Alarm Control Panels

INTEGRA

Firmware Version 1.04

PROGRAMMING

integra_p_e 09/06

The SATEL's goal is to continually upgrade the quality of its products, which may result in alterations of their technical specifications and firmware. The current information on the introduced modifications is available on our website.
Please visit us:
http://www.satel.pl

<table>
<tr><th colspan="2">DECLARATION OF CONFORMITY</th><td rowspan="2">CE</td></tr>
<tr><td><b><i>Products:</i></b>
CA424P, CA832, CA16128P
- mainboards of INTEGRA control panels.
- INTEGRA 24
- INTEGRA 32
- INTEGRA 64
- INTEGRA 128</td><td><b><i>Manufacturer:</i></b> SATEL spółka z o.o.
ul. Schuberta 79
80-172 Gdańsk, POLAND
tel. (+48 58) 320-94-00
fax. (+48 58) 320-94-01</td></tr>
<tr><td colspan="3"><b><i>Product description:</i></b> Mainboards for alarm control panels intended for use in intruder alarm systems.</td></tr>
<tr><td colspan="3"><b><i>These products are in conformity with the following EU Directives:</i></b>
<b>LVD</b> 73/23/EEC+93/68/EEC
<b>EMC</b> 89/336/EWG + 91/263/EEC, 92/31EEC, 93/68/EEC
<b>R&TTE</b> 1999/5/EC (network connection, TBR21)</td></tr>
<tr><td colspan="3"><b><i>The product meets the requirements of harmonized standards:</i></b>
LVD: EN 50131-1:1997; EN 50131-6:1997; EN60950:2000, EN60335-1:1994/A1:1996 Annex B
EMC: EN 55022:1998; EN 61000-3-2/-3; EN 50130-4:1995, EN 61000-4-2/-3/-4/-5/-6/-11
R&TTE: TBR 21(1998)</td></tr>
<tr><td>Gdańsk, Poland 07.03.2005</td><td colspan="2">Head of Test Laboratory<i>:</i>
Michał Konarski</td></tr>
<tr><td colspan="3">Latest EC declaration of conformity and product approval certificates are available for downloading on website <b><i>www.satel.pl</i></b></td></tr>
</table>

The INTEGRA alarm control panels meet requirements as per CLC/TS 50131-3, Grade 3, and have been certified by Det Norske Veritas Certification AS, Norway.

New functions of the INTEGRA control panels in version 1.04

Control panel options	TROUBLE MEMORY UNTIL REVIEW DO NOT SHOW ALARM IF ARMED LIMIT EVENTS REMOTE SYSTEM RESET AVAILABLE
Arming options	VIOLATED / BYPASSED ZONES PREVIEW WHEN ARMING REQUIRED SYSTEM RESET AFTER VERIFIED ALARM DO NOT ARM IF TAMPERED DO NOT ARM IF REPORTING TROUBLE DO NOT ARM IF BATTERY TROUBLE DO NOT ARM IF OUTPUTS TROUBLE DO NOT ARM IF TROUBLE
Partitions	Shortening of partition exit time
Zones	New reaction types: 62. TECHNICAL – OVERLOAD 89. FINISHING EXIT DELAY 90. DISABLING VERIFICATION Alarm from the zone type 13. PANIC-SILENT is not audibly signaled in the keypad. MAX. NO VIOLATION TIME can be programmed in minutes. New zone options: CHIME IN MODULE WITH VERIFICATION BLOCKS VERIFICATION REPORTING DELAY CHECK ARM POSSIBILITY RESTORE DISARMS RESTORE DISABLES VERIFICATION
Outputs	Zone type 30. AC LOSS (FROM EXPANDERS) also signals troubles of AC supply of mimic boards. Output type 33: EXPANDER BATTERY TROUBLE also signals troubles of mimic board batteries. New output types: 95. ETHM/GSM/ISDN REPORTING TROUBLE 105. SHUTTER UP 106. SHUTTER DOWN 107. CARD ON READER A 108. CARD ON READER B 109. ZONES LOGICAL AND 110. ALARM – NOT VERIFIED 111. ALARM – VERIFIED 112. VERIFIED – NO ALARM 113. VERIFICATION DISABLED STATUS

	114. ZONE TEST STATUS 115. ARMING TYPE STATUS 116. INTERNAL SIREN
Keypad	Exit delay shortening available Keypad name shown in 2nd line of display Audible signaling of new trouble Code entry displayed Information (sound and message) on disarming keypad controlled partitions Control of keypad sounder volume After violation of CHIME disabling zone, key sounds and exit time signaling are not disabled. The REVIEWS submenu has been modified because of a changed treatment of tampers.
Proximity card support by keypad	A new function in the keypad for card presenting / holding: "1 beep".
Monitoring	Monitoring by means of Ethernet (TCP/IP) network Monitoring by means of GSM (GPRS) and ISDN networks Periodical monitoring test transmissions can be sent every specified number of days
Messaging	Acknowledged reception of message by a user may reset the function of messaging to other users.
Event history	Function resetting the event history has been deleted.

CONTENTS

1. General

The INTEGRA series control panels are characterized by a high flexibility of firmware, which enables their functionality to be customized as per individual requirements of the protected premises. The DLOADX and GUARDX programs, which are offered free of charge, facilitate configuration of settings and operation control of the alarm system. The control panels may be programmed locally or remotely.

2. Control Panel Firmware Replacement

The control panel program is saved in the FLASH-type memory. Replacement of the firmware is possible without the necessity to dismantle the control panel and the system. It is performed via the RS-232 port installed on the control panel board. The mainboard RS-232 port and the computer port should be connected as shown in Figure 1.

Notes:

- *Do not short or touch the serial port RS-232 pins with your fingers.*
- *Prior to connecting the cable, the installer should preliminary remove the electrostatic charge, e.g. by touching a grounded equipment (faucet, heater, etc.). with the top of his hand.*
- *It is recommended that the cable be connected first to the control panel connector, and then to the computer connector.*

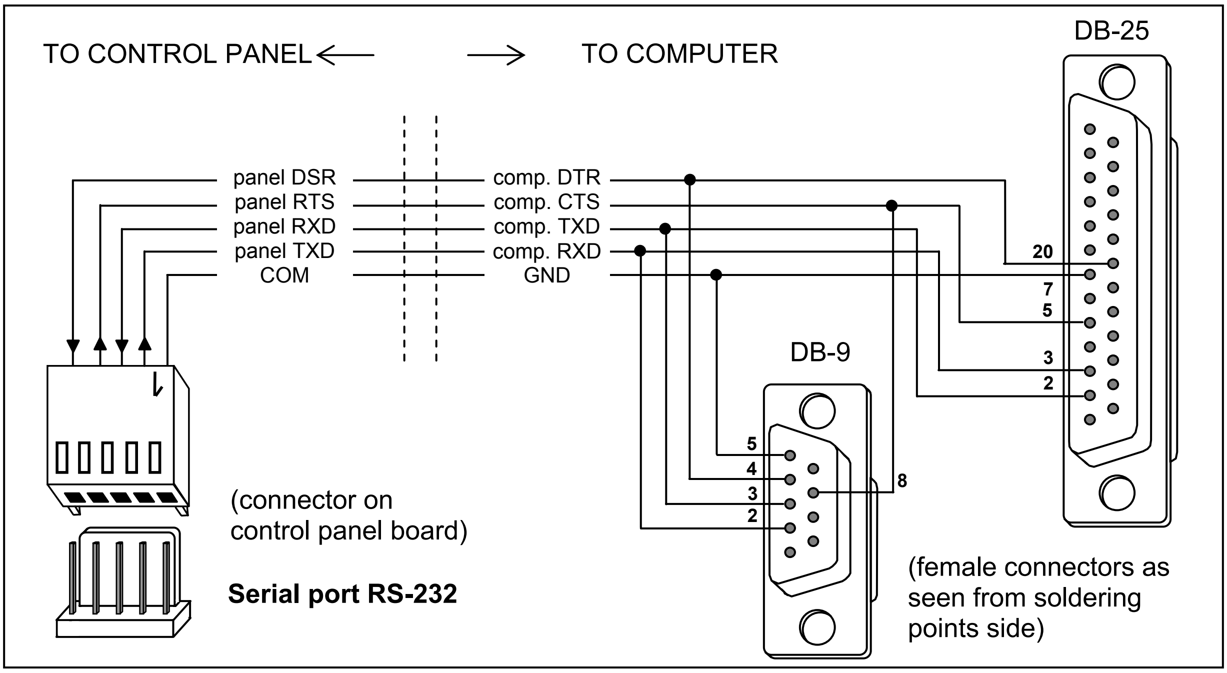


Fig. 1. Connection of computer to the control panel serial port.

The firmware replacement is possible owing to the STARTER program, stored in the control panel memory, and the FLASHX program, which can be downloaded from the website **www.satel.pl**. Available on the website is also the latest version of control panel firmware.

Note: *After installation, but prior to programming of the control panel, the SATEL Company recommends you check that the current firmware version is stored in the control panel memory and update it, if necessary.*

In order to begin the firmware replacement, launch the STARTER program in the control panel. It can be done in two ways:

1. Select the function from the service mode menu (→*Service mode* →*Restarts* →*Starter*).

2. Short-circuit the RESET pins when starting the control panel. Remove the short-circuit immediately after power-up (approx. 1 second). If the pins are shorted longer, the function of programming from computer will be started (provided that a computer with running DLOADX program is connected to the control panel) or the service mode will be entered.

Running of the STARTER program is signaled by rapid blinking of the "DIALER" LED, suitable message displayed on all LCD keypads, as well as blinking of LED indicators on keypads, partition keypads and code locks.

Note: *During operation of the STARTER program the control panel does not perform its normal functions (only the status of electronic fuses being monitored).*

The STARTER program is waiting 2 minutes for the procedure of control panel firmware replacement to begin. If this does not happen, the control panel will return to its normal working mode (operation of the STARTER program can be terminated before expiry of 2 minutes by means of the RESTART command in the FLASHX program).

Taking into account the a.m. time limitations, launch the FLASHX program on the computer, select the file with new program for control panel, indicate the port through which communication is effected, and start the procedure of firmware replacement.

Note: *If, for any reason, the procedure of firmware replacement is suddenly interrupted (e.g. because of power supply failure) and, as a result, the control panel firmware is corrupted, the STARTER program will be launched automatically and will remain active until the correct firmware is installed.*

3. Programming

The control panel can be configured from the LCD keypad (locally) or by the computer with a suitable firmware (locally and remotely). If the ETHM-1 module is installed in the alarm system, remote programming is also possible by means of an internet browser or cellular phone (after appropriate application is installed on it).

Programming the control panel is only possible when it is accessible to the service. By default, the option PERMANENT SERVICE ACCESS. ([*master code*][*] →*Change option* →*Perm. serv. acc.*). Thus, you can easily proceed to programming as soon as installation is completed. However, the master users (administrators) are bound by the normative requirements to limit the service access after installation is over. Therefore, prior to commencement of the programming at a later date, it is necessary to contact the administrator to get access to the control panel. The master user function SERVICE ACCESS enables access time to be defined in hours.

Note: *Should the master user forget his code and the service access be disabled (service access time=0), it is still possible for the installer to enter a new master code (without the necessity to delete the previously entered user codes). To this effect he must enter the service code by hardware means ("from pins" - see description further in this manual). After quitting the service mode, the installer can within approx. 20 seconds call up the function MASTERS for editing by means of the service code and enter a new code.*

3.1 LCD keypad

Programming the control panel from LCD keypad is carried out by means of the service functions, available in the service mode menu.

3.1.1 Service mode

In order to start the service mode:

1. Enter the **service code** (by default 12345) and press [*].
2. Select the item SERVICE MODE from the list and press the [#] or [▶] key.

The service mode is indicated on LCD keypads by the [SERVICE] LED. It can be also signaled by beeps, provided that the corresponding option is enabled.

Note: *When in the service mode, the only possible alarms are those from zones 24H VIBRATION, 24H CASH MACHINE, PANIC-AUDIBLE and PANIC-SILENT.*

The control panel remains in the service mode until it is quitted by means of the function END SERVICE. It is possible to hide the service mode after expiry of a programmed time period if no operations are performed on the keypad. Then the control panel remains in the service mode, though the keypad quits the service mode. The service mode will be still indicated on the keypad by the [SERVICE] LED (provided that audible signaling option is enabled). Return to the service mode menu in the keypad will only take place after the service code is entered again and the SERVICE MODE selected in the user menu.

When quitting the service mode, the INTEGRA control panel will perform a check for possible changes in the settings of service programmed parameters. If no changes are found, exit from service mode follows. If any settings have been changed, the message "Store settings in FLASH ? 1=Yes" will be displayed. Pressing the key [1] will store the current data in the FLASH memory. This will guarantee their saving and enable their later retrieval e.g. in case of a power failure in the control panel.

