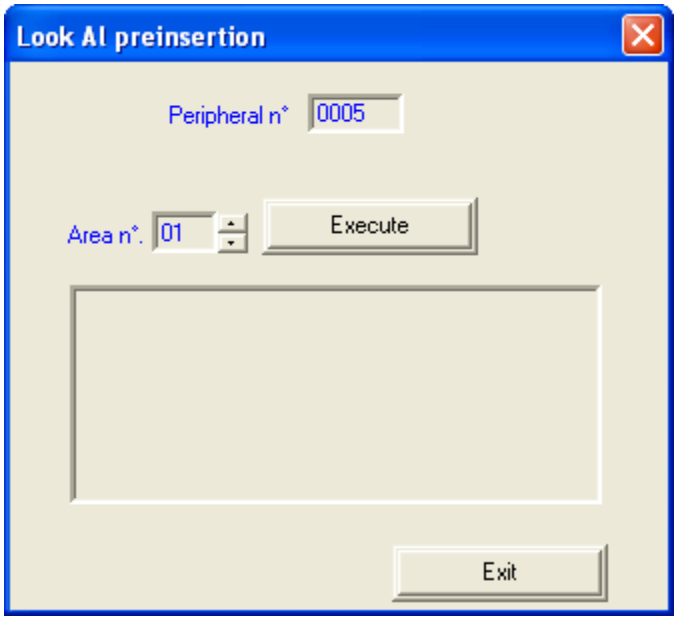
Select function *Supervision* → Look *Global Excluded Inputs*.

The window appearing (like figure above) shows the excluded inputs of all the units connected to the system.

11.2.5 Look alarm pre-insertion

Select function *Supervision* → *Look alarm pre-insertion* to display the status of inputs under alarm, belonging to a certain area of the selected unit.

It is useful to do this operation before arming an area, in order to avoid an instantaneous alarm due to the presence of an input in alarm of the area itself.

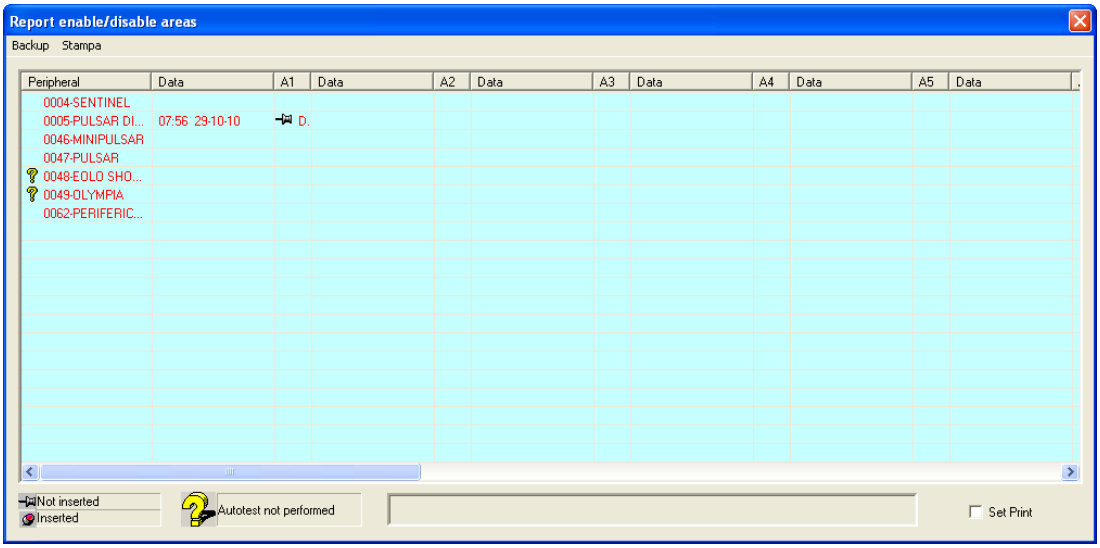


Select the desired area and press **Execute**.

The field underneath shows all inputs under alarm; if within the selected area there are no input is under alarm, a popup will appear with written *No input*.

11.2.6 View arming and disarming of areas

Select function *Supervision* → *Areas connected / disconnected*.



The window now appearing (previous figure) gives the following information:

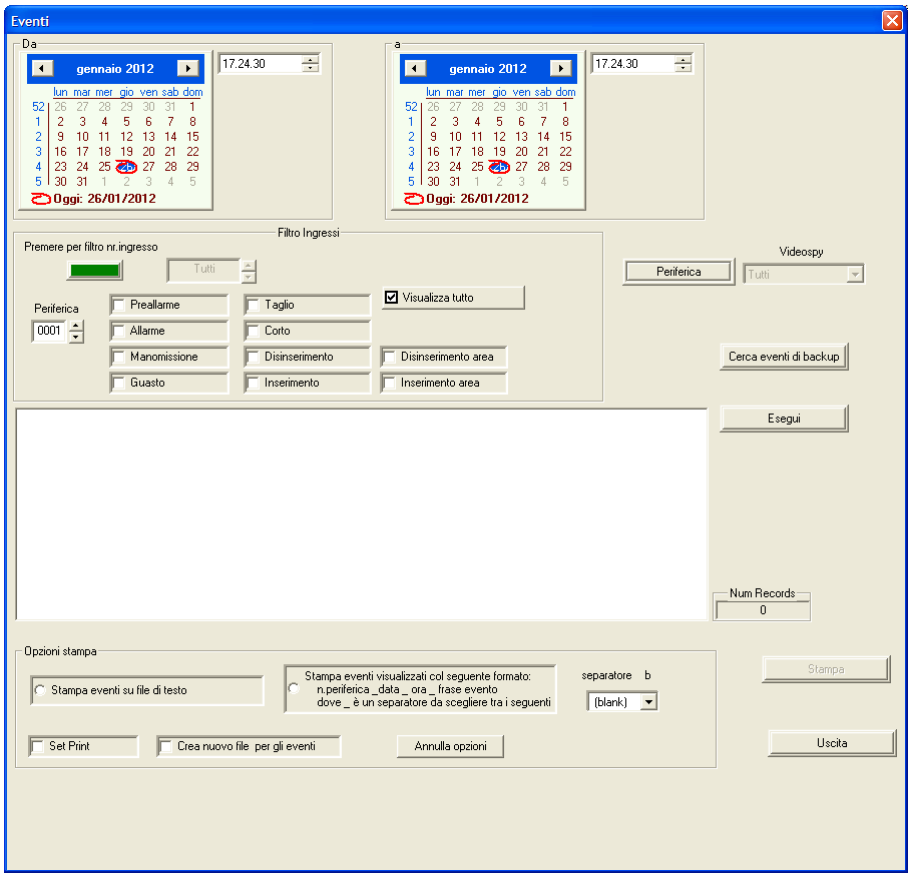
- Unit name and number;
- Indication of the event (armed or disarmed);