Note: *RAM memory errors should not occur, if the system is correctly configured and properly supplied.*

3.1.2 Entering service mode "from pins"

If entering the service mode by the use of above mentioned methods is impossible, e.g. the keypad is not supported, for whatever reason, by the control panel, it is necessary to perform a special procedure which makes it possible to start the control panel and enter the service mode "**from pins**". To make sure that all settings correspond to the factory default values, perform the settings restart functions.

Follow the procedure below:

1. Disconnect in turn the AC supply and the battery and check keypad connections to the keypad bus.
2. Place the jumper on RESET pins located on the control panel board.
3. Connect in turn the battery and the AC supply - the DIALER LED will start blinking (the control panel will not start when connected to battery only).
4. Wait until the LED goes off, then remove the jumper from pins – the control panel should automatically enter the service mode menu - the message "→End service" appears on the display of keypad with the lowest address number, and the [SERVICE] LED starts blinking. If the "Clear settings? 1=Yes" message appears on the main display, this means that the access to the service mode "with the use of jumpers" has been disabled in the control panel program (→Service Mode →Configuration →Block SM). Then you can enter the service mode by pressing the number key 1, but this will erase all settings previously programmed in control panel (just like after performing functions mentioned in point 5 of this procedure). Having completed this operation, you may proceed to point 6.
5. Perform restart functions (→Restarts →Clear settings / →Clear codes).
6. Perform identification functions for modules connected (→Structure →Hardware →Identification →LCD keypads id. / →Expanders id.).

***Note:** After identification, the addresses in keypads and expanders must not be changed.*

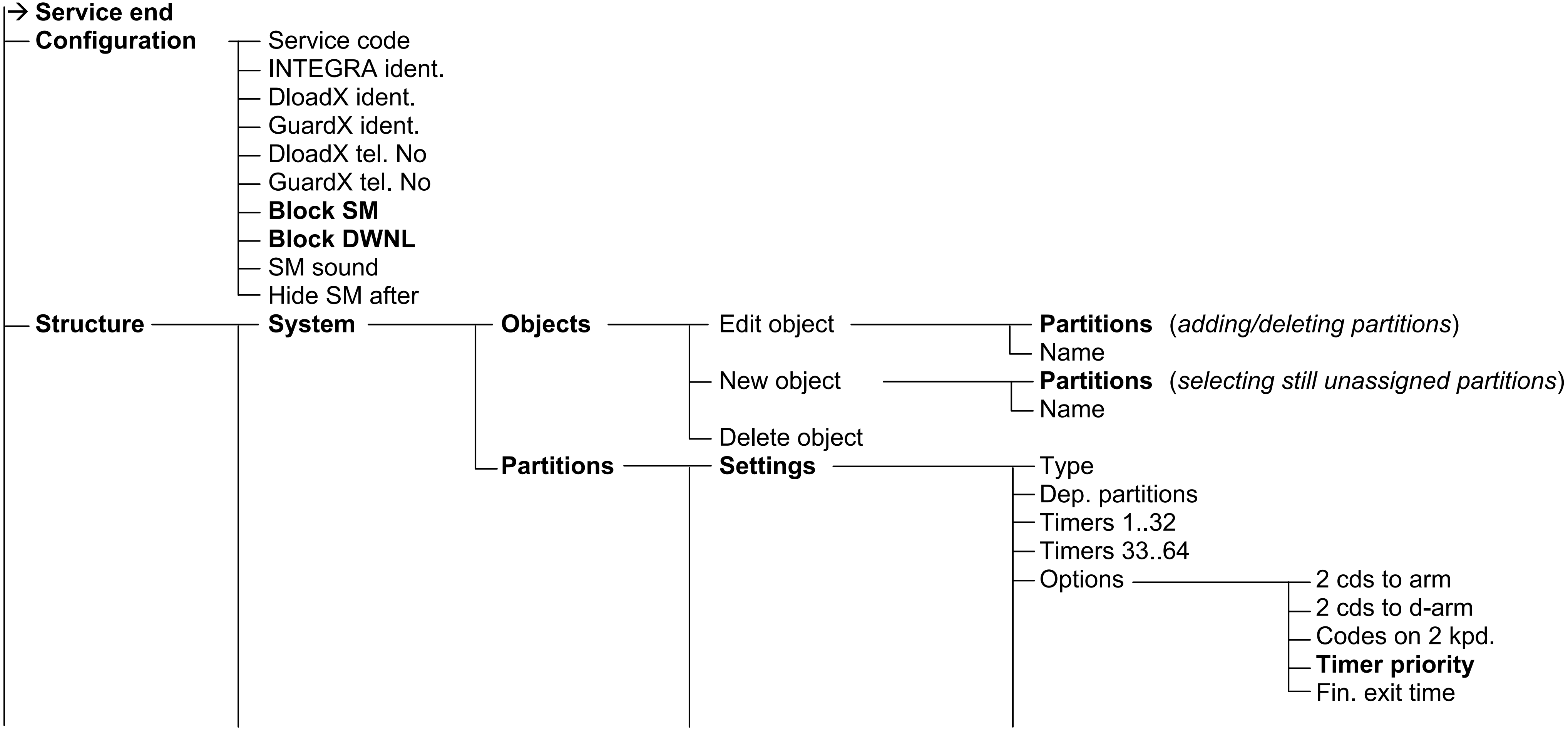
7. End the service mode with the function END SERVICE. When the keypad displays the message "Save data to FLASH memory?   1=Yes", press the key with number 1 to save the new settings.
8. Call up the service mode once more. If the control panel enters the service mode again, it is functioning OK.

Notes:

- *If the control panel is connected to a computer with running DLOADX program, the function of downloading via RS-232 will be started instead of the service mode.*
- *You can disable starting the service mode "from pins" by using the service mode function Block SM (Service mode →Configuration →Block SM). It will be possible to start the service mode from pins on giving consent to restoration of default settings.*

3.1.3 Service mode menu

[SERVICE CODE][*][9] (starting the service mode with a shortcut)



- → **Service end**
- **Configuration**
  - Service code
  - INTEGRA ident.
  - DloadX ident.
  - GuardX ident.
  - DloadX tel. No
  - GuardX tel. No
  - **Block SM**
  - **Block DWNL**
  - SM sound
  - Hide SM after
- **Structure**
  - **System**
    - **Objects**
      - Edit object
        - **Partitions** (*adding/deleting partitions*)
        - Name
      - New object
        - **Partitions** (*selecting still unassigned partitions*)
        - Name
      - Delete object
    - **Partitions**
      - **Settings**
        - Type
        - Dep. partitions
        - Timers 1..32
        - Timers 33..64
        - Options
          - 2 cds to arm
          - 2 cds to d-arm
          - Codes on 2 kpd.
          - **Timer priority**
          - Fin. exit time

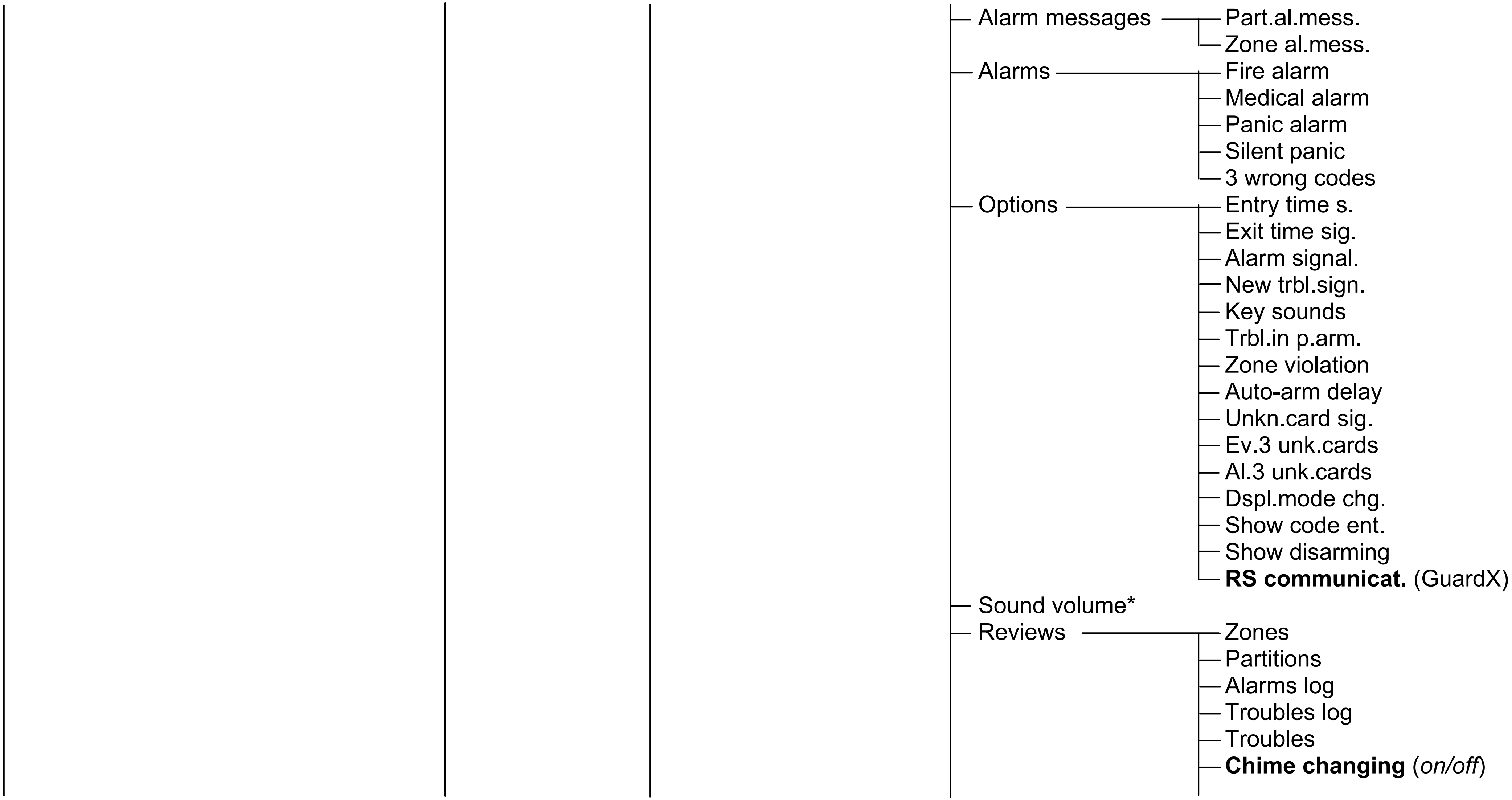
- Exit delay
- Auto-arm delay
- Al. verify time (*prealarm*)
- Al. verify time (*audible*)
- Guard - armed
- Guard - disarm.
- Time for guard.
- C.mach.blk.del.
- C.mach.blk.time
- **Zones**
- Name

Names (*by numbers*)

Hardware — **LCD keypads** — **Settings** — *Name*

- Partitions
- Alarms
- Fire alarms
- Chime zones
- Chime bps. zone
- Chime bps. time
- Quickarm part.
- Fin. exit time
- Entry time p.
- Exit time part.
- DateTime format
- Name (2nd row)
- LCD backlight
- Keys backlight
- Auto backlight

(Configuration functions for mimic board working in keypad mode are provided after the main menu of service functions.)



*option available for INT-KLCD-GR/BL and INT-KLCDR-GR/BL keypads

- State part. (*select*)
- Zone characters
- Part.characters
- **Code+arrows**
  - Code ↑ function (←→↓)
  - Code ↑ part (←→↓)
  - Code ↑ outputs (←→↓)
  - Code ↑ zones (←→↓)
- Card close
- Card close long
- Door to open
- Kpd tamper
- **Z1 (n) in kpd** (n – zone no. in system)
- **Z2 (n) in kpd**

- Names (*by addresses*)
- DTM short
- Loud tamp.DTM

- **Expanders**
  - **Settings**
  - Names
  - DT1 short
  - Loud tamp.DT1
  - DT2 short
  - Loud tamp.DT2

(The functions related to expander settings are made available, depending on system configuration. Description of available settings can be found on next pages, after service functions menu for the mimic board.)

- **Identification**
  - LCD keypads id.
  - Expanders id. *(Ident. of addressable zones)*
  - **Keypads addr.**

- **Options**
  - **Tel. options.**
    - Mon. TELEPHONE
    - Mon. GPRS/ISDN
    - Mon. ETHM-1
    - Tel.messaging
    - Modem answer.
    - Voice answer.
    - Remote control
    - Tone dialing
    - Groud start
    - No dialton.tst
    - No answer test
    - Dbl.voice msg.
    - Double call
    - External modem
    - ISDN/GSM modem
    - Pulse 1/1.5
  - **Printer options**
    - Printing
    - Monitor.status
    - Names/descript
    - Wide paper
    - 2400bps (*off: 1200 bps*)
    - CR+LF (*off: CR*)
    - Parity bit
    - Parity: EVEN (*off: ODD*)
    - Zone alarms
    - Part/mod. al.
    - Arming/disarm.
    - Bypasses
    - Access control
    - Troubles
    - User functions
    - System events
  - **Active rights** (*see: USER MANUAL – USERS function*)

- **Various options**
  - Simple codes
  - Notify of code
  - Confirm with 1
  - Autoabort msg. *(cancel messaging together with alarm clearance)*
  - SM -> menu (*reset*)
  - Tests -> menu (*reset*)
  - Powersaver *(switch off display/keys backlighting on AC loss)*
  - Fast exp. bus *(fast data transmission on expander buses)*
  - No rest. mon. (*do not monitor module restarts*)
  - Inf.aft.tamper *(display message after tamper alarm until service intervention)*
  - Zones bef. arm (*view violated / bypassed zones before arming*)
  - Arm, trb.warn. *(warn of troubles before arming)*
  - Blk aft.w.code *(after a wrong code is entered (or a wrong card/chip is read in) three times, the keypad (reader) will be blocked for 90 seconds; when this time period expires, each wrong code entered (or a wrong card read) will result in instant blocking)*
  - Troubl. memory (*trouble memory displayed until reset*)
  - Hide alarms (*in armed mode, alarms are not displayed on keypads*)
  - Events limit. *(in armed mode, events from the same source will only be saved 3 times)*
  - Remote reset *(remote system restore after verified alarm)*
- Do not arm
  - If verif. al. *(re-arming after verified alarm will only be possible after system restoration by the installer)*
  - If tamper *(do not arm if tamper)*
  - If monit.trbl. *(do not arm if monitoring trouble)*
  - If batt. trbl. *(do not arm if battery trouble)*
  - If zones trbl. *do not arm if outputs trouble)*
  - If other trbl. *(do not arm if other trouble)*
- **Times**
  - Global entry delay
  - Global alarm time
  - Suppr.arm status after
  - AC loss report delay
  - Tel. loss report delay

- Rings to answer
- **Prefix length**
- Clock adjustm.
- Daylight saving
- Summer time
- Winter time

- **Zones**
  - Details
    - EOL
    - Sensitivity [x20ms]
    - Type
    - Entry delay / Alarm delay / Surveillan.time / Signal. delay / Bypass time (64-79) / Kpd number (*58*) / Arming mode (*80, 82*) / Group (*80, 81, 83*)
    - Max.viol.time / Max.opening t. (*for 57 type zones*)
    - Max.n-viol.time
    - No viol [min]
    - Partition
    - Power up delay
    - Priority / Disrm.on viol. (*for 82 type zones*)
    - Chime in exp.
    - Video,disarmed
    - Video,armed
    - Bypass disabl.
    - Bypass no exit
    - Bell delay / Alarm if armed (*64-79*) / Clear alarm (*81 i 82*) / Restore=disarm (89)
    - Auto-reset 3
    - Auto-reset 1
    - Auto-rst. clr.
    - Pre-alarm / Attend verif. (*for zones type 0-2 and 85-86*)
    - Abort delay / Part.tmp.block (*for 84 type zones*)
    - Rest.after bell
    - Rest.aft.disarm
    - Al.on exit end (*when violat.*) / Violat.events (*47*) / No bp.if armed (*64-79*) / Abort voice m. (*81, 82, 83*)
    - Al. aft.unbps. (*alarms when violated after unbypassing*)
    - Tamp. alw.loud
    - Monitor.delay (*4-7, 64-79*) / Chk.if can arm (*80, 82*) / Restore=bps.v. (*89*) / Bypass verif. (*0-2, 85-86*)
    - Name

- Parameters
  - Partition (*by zone nos.*)
  - EOL (*by zone nos.*)
  - Sensit. [x20ms] (*by zone nos.*)
  - Type (*by zone nos.*)
  - Entry delay (*by zone nos.*)
  - Max.violat.time (*by zone nos.*)
  - Max.no-viol.t. (*by zone nos.*)
  - Zone options (*by details & zone nos.*)
- **Counters**
  - **Counter n**
    - Max. value
    - Counting time
    - Omit recurs
- **Bypasses**
  - **Group n**
    - Zones
    - Bypass on/off (*off.: bypassing only*)
- Names (*by zone nos.*)

(*Counters and zone groups are made available after programming of suitable controlling zones – type 16-31 or 64-79.*)

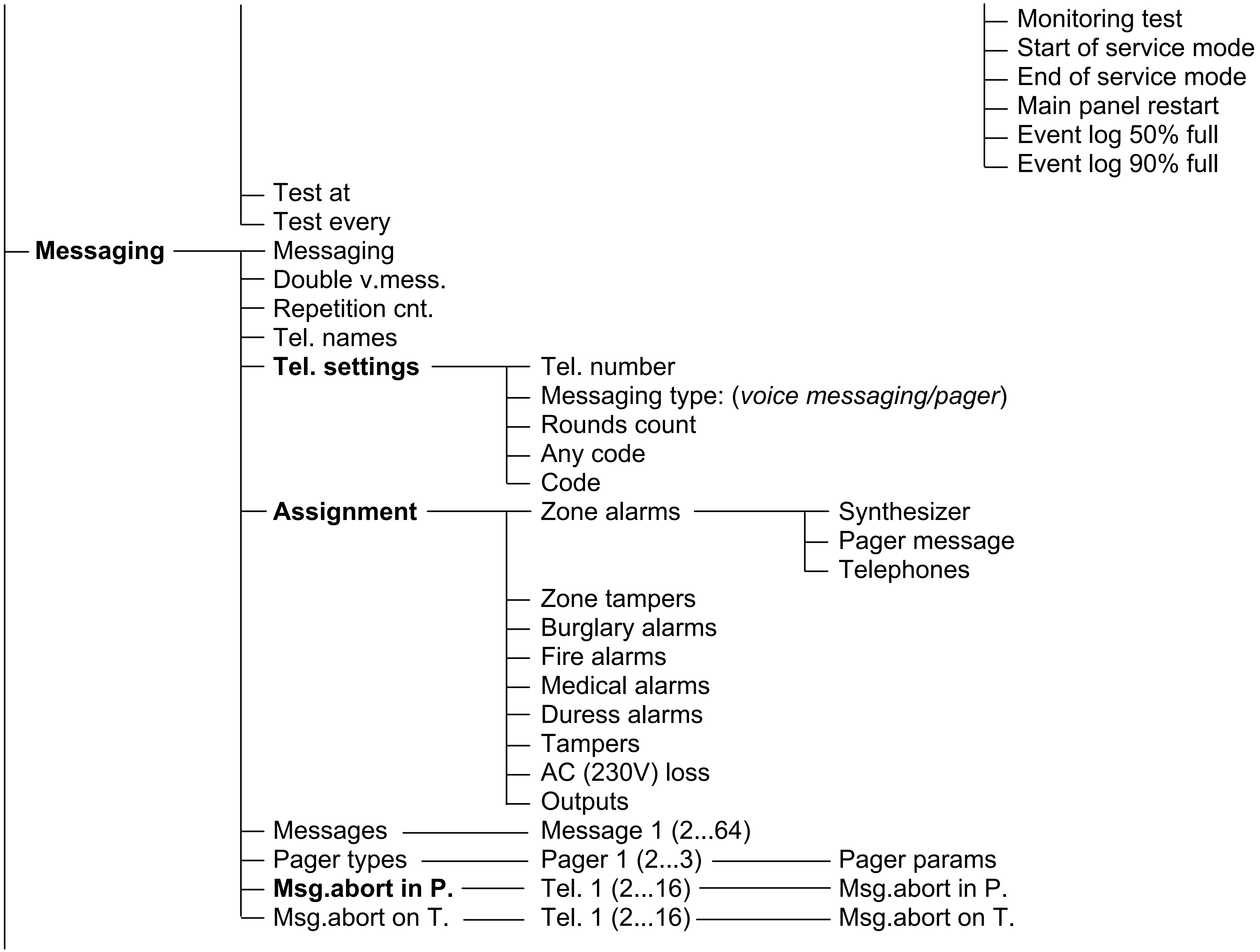
- **Outputs**
  - Details
    - Function
    - Cut-off time
    - Polarization +
    - Pulsating
    - Latch
    - Zones / Timers / Expanders / Outputs / Users / Doors / Voice mess. / Tel. switches (*triggering*)
    - LCD keypads / Master users / Arm mode sel. (*triggering*)
    - Partitions / Burg.tst.part. (*triggering*)
    - Fire.tst.part. (*triggering*)
    - Bypass.timers
    - Clear in parts.
    - Troubles
    - Name
  - Parameters
    - Function (*by output nos.*)
    - Cut-off time (*by output nos.*)
    - Options
      - Polarization +
      - Pulsating
      - Latch
  - Names (*by output nos.*)

- **Outputs groups**
  - Group 1 (2, 3, 4) outputs
  - Group 1 (2, 3, 4) name
  - Outs state by
- **Timers**
  - Times
    - Timer 1 (2...64)
  - Names
    - Timer 1 (2...64)
- **User schedules**
  - Settings
    - Schedule 1 (2...8) (*assign timers to schedule*)
  - Names
- **Monitoring**
  - Mon. TELEPHONE
    Mon.GPRS/ISDN
    Mon. ETHM-1
  - Dont rep.rsts.
  - Stations
  - Advanced
    - Long hsk.s1t1
    - Long hsk.s1t2
    - Long hsk.s2t1
    - Long hsk.s2t2
    - Long hsk.wait.
  - **Station 1**
    - Tel. 1 number
    - Tel. 2 number
    - Tel. 1 format
    - Tel. 2 format
    - Server address
    - Server port
    - Key (server)
    - Key (GPRS/ISDN)
    - Key (ETHM-1)
    - Repetition cnt.
    - Suspension time
    - TELIM prefix
    - Identifier 1 (2...8)
    - Identifier sys.
    - Event assign.

- **Station 2**
  - Tel. 1 number
  - Tel. 2 number
  - Tel. 1 format
  - Tel. 2 format
  - Server address
  - Server port
  - Key (server)
  - Key (GPRS/ISDN)
  - Key (ETHM-1)
  - Repetition cnt.
  - Suspension time
  - TELIM prefix
  - Identifier 1 (2...8)
  - Identifier sys.
  - Event assign.
- **Id. assignment**
  - Partitions
  - Zones
  - LCD keypads
  - Expanders
- TELIM codes
- **Event codes**
  - **Identifier 1** (2...8)
    - Zones
      - Alarm
      - Restore
      - Tamper
      - Tamper rst.
      - Trouble
      - Trouble rst.
      - Bypass
      - Unbypass
      - Violation

  - Partitions
    - Arm
    - Disarm
    - Clear alarm
    - Duress alarm
    - Defer autoarm
    - No guard
  - LCD keypads
    - Panic alarm
    - Fire alarm
    - Medical alarm
    - Tamper
    - Tamper rst.
    - Unauthorized
    - 3 bad codes
  - Expanders
    - Panic alarm
    - Fire alarm
    - Medical alarm
    - Tamper
    - Tamper rst.
    - Unauthorized
    - 3 bad codes
- **Identifier sys.**
  - Troubles
    - AC (230V) loss
    - Battery trouble
    - Settings clear
    - Monitoring trouble
    - Fire zones test
    - Burglary zones test
    - Real-time clock trouble
    - OUT1 trouble
    - OUT2 trouble

  - OUT3 trouble
  - OUT4 trouble
  - LCD keypads supply trbl.
  - Expanders supply trbl.
  - DTM bus trouble.
  - DT1 bus trouble
  - DT2 bus trouble
- Troubles rst.
  - AC (230V) ok
  - Battery ok
  - Settings restore from FLASH
  - Monitoring ok
  - Fire zones test finished
  - Burglary zones test finished
  - Real-time clock setting
  - OUT1 ok
  - OUT2 ok
  - OUT3 ok
  - OUT4 ok
  - LCD keypads supply ok
  - Expanders supply ok
  - DTM bus ok
  - DT1 bus ok
  - DT2 bus ok
- Other
  - RAM memory error
  - Call back
  - DWNL finished
  - Unsuccessful DWNL attempt
  - Manual test of monitoring
  - Periodical test of monitoring



- Monitoring test
- Start of service mode
- End of service mode
- Main panel restart
- Event log 50% full
- Event log 90% full

- Test at
- Test every

- **Messaging**
  - Messaging
  - Double v.mess.
  - Repetition cnt.
  - Tel. names
  - **Tel. settings**
    - Tel. number
    - Messaging type: (*voice messaging/pager*)
    - Rounds count
    - Any code
    - Code
  - **Assignment**
    - Zone alarms
      - Synthesizer
      - Pager message
      - Telephones
    - Zone tampers
    - Burglary alarms
    - Fire alarms
    - Medical alarms
    - Duress alarms
    - Tampers
    - AC (230V) loss
    - Outputs
  - Messages
    - Message 1 (2...64)
  - Pager types
    - Pager 1 (2...3)
      - Pager params
  - **Msg.abort in P.**
    - Tel. 1 (2...16)
      - Msg.abort in P.
  - Msg.abort on T.
    - Tel. 1 (2...16)
      - Msg.abort on T.