- Number of the areas involved;
- Date and time of last arm or disarm.

11.3 Display of Events

By calling from menu *Supervision* → *Look events*, some functions are available in order to view the received events:

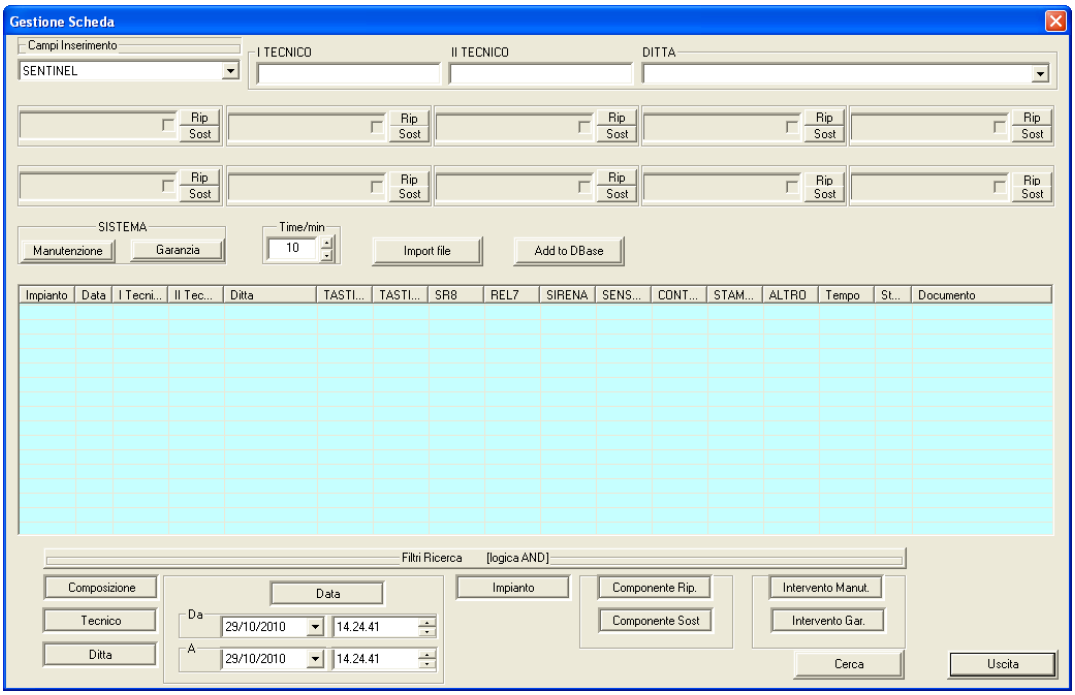
- *On range*: search all the events received from all the units during a period of time (from, to). It is possible to filter the research by:
  - Type of event with a multiple choice by using the flags;
  - On all the unit or by single input by pressing the green button and choosing the interested zone;
  - Print the results
- *On range and peripheral*: search all the events received by a single unit during a period of time (from, to). It is possible to filter the research by:
- *Latest n. events*: searches the last N events received from all the units;
- *Areas Connected/Disconnected*: report of the last arming / disarming of all the units, for the areas from 1 to 16.
- *Areas Connected/Disconnected II*: report of the last arming / disarming of all the units, for the areas from17 to 32.



11.4 Various displays

11.4.1 Service report sheets

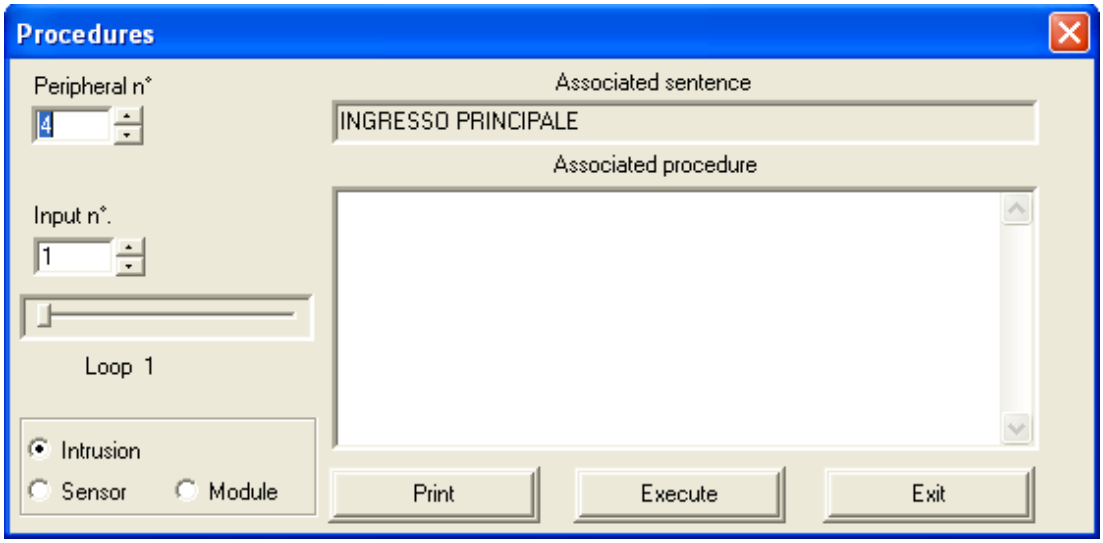
Select function *Supervision* → *Management cards*.