- **Tel.answ./ctrl.**
  - Answering
  - Double call
  - Rings count
  - On armed part. (*select partitions*)
  - Remote control
  - Users (all) (*assign remote switches to control*)
  - Users (t.code) (*assign remote switches to control*)
- **Note**
  - Text
  - Valid (*days*)
  - From (*date*)
  - For (*select user*)
  - Who can erase (*select user*)
- **System status**
  - Partitions
  - Zones
  - Troubles
  - **Supply voltage**
  - Radio devices
  - IP/MAC ETHM-1 (*IP address / MAC number of the ETHM-1 module*)
  - Modules version
- **Restarts**
  - Clear all
  - Clear settings
  - Clear codes
  - Settings<-FLASH
  - **Starter**

Menu of service functions for modules to be connected to the keypad bus (→Structure →Hardware →LCD keypads →Settings).

- **Settings**
  - *Mimic board*
    - Zones
      - Bypass pattern
      - Long violation pattern
      - No violation pattern
      - Tamper alarm pattern
      - Alarm pattern
      - Tamper memory pattern
      - Violation pattern
      - Tamper memory pattern
      - Alarm memory pattern
      - Zone ok pattern
    - Partitions
      - Entry time pattern
      - Exit time <10s pattern
      - Exit time >10s pattern
      - Armed pattern
      - Not armed pattern
    - Alarms
      - Fire alarm pattern
      - Alarm pattern
      - Fire memory pattern
      - Alarm memory pattern
      - No alarms pattern
    - What to show
      - Zn.1..64 + part.
      - Zn.65..128+part.
      - Zones 1..128
    - AC delay
    - RS communicat.
    - PTSA tamper

- *ETHM-1 module*
  - Use DHCP
  - DHCP-DNS
  - DNS
  - Port (WWW)
  - Address IP
  - Netmask
  - Gateway
  - Port (DloadX)
  - Port (others)
  - Key (DloadX)
  - Key (others)
  - Connect DloadX
  - Connect GuardX
  - Connect Intern.
  - Tamper
  - Fail. – event
  - Fail. – alarm

Menu of service functions for modules to be connected to the keypad bus (→Structure →Hardware →Expanders →Settings).

- **Settings**
  - *Partition keypad*
    - Lock feature
    - Lock
      - Lock feature
      - Relay ON time
      - Relay type
      - Unauth.event
      - Unauth.alarm
      - Max.door open
      - Dependent door1
      - Dependent door2
    - Master users
    - Users
    - Alarms
      - Fire alarm
      - Medical alarm
      - Panic alarm
      - Silent panic
      - 3 bad codes
    - Options
      - Quick arm
      - Fin.exit time
      - BI outs ctrl.
      - MONO outs ctr.
      - Part.blocking
      - Guard control
      - Changing code
      - Code* not dis.
      - Code* in arm
    - Signalling
      - Alarm (latch)
      - Alarm (time)
      - Entry time
      - Exit time
      - Auto-arm delay
      - Code entered
      - Chime zones

- Confirmation
- Backlight
- Auto backlight
- No autorst.3t.
- Partition

- *Code lock*
  - Lock
    - Lock feature
    - Relay ON time
    - Relay type
    - Unauth.event
    - Unauth.alarm
    - Max.door open
    - Dependent door1
    - Dependent door2
  - Master users
  - Users
  - Alarms
    - Fire alarm
    - Medical alarm
    - Panic alarm
    - Silent panic
    - 3 bad codes
  - Options
    - Part.blocking
    - Guard control
    - Changing code
  - Signaling
    - Code entered
    - Chime zones
  - Confirmation
  - Backlight
  - Auto backlight
  - No autorst.3t.
  - Partition

- *Wireless system controller*
  - No autorst.3t.
  - Tamper
  - Response period
  - New device
  - Active mode
  - Configuration
  - Filter
  - Remove device
  - Synchronization
  - Test mode on
  - Test mode off
- *Expander for proximity card readers; expander for "DALLAS" chip readers*
  - Lock feature
  - Lock
    - Lock feature
    - Relay ON time
    - Unauth.event
    - Unauth.alarm
    - Max.door open
    - Dependent door1
    - Dependent door2
  - Master users
  - Users
  - Readers
    - Reader A
    - Reader A sound
    - Reader A LED.
    - Reader A arms
    - Reader B
    - Reader B sound
    - Reader B LED
    - Reader B arms

- Al.rdrs tamper
- Hardw. signal.
- 3 wrong codes
- BI outs ctrl.
- MONO outs ctr.
- Part.blocking
- Guard control
- Code* not dis.
- Code* in arm
- C.long not dis
- Signalling
    - Alarm (latch)
    - Alarm (time)
    - Entry time
    - Exit time
    - Auto – arm delay
    - Chime zones
- No autorst.3t.
- Partition

Zones expander
(addressable z. exp.;
outputs expander;
zone / output expander)

- No autorst.3t.
- Tamper *(in partition)*
- AC loss delay

3.2 DLOADX – INSTALLER PROGRAM

The DLOADX program enables data exchange between the computer and the control panel, facilitates alarm system configuration, and ensures easy viewing of the status of zones, partitions, outputs, troubles, doors supervised by the control panel, as well as other components of the system. The program makes it also data conversion possible between the INTEGRA series panels, and between the CA-64 and INTEGRA 64 panels.

For the purpose of programming, the communication between computer and control panel can be established in a few ways:

- direct connection through the RS-232 port of the control panel mainboard (local programming),
- by means of telephone line via the control panel internal modem (this programming method makes available all the downloading functions, but as the transmission rate is limited to 300 bauds, it takes longer to perform the functions),
- by means of telephone line via an external modem connected to the RS-232 port on the control panel mainboard,
- through the GSM-4 or GSM LT-1 communication module, used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the GSM mobile telephone network,

Note: *The data transmission service (HSCSD/CSD - modem transmission) is usually available as part of the basic service pack offered by the cellular network operator, however before running the program it is advisable to make sure that you can use the network.*

- through the ISDN module used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the ISDN digital telephone cable network.
- through the ETHM-1 module (connected to the RS-232 port of the control panel mainboard), connecting with the computer via the Ethernet network (TCP/IP).

Irrespective of the chosen method of establishing connection between the program and the control panel, it is necessary that the communication identifiers programmed in the control panel / program be equal or have default values. After establishing communication with a new alarm system, in which the identifiers have default values, the DLOADX program offers random generated identifiers. They can be accepted or own identifiers can be entered. The identifier must have 10 characters. It can be composed of numerals and letters from A to F. Entering an identifier used for another system operated from the same computer by the DLOADX program is impossible.

The control panel stores and makes available to the user the date and time when the date were saved to the control panel, as well as the file name in the DLOADX program (user function: *Tests →File in DloadX*).

3.2.1 Local programming

Connection of the control panel RS-232 port and the computer port should be made in the same way as that for replacement of the control panel firmware (see Fig. 1, page 4).

In order to start local programming (downloading) from the computer you should:

1. Enter the **service code** from the keypad (by default 12345) and press [*].
2. Using the arrow keys, scroll the function list until the arrow indicates the function DOWNLOADING.
3. Press the [#] or [▶] key.
4. Select the item START DWNL-RS and press the [#] or [▶] key.

5. Start the DLOADX program on the computer. If the control panel RS-232 port is connected to the computer COM1 port, communication with the control panel will start automatically. Otherwise, click on the icon, and then on the window which will appear, and indicate the computer port through which communication is to be effected.
6. Establishing communication will be signaled on the monitor screen by a corresponding message. The message contents depends on whether the program has been connected to a new alarm system, or a system whose data have already been saved.

Note: *The downloading function will start automatically if the INTEGRA control panel is connected through the RS-232 port with the computer on which the DLOADX program is running, and then control panel power is turned on.*

The function of local programming from computer (downloading) can be ended by the command END DWNL-RS ([*service code*][*] →*Downloading* →*End DWNL-RS*). The function will be switched off automatically after 255 minutes have passed since the last use of the DLOADX program, and the service access was blocked or expired in the meantime.

3.2.2 Remote programming with the use of modem

The control panels have a built-in internal modem, the transmission rate of which is rated at 300 baud. With this speed, reading all the control panel settings and programming the new ones can take tens of minutes. The transmission rate imposes an additional restriction: an analog modem must be connected on the computer side. These limitations can be omitted by connecting an external modem to the control panel. This will enable programming with an identical speed as with local programming. The INTEGRA control panels can interact with external analog, ISDN and GSM modems. The table below shows available configurations for remote programming with the use of telephone line.

Control panel configuration	**Computer configuration**
Control panel with built-in modem	Computer with analog modem
Control panel with external analog modem	Computer with analog modem
	Computer with GSM modem
Control panel with external ISDN modem	Computer with ISDN modem
	Computer with GSM modem
Control panel with external GSM modem	Computer with analog modem
	Computer with ISDN modem
	Computer with GSM modem

Table 1. Ways to connect alarm control panel with computer for telephone communication.

When connecting the ISDN modem or GSM-4 & GSM LT-1 communication modules, connect the control panel RS-232 port and the module port using a suitable cable (Fig. 3). The ISDN modem analog output, if any, can be connected to the control panel TIP, RING terminals. Thus, if a connection is initiated from outside by the analog modem, the ring signal will be transferred to the control panel telephone connection and the call will be answered by the internal modem.

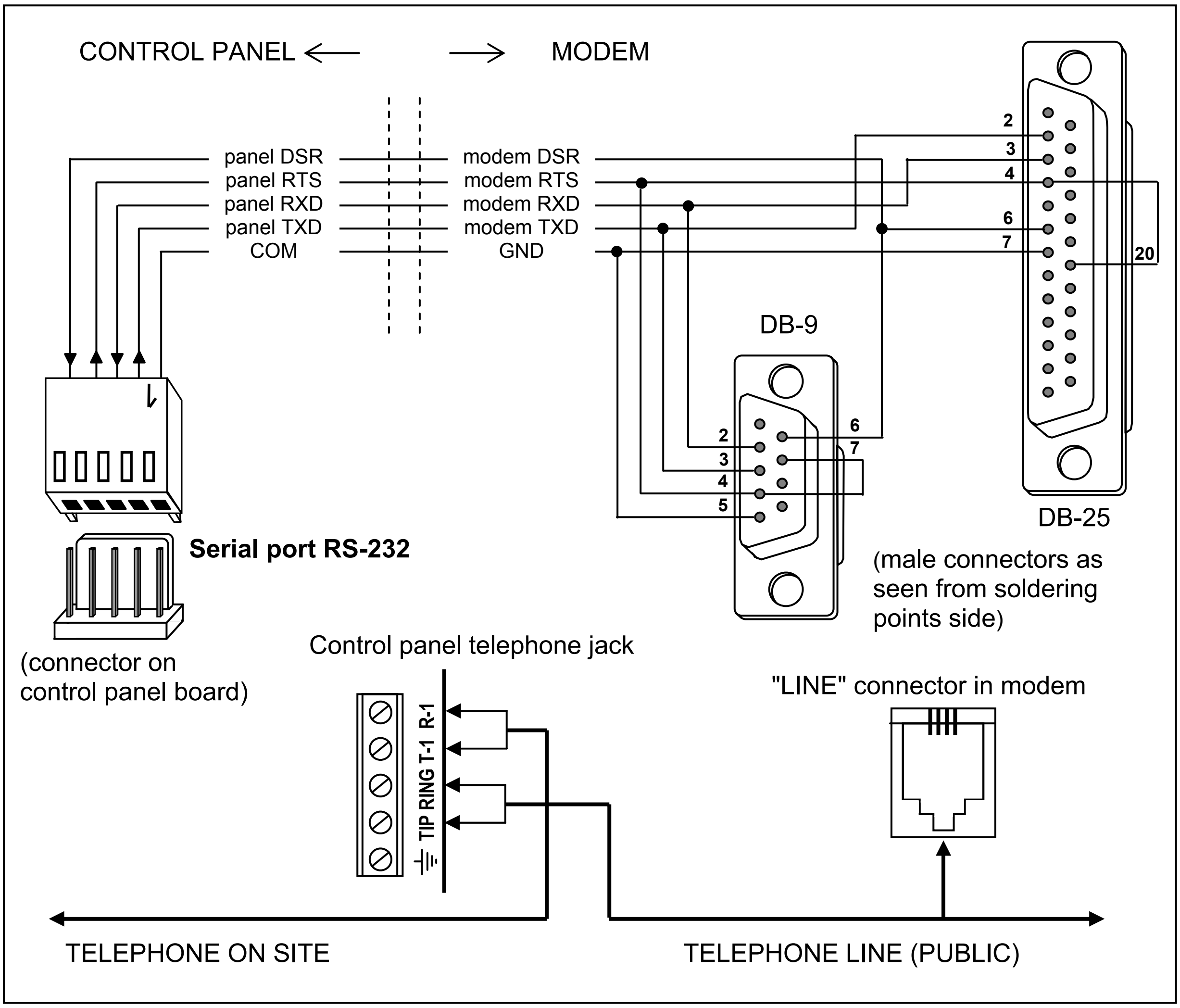


Fig. 2. Connection of external modem to the control panel.

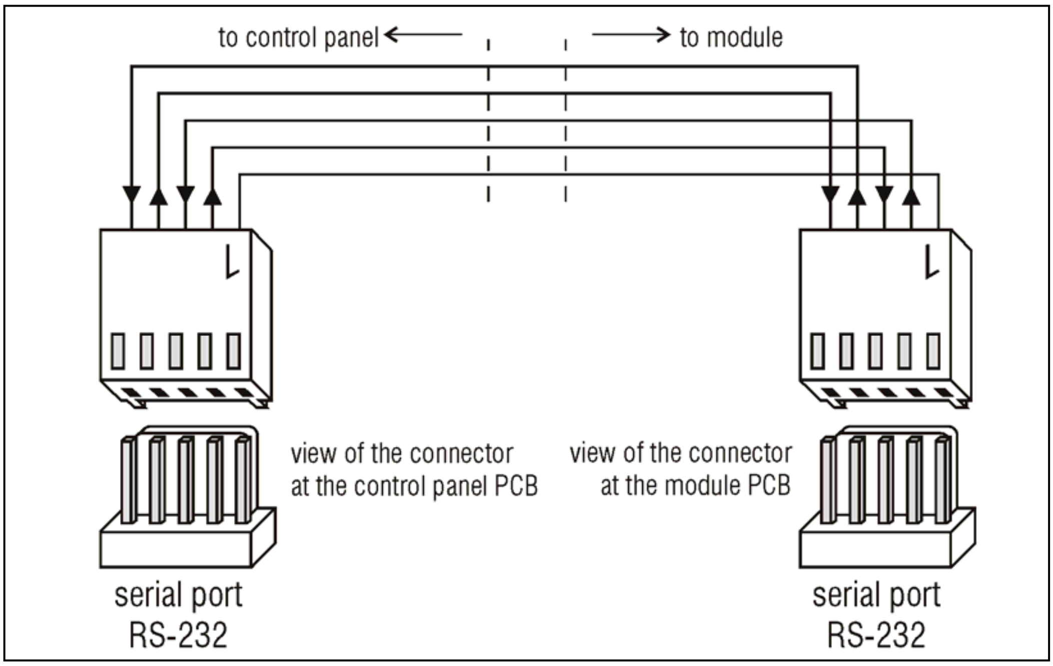
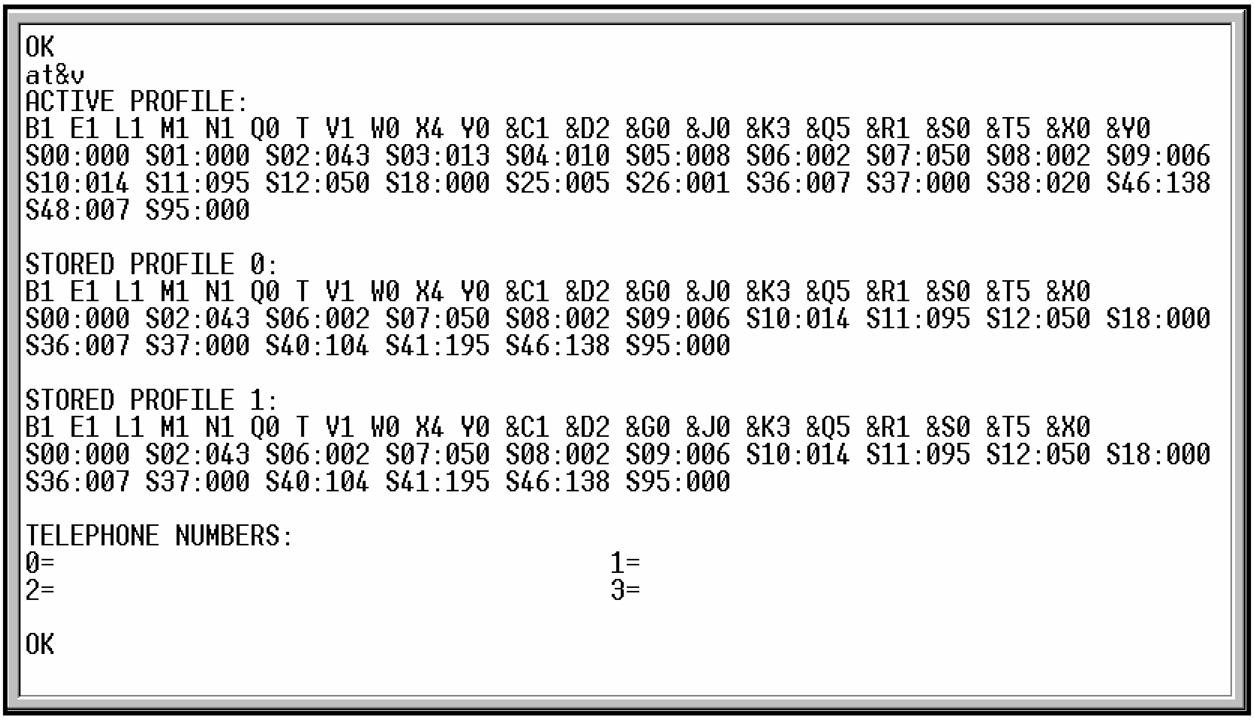

to control panel
to module
view of the connector at the control panel PCB
view of the connector at the module PCB
serial port RS-232
serial port RS-232

Fig. 3. Connection of RS-232 ports of INTEGRA panel and GSM-4, GSM LT-1,ISDN and ETHM-1 modules.

Before connection to the control panel, the modem must be suitably prepared: connect it to the computer and, using the *Terminal* type program, set the suitable operating mode and save its settings.

You should follow the procedure below:

1. Check whether the modem is connected to the terminal – modem should answer OK after writing at↵ (if modem does not answer, try ate1↵ ; if there is still no answer, check the modem connection to the computer and make sure that the COM port is properly selected in settings of the program of *Terminal* type).
2. Check the settings of parameters which determine the modem operation mode. After the command at&v↵, the modem will present a list of parameters for programming. A typical set of parameters is shown in Fig. 4. For the control panel to properly work with the modem just a few parameters must be set – the parameter block stored as “profile 0" ("STORED PROFILE 0" in Figure 4) must include E1 Q0 V1 X4 &D2 &S0 and S00:000.



```
OK
at&v
ACTIVE PROFILE:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0 &Y0
S00:000 S01:000 S02:043 S03:013 S04:010 S05:008 S06:002 S07:050 S08:002 S09:006
S10:014 S11:095 S12:050 S18:000 S25:005 S26:001 S36:007 S37:000 S38:020 S46:138
S48:007 S95:000

STORED PROFILE 0:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0
S00:000 S02:043 S06:002 S07:050 S08:002 S09:006 S10:014 S11:095 S12:050 S18:000
S36:007 S37:000 S40:104 S41:195 S46:138 S95:000

STORED PROFILE 1:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0
S00:000 S02:043 S06:002 S07:050 S08:002 S09:006 S10:014 S11:095 S12:050 S18:000
S36:007 S37:000 S40:104 S41:195 S46:138 S95:000

TELEPHONE NUMBERS:
0=                                     1=
2=                                     3=

OK
```

Fig. 4. Correct setting of external modem parameters.

3. If the parameters mentioned above are set correctly, the modem is ready for operation with the control panel. If any parameter is set to other value, set it properly. Command for parameter setting consists of fixed prefix AT and parameter value required (for example, when profile specifies E0 V0, the command for setting the proper parameter value is ate1v1↵, after which the modem answers OK).
4. Having set the parameter values acc. to the list mentioned above in point 2, save the settings in the “profile 0" (using the at&w0↵ command).
5. Finally, you can check whether all parameters are properly saved – after the atz↵ command followed by at&v↵, the settings in ACTIVE PROFILE should be the same as in STORED PROFILE 0 (note: often STORED PROFILE set contains less parameters than ACTIVE PROFILE set, which is normal).

Notes:

- *The modem S0 register is to be set with the ats0=0 command (in Figure 4 the modem register is shown in slightly different notation S00:000).*
- *When restarting the modem, the control panel generates ATZ command, which sets parameters in accordance with the values saved in the “profile 0". Therefore, the current*

values of parameters mentioned in point 2 ("ACTIVE PROFILE") are not important, but it is important that they be correctly set in the "profile 0".

Every configuration in which an external modem is connected to the control panel requires that the option **EXTERNAL MODEM** (*Service mode →Options →Tel. options →External modem*) be enabled in the telephone options. Additionally, if an ISDN or GSM modem is connected to the panel as an external modem, the option **ISDN/GSM MODEM** (*Service mode →Options →Tel. options. → ISDN/GSM modem*) should be enabled.

Telephone communication requires that telephone numbers be programmed. The procedure is as follows:

1. Start the service mode.
2. Enter the submenu CONFIGURATION.
3. Start the function DLOADX TELEPHONE.
4. Program the computer telephone number. Numerals and special characters can be used. In order to program special characters in the telephone number by means of LCD keypad you should:
   - enter the digit to which the special character is assigned (see Table 2);
   - press the ▼ key – a flashing cursor will appear (large rectangle);
   - press the ◀ key to move the cursor onto the previously entered digit
   - press the key with the same digit again – the special character will be displayed (if characters "a", "b", "c" or "d" are to be entered, press repeatedly the key with digit 8).

Special character	Numeric key	Description of function
A	0	end of number
B	1	switch to pulse dialing
C	2	switch to tone dialing
D	3	wait for additional signal
E	4	3-second pause
F	5	10-second pause
∗	6	∗ signal in DTMF mode
#	7	# signal in DTMF mode
a b c d	8	other signals are generated in DTMF mode

Table 2. Assignment of special characters to numeric keys in the keypad.

Note: *Do not program the A character (end of number marker) in telephone numbers. It is added automatically after the character that was entered as the last one.*

In the telephone programming mode, access to the control panel is protected by a ten-byte code (over 1.2x10^{24} combinations). This ensures a very good safeguard against an attempt to break into the control panel by means of the telephone links. Additionally, the control panel is protected against attempts of scanning the access code – after three consecutive attempts to get access to the panel by using wrong codes during one session, the modem signal answering engine is disabled for 30 minutes.

There are 4 methods to initiate communication between the alarm control panel and the computer:

1. Connection initiated by the control panel.

2. Connection initiated from the DLOADX program.
3. Connection initiated from the DLOADX program, but the control panel calls back and sets up the connection.
4. Connection initiated by means of SMS-message, after reception of which the control panel sets up the connection.

Connection initiated by the control panel

This method of establishing connection requires that the computer telephone number be programmed in the control panel (*Service mode* →*Configuration* → *DloadX tel. No*). Start the DLOADX program and initialize the modem in the computer. Communication will be established after the function START DWNL-TEL ([*code*][*] →*Downloading* →*Start DWNL-TEL*) is started from the keypad. The function is available to the service and master user having the DOWNLOADING authority. Established connection is indicated by suitable messages on the keypad display and computer monitor.

Connection initiated from the DLOADX program

The control panel telephone number should be programmed in the DLOADX program. The option ANSWERING – MODEM (*Service mode* →*Options* →*Tel. options* →*Modem answer.*) must be enabled in the control panel. Additionally, you must specify the number of rings before the control panel goes off hook (*Service mode* →*Options* →*Rings to answer*) and determine whether the connection is to be established after a single or double call (*Service mode* →*Options* →*Tel. options* →*Double call*). In order to initiate the connection by the DLOADX program, click on the icon and select suitable configuration of the connection. After the programmed number of rings (or after the second number call, if the DOUBLE CALL option has been selected) the control panel will answer the call and the connection will be established.