The window now appearing (figure above), shows a sheet containing the information of the selected unit. The filling of this sheet has no functional influence on the system.

11.4.2 Displaying the procedures

The function *Supervision* → *Display Procedure* shows the procedures to be executed, in case of alarm for each sensor and the phrase associated to every input.



- Set the unit number, the input number and the input type;
- In case of fire alarm units, select also the relative loop;
- Digit the procedure to be followed in case of alarm.

The procedure will be displayed on the terminal in case of alarm at the selected input.

11.4.3 Look change SK key time

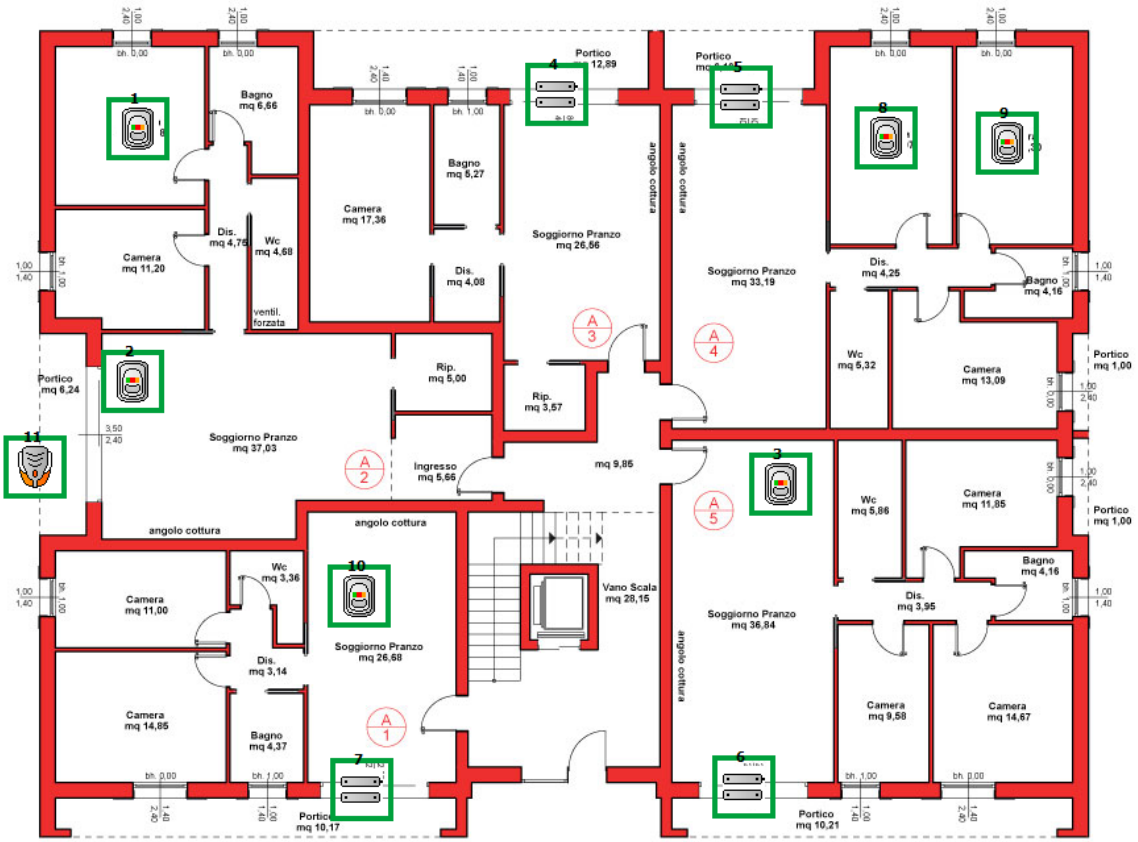
The function *Supervision → Look change SK key time* shows when the next change of the dynamic SK key will occur (protocol CEI ABI 79/5 79/6).

11.4.4 Look change ID time

The function *Supervision → Look change ID time* shows when the next change of the identification time will occur (protocol CEI ABI 79/5 79/6).

11.4.5 Look Alarm status

Press the key and select the desired unit.