Notes:

- *The computer telephone number cannot be programmed in the control panel, if the connection is to be set up by the computer (the costs are charged to the computer telephone number).*
- *The number of rings and the DOUBLE CALL option do not apply to the control panels with external ISDN or GSM modem.*

Connection initiated from the DLOADX program, but the control panel calls back and sets up the connection

The control panel telephone number should be programmed in the DLOADX program, and the computer telephone number - in the control panel. Additionally, the option ANSWERING – MODEM (*Service mode* →*Options* →*Tel. options* →*Modem answer.*) must be enabled in the control panel. You need also do specify the number of rings after which the control panel will go off hook (*Service mode* →*Options* →*Rings to answer*) and determine whether the connection is to be established after a single or double call (*Service mode* →*Options* →*Tel. options* →*Double call*). In order to initiate the connection by the DLOADX program, click on the icon and select suitable configuration of the connection. After the programmed number of rings (or after the second number call, if the DOUBLE CALL option has been selected) the control panel will answer the call, acknowledge receiving the call, and disconnect. Then it will call back the number programmed in the control panel and the connection will be established.

Note: *The number of rings and the DOUBLE CALL option do not apply to the control panels with external ISDN or GSM modem.*

Connection initiated by means of SMS, after reception of which the control panel sets up the connection

This programming method requires that a GSM module be connected to the control panel to serve as a modem. The option ANSWERING – MODEM (*Service mode* ➔*Options* ➔*Tel. options* ➔*Modem answer.*) must be enabled and the computer telephone number programmed in the control panel. The code for starting remote communication between control panel and computer should be programmed in the GSM module. Start the DLOADX program in the computer. Having sent an SMS containing the code to the GSM module number, the control panel will call the computer telephone number stored in its memory and establish connection with the program. The control panel can also call another number, indicated in the contents of sent SMS. The SMS should then have the following form: "**xxxxxx=yyyy.**", where "xxxxxx" denotes the code for starting remote communication, and "yyyy" – telephone number, the control panel is to call back. A dot is to be put after the telephone number.

3.2.3 Remote programming through the Ethernet (TCP/IP) network

This method of programming requires that a ETHM-1 module be connected to the control panel. The RS-232 port of the control panel should be connected to the module port by means of a suitable cable (Fig. 3). The way of control panel / module configuration is described in the ETHM-1 module manual.

3.3 GUARDX – USER PROGRAM

The GUARDX program makes possible visualization of the protected facility on the computer monitor, operating the system from an independent on-screen LCD keypad, access to the event log, as well as creating and editing the system users. For the purpose of programming, communication between the computer and the control panel can be established in a number of ways:

- direct connection through the RS-232 port of LCD keypad - this operating mode can be used simultaneously on all connected LCD keypads,
- LAN/WAN network (TCP/IP communication) by means of the *GUARDSERV* program running on the computer connected to the RS-232 port of LCD keypad,
- by means of telephone line via an external modem connected to the RS-232 port on the control panel mainboard,
- through the GSM-4 or GSM LT-1 communication module, used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the GSM mobile telephone network,
- through the ISDN module, used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the ISDN digital telephone network.
- through the ETHM-1 module, connecting with the computer via the Ethernet network.

3.4 Web browser

The Java application to be started in the web browser will make a virtual keypad available to enable the control panel to be operated in much the same way as by using the regular LCD keypad. This method of programming requires that a ETHM-1 module be connected to the control panel. The way of control panel / module configuration is described in the ETHM-1 module manual.

3.5 Mobile phone

The cellular phone with a special application installed will adopt the role of a remote keypad. It enables the control panel to be operated in much the same way as by using the regular

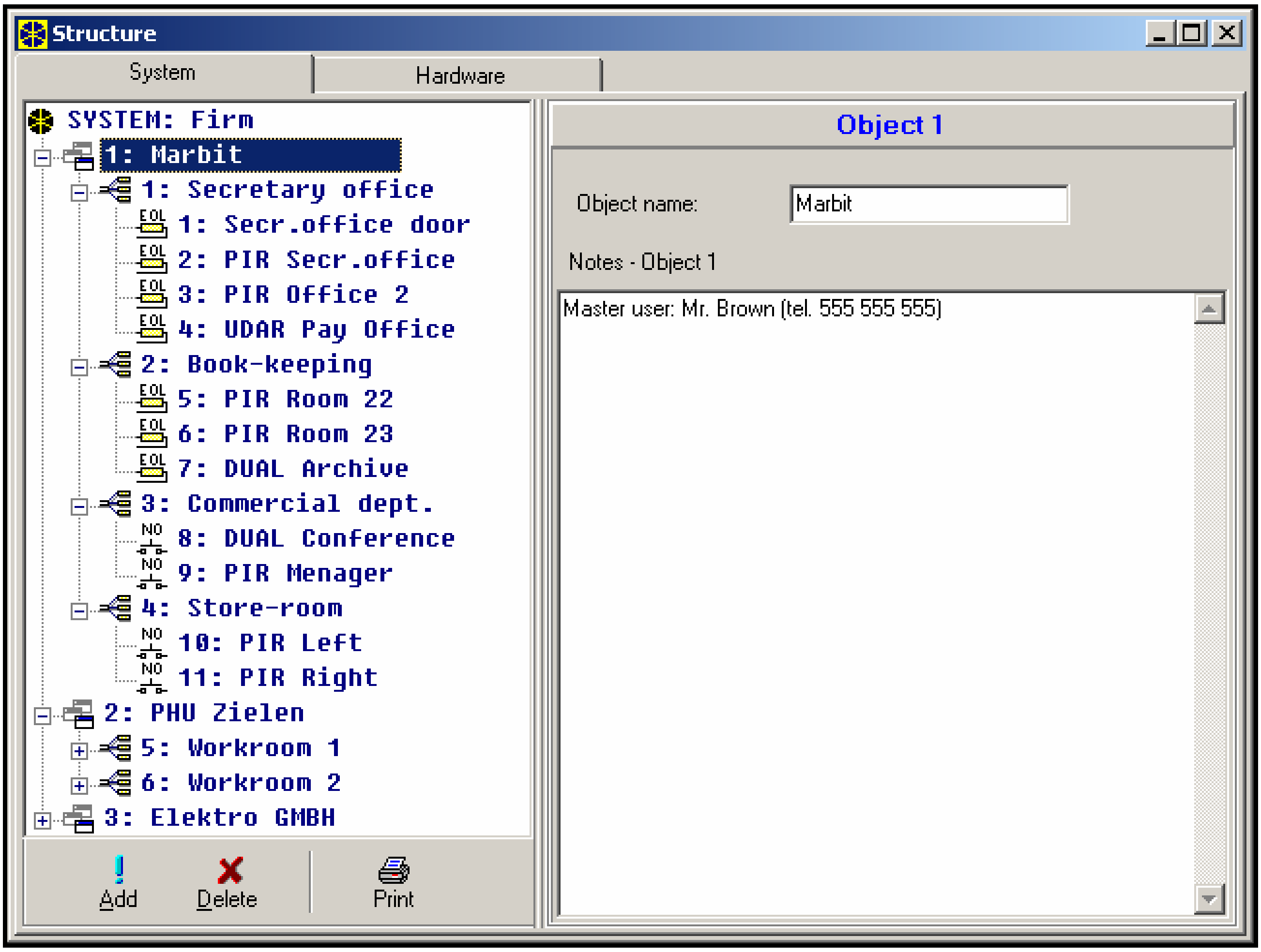
LCD keypad. This method of programming requires that a ETHM-1 module be connected to the control panel. Configuration of the control panel and module, as well as application to be downloaded for the mobile phone, are described in the ETHM-1 module manual.

4. System structure

4.1 Objects

Depending on its size, the INTEGRA control panel makes it possible to create 1, 4 or 8 objects. The objects are created in the service mode by using the EDIT OBJECT function or the DLOADX program. They are recognized as separate alarm systems. It is possible to configure the control panel so that individual objects have their own separate controls (LCD keypads, partition keypads, code locks) and signaling units, or, alternatively, they share the equipment (LCD keypads and signaling units).

In the case of common LCD keypads, the controlled partition is recognized by the code of the user who gives the command (i.e. the LCD keypad is not "assigned" to the object or partition.



- SYSTEM: Firm
  - 1: Marbit
    - 1: Secretary office
      - 1: Secr.office door
      - 2: PIR Secr.office
      - 3: PIR Office 2
      - 4: UDAR Pay Office
    - 2: Book-keeping
      - 5: PIR Room 22
      - 6: PIR Room 23
      - 7: DUAL Archive
    - 3: Commercial dept.
      - 8: DUAL Conference
      - 9: PIR Menager
    - 4: Store-room
      - 10: PIR Left
      - 11: PIR Right
  - 2: PHU Zielen
    - 5: Workroom 1
    - 6: Workroom 2
  - 3: Elektro GMBH

Object 1

Object name: Marbit

Notes - Object 1

Master user: Mr. Brown (tel. 555 555 555)

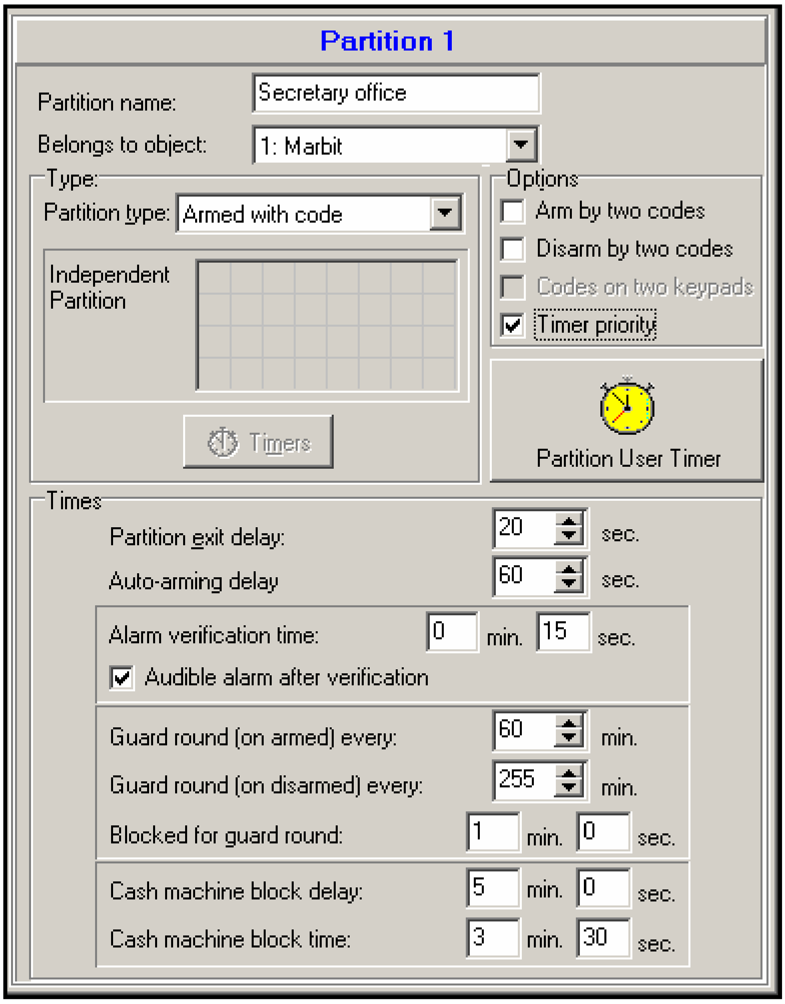
Fig. 5. System division into objects and partitions.

Events from particular objects are sent to the monitoring station with individual identifiers. After selecting the Contact ID format, the control panel sorts the events automatically. For other formats, the events are assigned to identifiers by the installer, according to the assignment of system components (zones, partition, users) to individual objects.

4.2 Partitions

The partition is a **group of zones** to supervise a selected part of the object, which are armed or disarmed at the same time. The partition can only belong to one object. Division of the object into partitions improves security of the object (some object partitions may be armed while the others are still accessible to the users), and permits to restrict the users' access to some parts of the facility. For example, in the facility shown in Figure 5, the workers of Commercial Department (partition 3) will not be able to enter the book-keeping offices (partition 2), unless they are granted authorization to arm / disarm the "Book-keeping" partition.

A partition can be created in the service mode with the use of the EDIT OBJECT function, by assigning it to the selected object. When creating a partition, it can be given a **name** (up to 16 characters). Also, the **partition type** should be defined (by default: ARMED WITH CODE). The function also removes partitions from the given object.



Partition 1

Partition name: Secretary office

Belongs to object: 1: Marbit

Type:

Partition type: Armed with code

Independent Partition

Timers

Options

☐ Arm by two codes

☐ Disarm by two codes

☐ Codes on two keypads

☑ Timer priority

Partition User Timer

Times

Partition exit delay: 20 sec.

Auto-arming delay 60 sec.

Alarm verification time: 0 min. 15 sec.

☑ Audible alarm after verification

Guard round (on armed) every: 60 min.

Guard round (on disarmed) every: 255 min.

Blocked for guard round: 1 min. 0 sec.

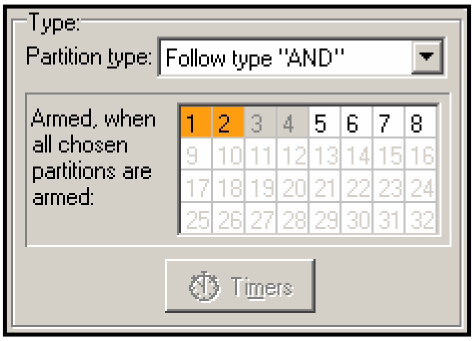
Cash machine block delay: 5 min. 0 sec.

Cash machine block time: 3 min. 30 sec.

Fig 6. Partition settings.

The INTEGRA control panel makes it possible to create the following types of partitions:

- **Armed with code** – the basic type of partition. Arming and disarming is performed by the user. Partition of this type is provided with a timer of its own to arm and/or disarm it, if it was not done earlier by the user.
- **With temporary blocking** – it is a version of the previous type of partition. The difference is that at the time of arming the control panel asks to indicate the blockage time period. Disarming of this partition is only possible after expiry of the blockage time. To disarm the partition before the blockage time is up you have to use a code with ACCESS TO TEMPORARY BLOCKED PARTITIONS authority, or another code, if an alarm occurred in that partition.
- **Follow type "AND"** – the partition controlled by status of other partitions. This partition is not armed directly by the user, but automatically – when all partitions indicated to the control panel become armed. The list of partitions is defined by the service when creating the dependent partition. The arming time is recorded in the event log, with indication of the user who armed the last partition from the list. When any partition from the list is disarmed, the dependent partition will be disarmed as well. Figure 7 shows the selection field of partitions that control partition 3 (partitions 1 and 2 are selected, other colors of background for partitions 3 and 4 show that partitions 3 and 4 cannot be selected for controlling the dependent partition) For FOLLOW



Type:

Partition type: Follow type "AND"

Armed, when all chosen partitions are armed:

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Timers

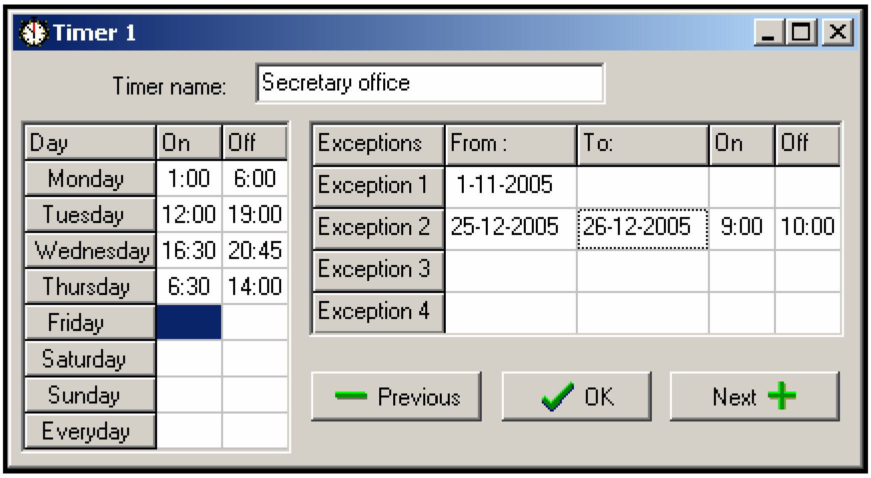
Fig. 7. Definition of FOLLOW TYPE "AND" partition.

TYPE "AND" partition no exit delay is defined – the moment of switching over from "exit delay" to "armed" mode is set by the last partition from the control list entering the armed status. The dependent partitions cannot be controlled by timers.

Note: *FOLLOW TYPE "AND" partitions are normally used for protection of common corridors.*

- **Follow type "OR"** – the partition becomes armed when any partition from the list of control partitions becomes armed. The partition is disarmed at the moment when the last partition from the list is disarmed. The exit delay time is the same as for the controlling partition which causes arming of the FOLLOW TYPE "OR" partition.
- **Access according to timer** – the partition is controlled by the user, but partition arming and disarming is only possible within time periods determined by operation of selected timers. Depending on the control panel size, an option with 16 or 32 timers is provided. Beyond those time periods neither arming, nor disarming of the partition is possible. For example, if the timer shown in Figure 8 is selected to control access to the "Secretary office" partition, the partition arming / disarming will be possible according to schedule – on Monday between 16:30 and 16:45, on Friday between 18:00 and 18:15 and so on, except for the time periods given in the timer exception table.

Note: *The ACCESS TO TEMPORARY BLOCKED PARTITIONS authority allows the user to freely control the partition armed mode, irrespective of the timer status.*



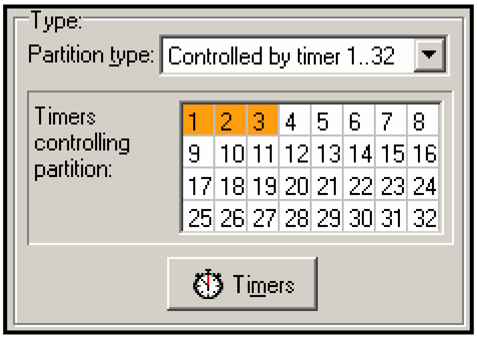
Timer name: Secretary office

Day	On	Off
Monday	1:00	6:00
Tuesday	12:00	19:00
Wednesday	16:30	20:45
Thursday	6:30	14:00
Friday		
Saturday		
Sunday		
Everyday		

Exceptions	From :	To:	On	Off
Exception 1	1-11-2005			
Exception 2	25-12-2005	26-12-2005	9:00	10:00
Exception 3				
Exception 4				

Fig. 8. Timing for CONTROLLED BY TIMER partition.

- **Controlled by timer** – the partition, which is armed in time periods determined by selected timers, and may also be controlled by the user code. When creating the CONTROLLED BY TIMER partition, you should specify the list of timers which set the periods when the partition is armed. Depending on the control panel size, an option with 16 or 32 timers is provided. The control panel analyzes the status of timers selected, and, if any timer status changes to "ON", the control panel arms the partition. Countdown of the exit delay time takes place before entering the full armed status. Disarming occurs when all the selected timers are "OFF". The partition can be also controlled by means of a separate **PARTITION USER TIMER**, whose mode of operation is programmable through the CHANGE OPTION user function. This timer controls the partition in much the same way as the other timers. This method to control the partition armed status is closely connected with the **TIMER PRIORITY** option.



Partition type: Controlled by timer 1..32

Timers controlling partition:

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Fig. 9. Selection of partition controlling timers.

Note: *When the partition is armed by the timer, the “Automatic arming" event is recorded. The timer number is included in the event. The "0" number indicates that the user timer armed the partition.*

The following **options** and **time settings** can be programmed for the partition:

Arm by two codes - arming after two different codes authorized to control the partition are entered in succession.

Disarm by two codes - disarming after two different codes authorized to control the partition are entered in succession.

Codes on two keypads - enabling this option will prevent codes to be entered from the same keypad (which applies to arming/disarming by means of two codes).

Timer priority - with this option selected, the timer will always perform arming and disarming according to the preset times. With this option deselected, the disarming will only follow if the arming is performed by timer - if the user sets armed mode with a code, the timer will not disarm the partition.

EXAMPLE: If the partition is armed/disarmed by timer every day, and the user is leaving and wants the armed mode to be on for a longer period of time - he will arm the partition himself. With the "timer priority" option disabled, the timer will not disarm the partition at the preset time and the user will not have to remember blocking the timer. When the user comes back and disarms the partition by using the code, the automatic control of the partition is restored according to the timer settings.

Partition user timer – see: **Controlled by timer partition** (for the DLOADX program the function is only available during connection with the control panel).

Partition exit delay - countdown of the partition arming delay as from the moment of entering the code or activating the timer to the actual arming of the partition.

Exit delay clearing – if this option is enabled for a partition, you can reduce the exit time countdown by entering [9][#] from the keypad / partition keypad. The partition will be armed immediately. The exit time clearing is only available from the same keypad / partition keypad, from which the partition was armed. See also LCD keypad option: EXIT DELAY CLEARING ENABLE.

Auto-arming delay - the time by which the **timer** will delay the automatic arming of a partition. Countdown of this time may be indicated on the partition keypads, LCD keypads and on the control panel outputs. Entering a value bigger than zero will enable an additional menu, which makes it possible to delay auto-arming (by entering a deferment time). During the auto-arming countdown it is possible to block the auto-arming function (until the next auto-arming time) by entering zeros alone in the DEFER AUTO-ARM user function. The delay countdown completed, the control panel begins the countdown of the "partition exit time" (provided that it has been set).

Alarm verification time - if the partition contains zones with selected **prealarm** option, then alarm on violation of such a zone will only be triggered if during the alarm verification time another zone with enabled prealarm option is violated.

Audible alarm after verification - with this option enabled there will be no audible signaling of unverified alarm (prealarm), i.e. violation of the zone with PREALARM option "on". The unverified alarm (prealarm) can be signaled on output type 9. DAY ALARM, 12. SILENT ALARM or 116. INTERNAL SIREN. The audible signaling will only be triggered after alarm verification (violation of another zone with enabled PREALARM option during alarm verification).

Guard round (on armed) every – setting the maximum period of time that can elapse since the last guard round when the partition is armed. If the time is exceeded, the control panel will record the "no guard round" event. Programming the value "0" will disable the guard round control.

Guard round (on disarmed) every – setting the maximum period of time that can elapse since the last guard round when the partition is disarmed. If the time is exceeded, the control panel will record the "no guard round" event. Programming the value "0" will disable the guard round control.

Blocked for guard round – When the partition round requires violation of detectors and the guard is not authorized to switch the detectors off, it is possible to set the partition blocking time period, which starts when the guard enters his code (read in the card / chip) to make a round.

The partition can also be bypassed by entering the TEMPORARY PARTITION BYPASSING type of code. The bypass time value is to be specified individually for particular codes.

Cash machine block delay

Cash machine block time

These times are to be programmed if the system supervises the cash machines (dispensers) by means of the 24H CASH MACHINE zones. Just one cash machine may be assigned to each partition. Access to the cash machine is possible after entering the ACCESS TO CASH DISPENSER type of code. Entering the code from a keypad will start the “time to approach" the cash machine (24H CASH MACHINE zone is still armed), followed by countdown of the bypass time (during the countdown the 24H CASH MACHINE zone is bypassed).

4.3 Zones

The zone in the alarm system is the interface of mainboard, LCD keypad or expansion module. Two electrical wires, commonly known as the "**line**", which is terminated with an alarm detector or another type of detector, are connected between the zone terminal and the common ground. Besides the detector, the electric circuit may incorporate the EOL parameter, i.e. a resistance which terminates the line. Depending on the detector configuration, it can be a 2.2kΩ resistor or 2 resistors 1.1kΩ each).