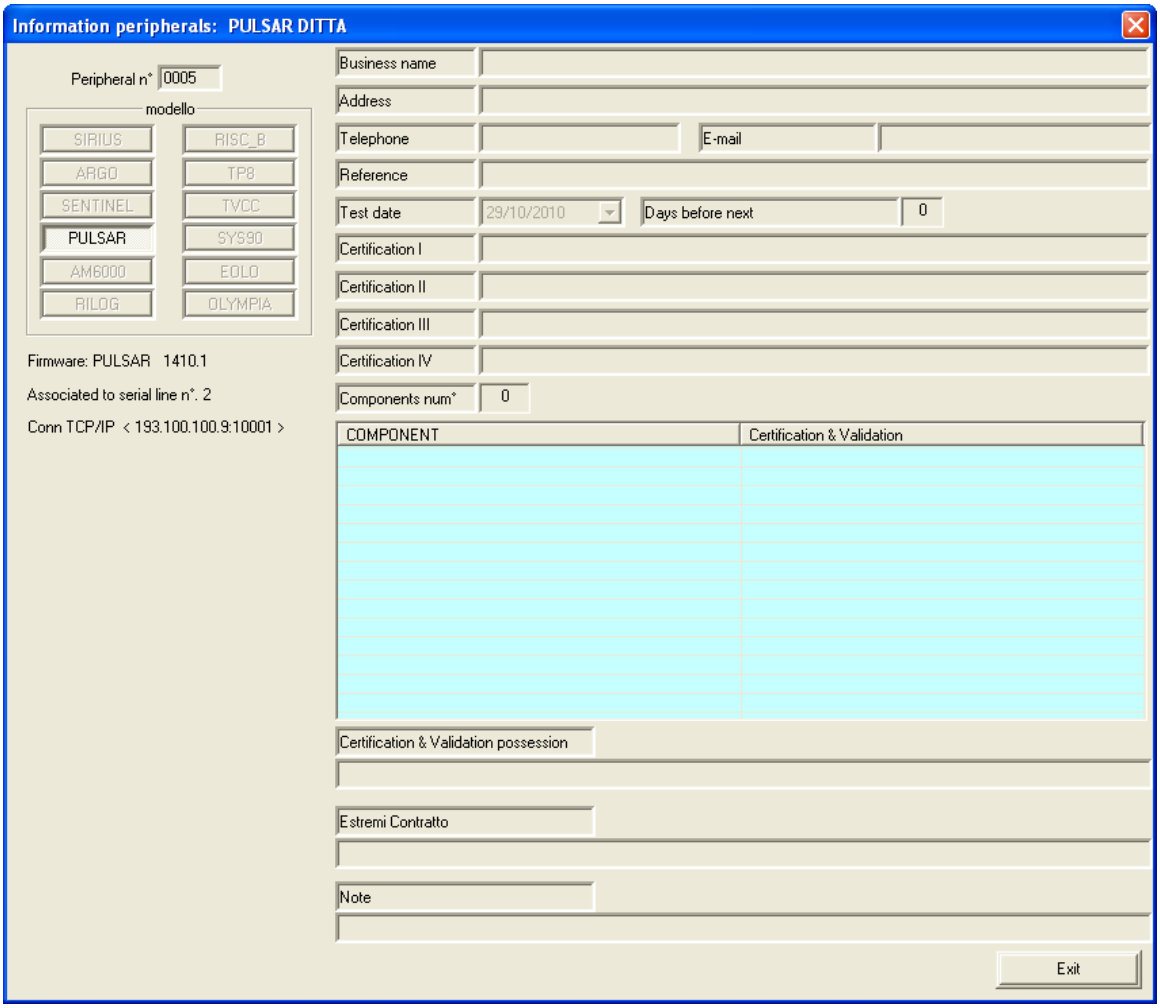
The window now appearing (previous figure) shows the map of the selected control unit, with the inputs displayed in different ways according to their status:

- Green square: input in rest

- Flashing red square: input under alarm
- Yellow square: input excluded (only for burglar alarm units)

11.4.6 Information on stations

Press the key and select the interested unit.

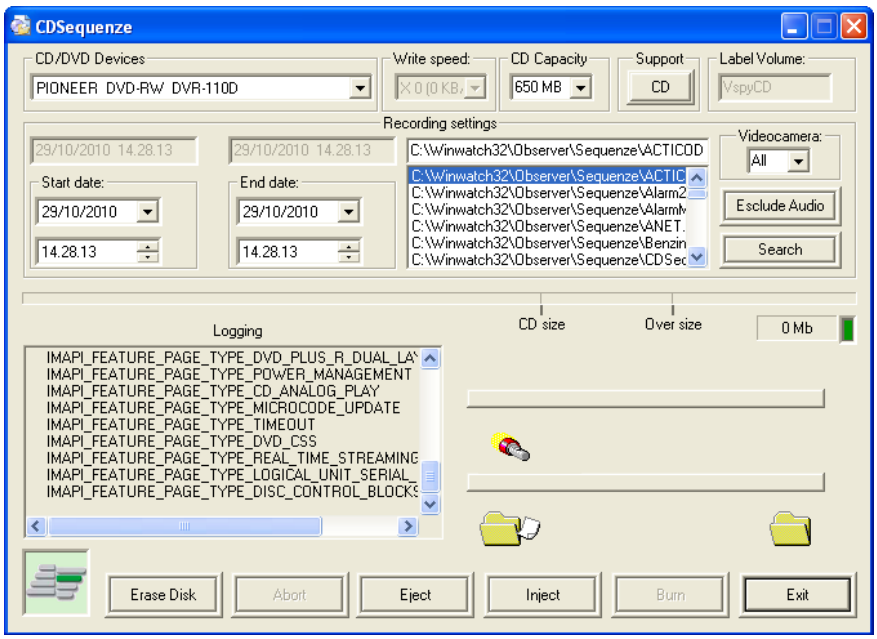


The window now appearing shows a sheet containing informing about the selected unit. Filling this sheet does not affect the system operation.

11.4.7 Alarm messages from DVR and TCP stats

Press the key and select a CCTV unit. In the appearing window is shown a list of alarms from the unit.

By pressing the key **Burn**, it is possible to store on CD/ROM the alarm sequences.



In the window appearing (previous figure) select the disc burner device, the start and end date and time of the alarms to be stored, the disc capacity, the type of support (CD or DVD); then press **Burn**.

11.5 How the switched line operates

If a dedicated serial link or a LAN is set as main communication, the telephone line (switched) is activated only under special circumstances, as described below.

The unit calls the monitoring centre in the following cases:

- The events buffer of the control unit is full: in this case the control unit starts a phone call to send to the monitoring centre the buffer of events, so that no trace is lost of any event;
- To communicate the occurrence of any event that, for malfunction of the primary line reasons, it was not possible to communicate with the centre.

The monitoring centre calls the unit in the following cases:

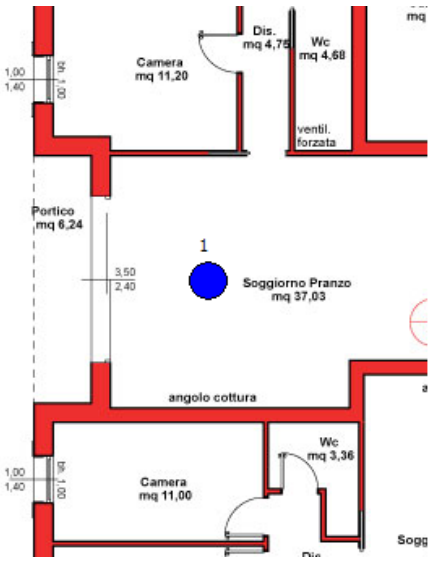
- As soon as the *Winwatch* software is launched, to check that the connection is active, if such action is set in the *Winwatch Setup*.
- When a command is sent from *Winwatch* that involves the unit.

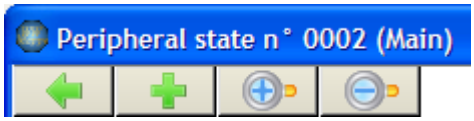
In case of call to a unit, the *Modem* window will appear, indicating in real time the modem status (in call to a unit, connection in progress, connection dropped, etc...)

11.6 Management of maps

11.6.1 Moving through map levels

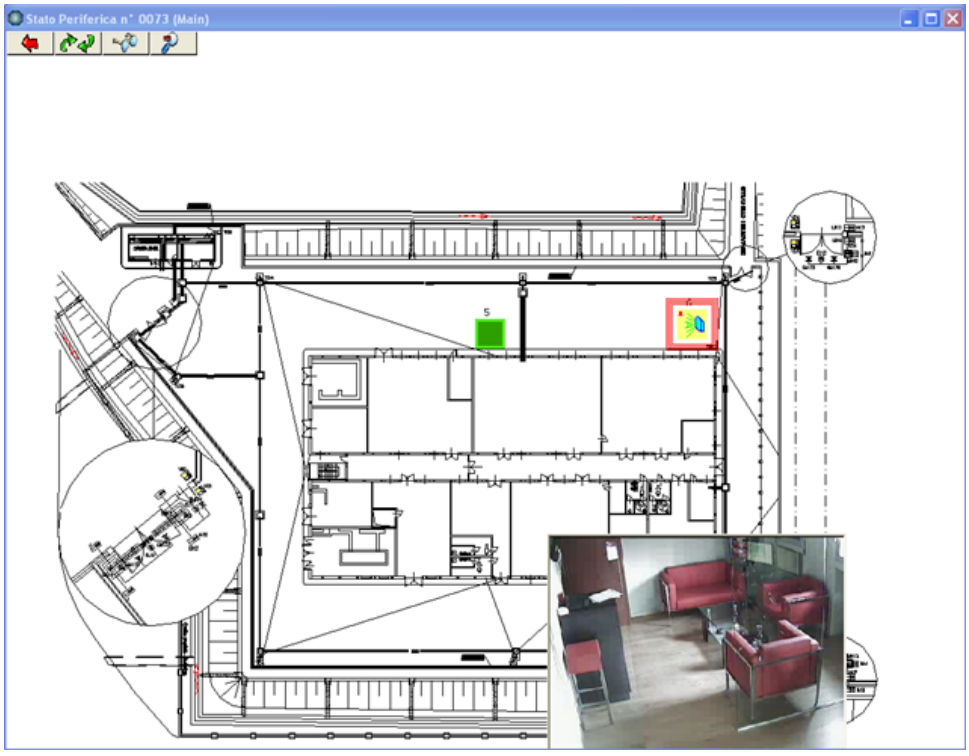
To move through the various map levels, double click the left mouse-key on the icons of the groups (blue circle). To return back, click on the green arrow.





11.6.2 What to do in case of alarm

If an alarm is triggered, the involved map will be displayed automatically if the function has been enabled by *Winwatch Setup* (paragraph **Errore. L'origine riferimento non è stata trovata.**). The detector under alarm is highlighted by a red flashing border.

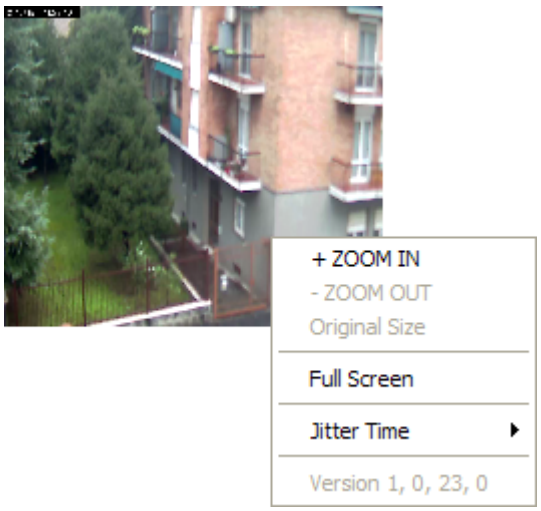


Double click on the symbol of the detector so that the following information is displayed: phrase associated, unit number, detector number, procedure to be executed in case of alarm.

To stop the buzzer sound, select the **Alarm acknowledgement** command, or press function key F9. If a video camera is associated to the map, the images taken by the video camera are displayed in real time.

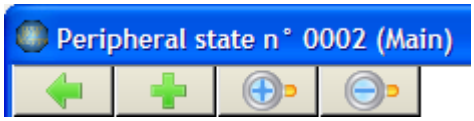
11.6.1 Videocameras management

In case an alarmi s received, and on the interessed map is present at least a camera, autmatically the real-time of these will be shown (if set to do it).



In case of IP cameras and/or cameras of a NetEye, it will be possible to open the camera on full screen by clicking with the right mouse button on the interested video, then on to *Full screen*. To exit from the full screen modality, it will be necessary to repeat the descript operation.

I twill also be possible to do a digital zoom by clicking in the video box an moving the mouse scroll ahead and back..



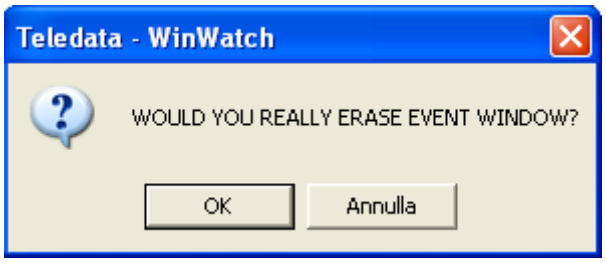
In case of classical analogical cameras, through the keys “+” and “-“ it will be possible to zoom in and out the cameras, enlarging the box of the camera itself. Press the desired zoom and double click in the video box. The function will remain in memory, so it will be possible to repeat the operation just by double clicking again in the box.

12. Maintenance

12.1 Management of Events

12.1.1 Clearing the window of events

Recalling this command from the pull-down menu *Maintenance* → *Clean up Event Window*, all events present in the *Events* window are deleted.

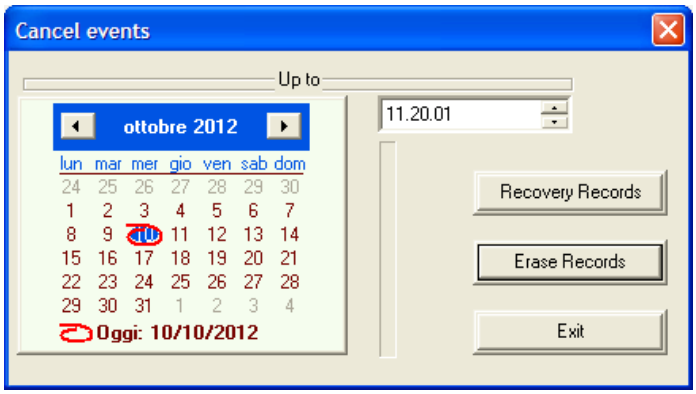


Press key **OK** to confirm the command.

The events, remain stored in the system. To erase them definitely, use the function Erase/*Recovery DBase Event* (paragraph 12.1.2).

12.1.2 Erase or Recovery events

Call these functions from the pull-down menu *Maintenance* → *Erase/Recovery DBase Event*

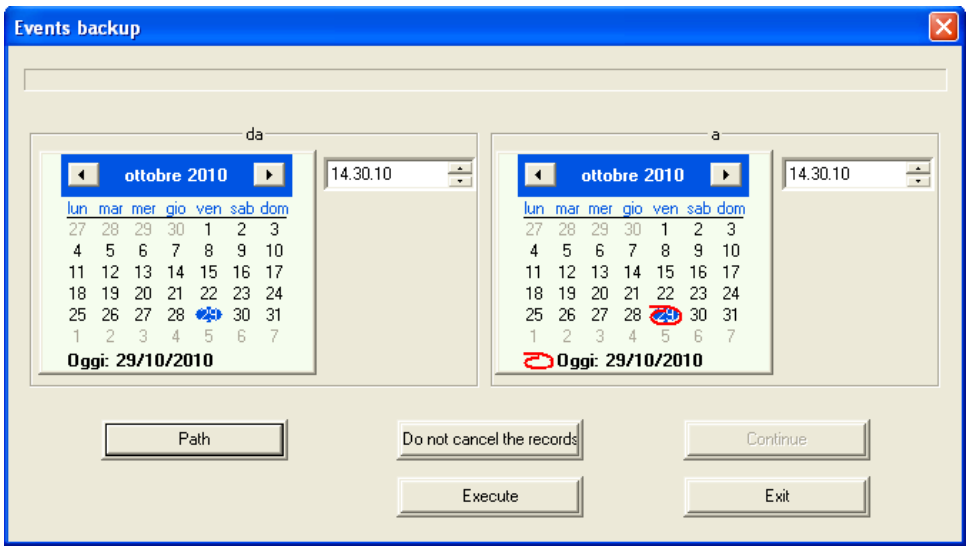


In the window appearing on the screen, select the date and time and one of the following functions:

- **Recover Records**: it recovers the events from the least recent one to the last one occurred before the selected date and time;
- **Erase Records**: it removes the events from the least recent one to the last one occurred before the selected date and time.

12.1.3 Backup events

To call this function from the pull-down menu select *Maintenance* → *Backup Events*. The function allows to make a backup of the events from a date to another.



In the window appearing (previous figure), proceed as follows:

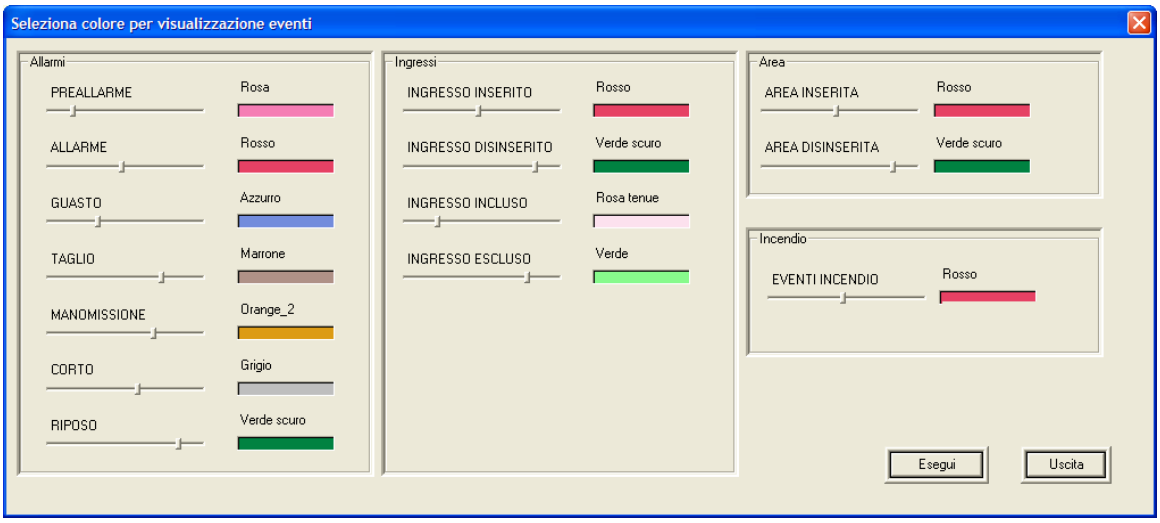
- Select the initial date and time in the left part.
- Select the end date and time in the right part.
- If you want to delete the events, press *Don't delete records* (now the key shows wording *Delete copied records*); then press **OK** to confirm.
- Press **Path** to select the path where to save the events.
- Press **Execute**.

12.1.4 Save Window Events on file

This function, called through the menù *Maintenance* → *Save Window Events on file*, allows saving the contents of the events window to the floppy disk unit A:\ or to the local disk, creating a file in the folder *C:\Winwatch32\Winwatch\CopiaWinEv.txt*.

12.1.5 Select Events colour

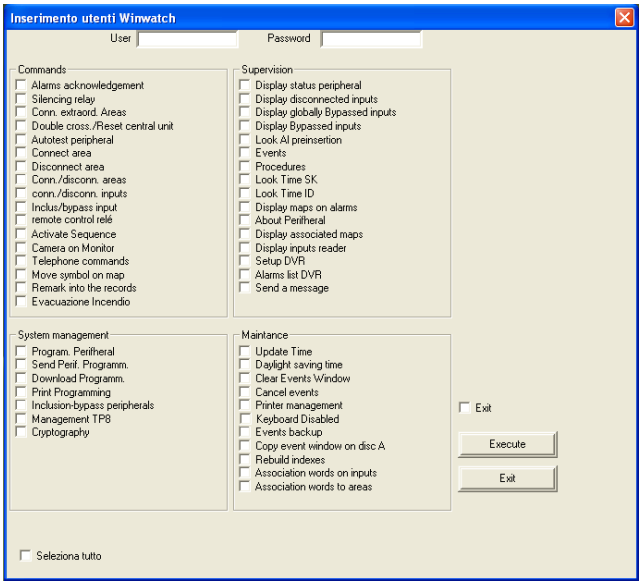
This function, called through the menu *Maintenance* → *Select Events colour*, allows to personalize the colour of the events received depending on the typology.



12.2 Management of Users

12.2.1 Enabling users

This function, called by selecting *Maintenance* → *Enable User* through pull-down menu, allows the system administrator to enable a user to the use of a certain number of functions of the system.

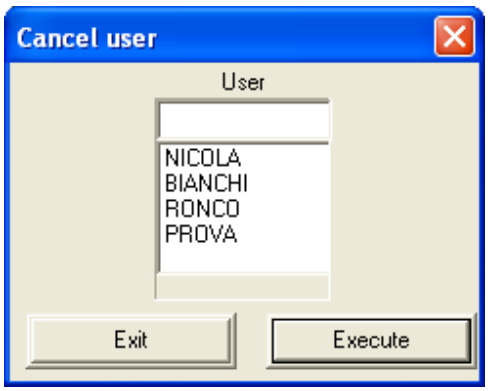


In the window appearing (figure above), proceed as follows:

- Digit user name and password of the new user;
- Enable the commands that the user will be able to use, divided by typology, one by one or press *Seleziona tutto* to select all.
- Press **Execute**.

12.2.2 Delete users

This function, which can be called only by the system administrator through the menu *Maintenance* → Erase *User* from the pull-down menu, allows to delete a user created previously.

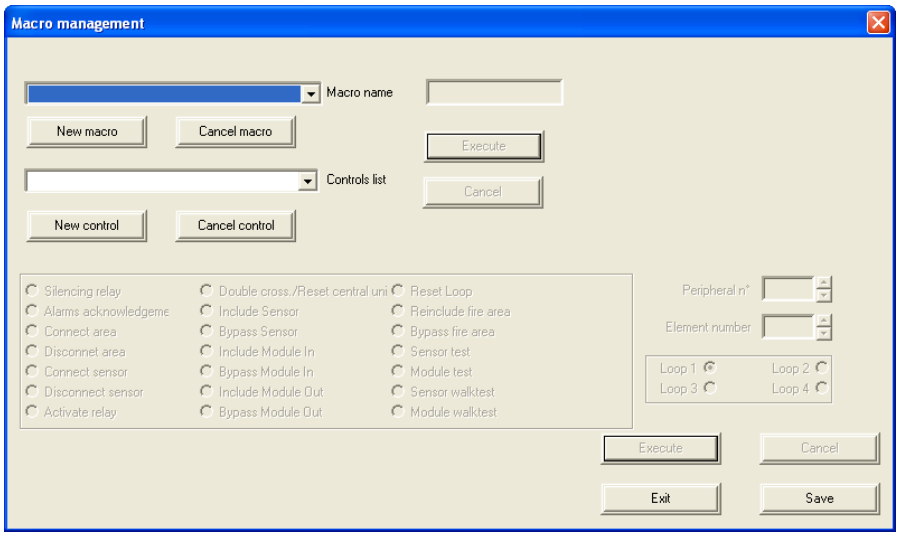


In the window now appearing, select the user to be deleted and press **Execute**.

12.2.3 Modifying users and creating macros

This function, which can be called by the system administrator only through selection *Maintenance → Modify User* from the pull-down menu, allows changing the user setting.

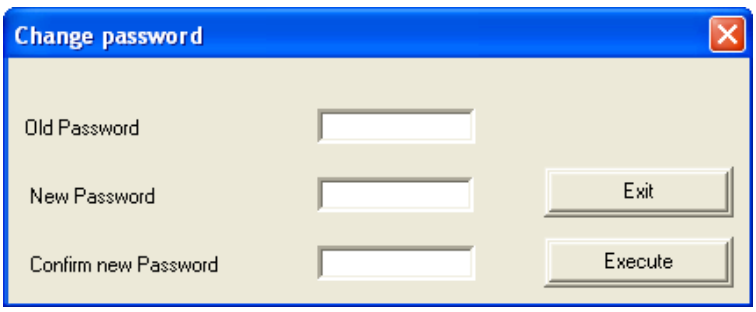
Moreover, every user can create a macro, namely a preset sequence of commands to be sent to the station. To do so, proceed as follows:



- Select *Users → Modify users*,
- Select a user from the list
- Press **New Macro**
- Digit the name of the macro in field *Macro Name*;
- Press **New Command;**
- Select the station's number, the loop (for fire alarm stations) and the type of command;
- Press key **Execute**;
- Press **New Command** till the end of the commands to be programmed;
- Press **Save** and **Exit**.

12.2.4 Changing a password

Through the function *Maintenance → Change Password* every user can change their own password

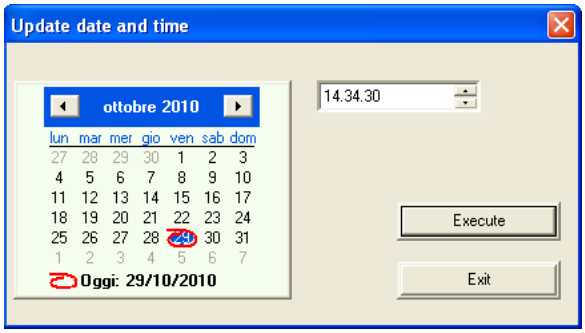


Enter the old and the new and confirm the password, then press **Execute**.

12.3 Date and Time management

12.3.1 Date and Time Setting

To update the system clock, select *Maintenance* → *Date and Time Setting*.

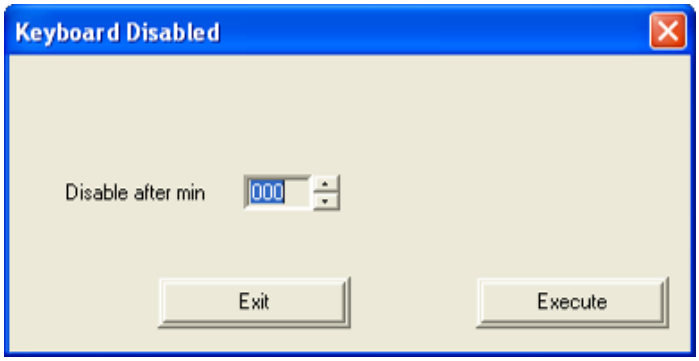


With this command, all the clocks of the control units connected will be synchronized with the monitoring centre.

12.4 Various

12.4.1 Disable user keyboard

The *Maintenance* → *Disable user keyboard* function allows to set a timeout which will disable the keyboard automatically in case of inactivity.



In the window appearing, set the desired timeout in minutes.

By setting 0, the keyboard will never be disabled. By setting a number higher than 0, after that amount minutes of inactivity the keyboard is disabled automatically (to reactivating it, a new login is required).

12.4.2 Enabling the printer

To enable the printer functionality, select *Maintenance* → *Enable printer* from the pull-down menu, and select *Events to printer*. With the printer enabled, every event received is printed instantaneously.

12.4.3 Rebuild Index

The function *Maintenance* → *Rebuild Indexes* allows reordering the lists of contents of the database in case the database of events is damaged.

With this function, lost or erased events will not be recovered.

12.4.4 Phrases associated to inputs

By calling the function *Maintenance* → *Input words* from the pull-down menu, it is possible to program the phrases associated to inputs without using the *Winwatch Setup* application. For more information, refer to paragraph **6.3.1**.

12.4.5 Phrases associated to the areas

By calling function *Maintenance* → *Areas Words* from the pull-down menu, it is possible to set phrases associated to the geographic areas that were programmed without using the *Winwatch Setup* application. For more information, refer to paragraph **6.3.3**.

12.4.6 Enabling acoustic alarm signals

With the *Users* → *Sound Blaster* function selected on, upon every alarm an acoustic signal be will be emitted through the loudspeakers of the computer in use.

13. Signalling of events

13.1 Introduction

The events can be generated by:

- **Units** (paragraph **Errore. L'origine riferimento non è stata trovata.**)
- **Monitoring centre** (paragraph 13.3)
- **Commands** (paragraph 13.4)

Upon their occurrence, the events are notified in the *Events* window.

If the printer is enabled, the events are printed in real time (paragraph 6.2)

13.2 Events from station

The unit can send the following messages:

DETECTOR ALARM	One of the five alarm levels
DETECTOR FAULT	One of the five alarm levels
DETECTOR CUT	One of the five alarm levels
DETECTOR SHORT-CIRCUIT	One of the five alarm levels
DETECTOR TAMPERED	One of the five alarm levels
UNIT TAMPERED	Unit cover opened
PERIPHERAL DEVICES TAMPER	Cover of peripheral devices opened (sensors, keyboards, etc...)
FUSE INTERRUPTION ON UNIT & PERIPHERAL DEVICES	Interruption of peripheral device fuses (sensors, keyboards, etc...)
PERIPHERAL DEVICES POWER SUPPLY FAILURE	Peripheral device power supply failure (sensors, keyboards, etc...)
PERIPHERAL DEVICES POWER SUPPLY RESTORED	Peripheral device power supply restored (sensors, keyboards, etc...)
BATTERY LOW	Battery charge level is low
BATTERY DISCONNECTED	Battery disconnected
BATTERY RESTORED	Battery connection OK
220V POWER SUPPLY FAILURE	Mains power supply failed
220V POWER SUPPLY RESTORED	Mains power supply OK (restored)

13.3 Events from supervision centre

The monitoring centre can send the following messages:

MISS LINE	Units in connection failure (serial links and/or LAN connection)
LINE RESTORED	Serial links and/or LAN connection restored
IDENTIFICATION FAILED (79/5 79/6)	Reports that the identification procedure has failed
PASSAGE IN DEGRADED (79/5 79/6)	Reports the corruption of the cryptography master key
20 MINUTES TIMEOUT NOW STARTING (SWITCHED!!)	In case of telephone call conflicts between monitoring centre and units, the centre starts a timeout to receive possible alarms. To reset the timeout, you should send any command.

13.4 Events by command

Whenever a valid command is sent, it is executed immediately by the unit, and an event is generated.

If for example area 1 of unit 3 is disconnected, at 13:11 of day 18/09/2009, the following event will be generated:

0003 13:11 18-09-09 AREA n.1 DISCONNECTED (area name)