4.3.1 Identification and numbering of zones in the system

The number of available (existing) zones is recognized by the control panel in the process of expansion module identification. Therefore, prior to assignment of the zones to partitions, it is necessary to:

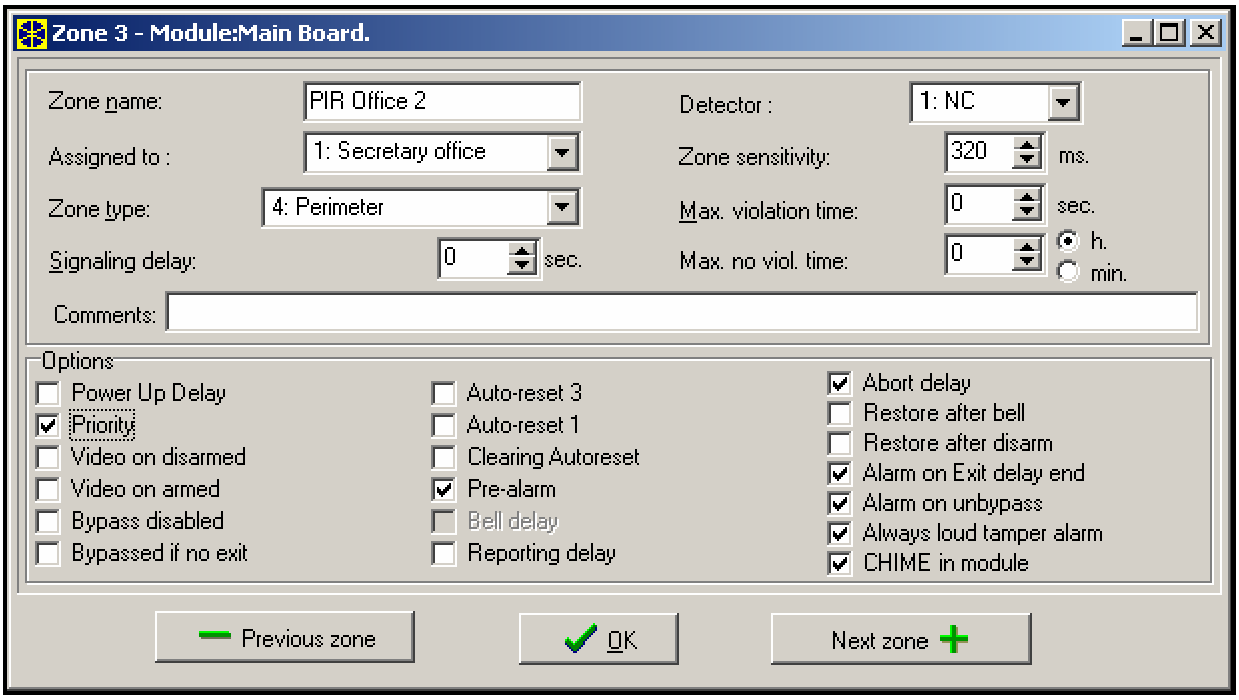
- complete the whole system installation,
- perform identification of keypads, expanders and zones (using functions available from the control panel LCD keypad in the service mode),
- when the control panel is programmed by means of computer - download the data from the control panel to the computer,
- perform logical partitioning of the system (creating additional objects, assigning partitions to the objects),
- assign zones to the created partitions.

Notes:

- *After restart of the settings (also in a new control panel), most of the service mode functions are not available until the control panel completes identification of hardware.*
- *The control panel will automatically assign numbers of the system zones to those of the mainboard and expanders (see the "CA-64 E Zone Expander" manual). The sequence of zone assignment depends on the addresses set at the expanders. The mainboard zones always carry the initial numbers: depending on the board size, these can be numbers 1-4, 1-8 or 1-16.*
- *The expander of addressable zones at the INTEGRA control panels can be installed together with other zone expanders. The identification process will assign to that expander*

a number of zones being a multiple of 8, depending on the number of actually connected addressable detectors which have an addressable module installed. Identification of the addressable zones (e.g. after adding some zones into the system) is carried out jointly with expander identification.

- *On the LCD keypad, the expander addresses in the name programming function are given in hexadecimal format in the following manner:*
  - *addresses from **00** to **1F** refer to the first expander bus (the numbering corresponds to the addresses set at microswitches – default names: **Expander 01** ... **Expander 32**)*
  - *addresses from **20** to **3F** refer to the second expander bus in the INTEGRA 64 and INTEGRA 128 control panels (continuation of the first bus addresses calculated as: microswitch setting +32 (20 in hexadecimal format) default names: **Expander 33** ... **Expander 64**.*
- *The same zone cannot be assigned to several partitions at the same time. However, it is possible to create partitions dependent on the status of other selected system partitions.*



Zone 3 - Module:Main Board.

Zone name: PIR Office 2

Assigned to : 1: Secretary office

Zone type: 4: Perimeter

Signaling delay: 0 sec.

Detector : 1: NC

Zone sensitivity: 320 ms.

Max. violation time: 0 sec.

Max. no viol. time: 0 ● h. ○ min.

Comments:

Options

□ Power Up Delay
☑ Priority
□ Video on disarmed
□ Video on armed
□ Bypass disabled
□ Bypassed if no exit
□ Auto-reset 3
□ Auto-reset 1
□ Clearing Autoreset
☑ Pre-alarm
□ Bell delay
□ Reporting delay
☑ Abort delay
□ Restore after bell
□ Restore after disarm
☑ Alarm on Exit delay end
☑ Alarm on unbypass
☑ Always loud tamper alarm
☑ CHIME in module

Fig. 10. Details of zone settings.

4.3.2 Parameters

Zone name - up to 16 characters

Assigned to partition

Panel reaction type (see: *Zone types*)

Alarm delay / Entry delay / Signaling delay / Surveillance time / Bypass time (parameter name depends on the control panel reaction type)

Keypad number – refers to type 58 zones: TECHNICAL - DOOR BUTTON.

Arming mode - the following armed modes are to be selected for type 80 and 82 zones:

1 – normal armed mode;

2 – INTERIOR DELAYED zones (type 3 zones) will be bypassed, EXTERIOR (type 8 zones) will trigger silent alarm, and the other ones - audible alarm;

3 – same as 2, but the DELAYED zones type 0, 1 and 2 will act as instant ones.

Group – for zone types 80, 81 and 83 it is possible to indicate one of 16 partition groups which will be controlled by means of the zone. These types of zones can also only control the partition they belong to (select 0 in the DLOADX program).

Detector configuration – configuration of the connected detector (NO, NC, EOL etc.). The INTEGRA control panel enables lines terminated with any detectors to be connected to the zones in the following configurations:

NC (detector with normally closed output),
NO (detector with normally open output),
EOL (detector in configuration with end of line resistor),
2EOL/NO (NO type detector in configuration with double end of line resistor),
2EOL/NC (NC type detector in configuration with double end of line resistor).

Zone sensitivity - the necessary duration of the actual zone violation until it is recorded by the control panel (typically approx. 0.5 sec., e.g. for the PANIC button a shorter time is recommended).

Max. violation time / Max. door opening time – exceeding the maximum time of violation / door opening is recognized by the control panel as a detector failure (e.g. damaging or masking the detector) / door. The "0" value will deactivate the time control. The time can be programmed in seconds or minutes.

Max. no violation time - exceeding the maximum time of no violation is recognized by the control panel as a detector failure (e.g. damaging or masking the detector). The "0" value will deactivate the time control. The time can be programmed in seconds or minutes.

Comment – this field is intended for entering important information regarding the particular zone. Length of the comment is limited to 256 characters.

4.3.3 Options

Power up delay - the zone will be bypassed for 120 sec. after power is switched on (which prevents triggering alarms e.g. when starting the alarm control panel).

Priority - this option makes arming impossible, if the zone with activated option is violated (e.g. in case when windows have been left open, etc.).

Note: *Prior to arming it is possible to preview the names of violated zones for which the* PRIORITY *option has not been activated. To do so, select the "Zones bef. arm" (→Service mode →Options →Various options).*

Disarm on violation – option for type 82 zone - consecutive violations of the zone alternately arm / disarm the partition. If the option is not selected, zone violation will arm and end of violation will disarm the partition.

CHIME in module – zone violation can be signaled in partition keypads, code locks and expanders of proximity card / DALLAS chip readers assigned to the same partition as the zone (the option CHIME must be enabled in the expander).

Video On Disarmed - violation of the zone will activate the VIDEO ON DISARMED type output (intended for starting cameras and video recorders).

Video On Armed - violation of the zone will activate the VIDEO ON ARMED type output (intended for starting cameras and video recorders).

Bypass disabled - the zone cannot be bypassed by the "zone bypass" user function.

Bypassed if no exit - the zone will be automatically bypassed, if during the zone exit delay no zone of the ENTRY/EXIT or EXIT type is violated.

Alarm if armed – option available to type 64-79 zones, when the **NO BYPASS IN ARMED** option is selected. Violation of the zone when the partition it belongs to is armed will trigger an alarm (provided that the control panel has recorded the partition exit after arming).

Auto-reset 3 - the zone will be automatically bypassed if 3 alarms have been triggered since arming time.

Auto-reset 1 - the zone will be automatically bypassed if 1 alarm has been triggered since arming time.

Clearing Autoreset - if this option is on, and the zone has *Auto Reset 1* or *Auto Reset 3* option on, the panel will automatically clear the bypass once every 24h, at midnight), provided that the zone was bypassed as a result of an alarm.

Prealarm - zone with alarm verification.

With verification – an option for zones type 0-2 and 85-86. If enabled, the zone is included in alarm verification.

Bell delay – an option for zones type 5 and 6. It changes the way of reaction to a zone violation when armed. If the option is disabled, the alarm from zone will be delayed by a programmed time period (ALARM DELAY). If the option is enabled, the zone will alarm immediately (event, monitoring and telephone messaging), but the loud signaling will be delayed by a programmed time period (SIGNALING DELAY).

Clear alarm – option available to zones type 81 and 82. Violation of the zone will clear alarm in the partition, if it is currently indicated.

Abort delay – with this option disabled, an "alarm” event will be registered after violation of the zone starting the entry delay time (without alarm signaling, but with monitoring and messaging as for the alarm). If the option is enabled, a "zone violation" event will be logged (without messaging, and with monitoring in 4/2 or 3/2 format only, provided that the code for "zone violation" event has been entered).

Partition temporary blocking – option for the zone type 84. Violation of the zone will block the partition for the time of guard round.

Restore after bell - the zone violation end code will be reported to the monitoring station not immediately but only after alarming is over.

Restore after disarm - the zone violation end code will be reported to the monitoring station not immediately but only after the alarm is cleared and the zone is disarmed.

Alarm on Exit delay end - the zone will trigger alarm if at the moment of ending the exit delay countdown it is in the state of violation (with this option disabled the alarm is triggered only if the zone state changes from normal to violation - when armed).

Write violations to event log - option for the zones type 47: NO ALARM ACTION – each zone violation will be recorded in the event log.

No bypass if armed – option for the type 64-79 zones. Violation of the zone when the partition it belongs to is in armed mode will block no group of zones (provided that the control panel has recorded the partition exit after arming).

Abort voice messaging – option for the zones type 81-83. Violation of the zone will cancel the messaging, if it is currently ongoing.

Alarm on unbypass – the zone will trigger an alarm if it is violated after unbypassing, and the partition is armed.

Always loud tamper alarm – if this option is on, tamper alarm is always loud (if option is off – tamper alarm is loud only when armed).

Reporting delay – an option for the reaction types 4-7 and 64-79. During the entry delay time the information on alarm will not be sent to the monitoring station instantly, but delayed by maximum 30 seconds. The delay also refers to the burglary alarm signaling (during the entry delay time, the alarm is signaled on outputs type 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN). The event will be sent earlier (the burglary alarm signaling output will activate) if the entry delay expires or another instant zone is violated. In case of disarming within 30 seconds, the event will not be sent. This option is required for conformance to the 50131-3 standard.

Blocks verification – an option for delayed zones type 0-2 and 85-86. Violation of the zone will block verification of alarms in the partition (similarly as violation of the zone type 90).

Check arm possibility – an option for the arming zones (type 80 and 82). Violation of the zone will not activate the armed mode, if a zone with enabled PRIORITY option is violated in the partition, or other circumstance have occurred which prevent arming (depending on the selected options, tamper, trouble, etc.).

Restore disarms – an option for the exit time shortening zone (type 89). The end of violation disarms the partition. This option overrides the option RESTORE DISABLES VERIFICATION.

Restore disables verification – an option for the exit time shortening zone (type 89). The end of zone violation will disable verification of alarms in the partition (similarly as violation of the zone type 90).

4.3.4 Zone type

0. ENTRY/EXIT - delayed zone combining two functions:

entry - violation of the zone starts entry delay counting in the partition and turns on delay for the interior delayed zones; the entry time may be signaled on keypads;

exit - during the exit delay the panel keeps watching the zone for violation - in case of no violation (the user has armed the zone but has not left the facility), the zones with the BYPASSED IF NO EXIT option active will be bypassed.

1. ENTRY - see the ENTRY/EXIT zone.

2. DELAYED WITH DELAY SIGNALING – a delayed-action zone with optional signaling of delay countdown in keypads.

3. INTERIOR DELAYED - conditionally delayed zone: delay is only activated when the ENTRY or ENTRY/EXIT zone has been violated first.

4. PERIMETER - instantly armed zone, allowing no exit delay (total or partition).

5. INSTANT - instant zone, without additional functions.

6. EXIT - see the ENTRY/EXIT zone.

7. DAY/NIGHT - if disarmed, the zone will signal violation acoustically in keypads and on the 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN type outputs (signaling for a time period preset for the given output); when armed, the zone acts as the INSTANT zone.

8. EXTERIOR – a zone with alarm verification: violation of the zone will start counting the observation time (programmed as the zone entry delay) - if a second violation takes place during this time, an alarm will be triggered. The first violation may be signaled at the 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN type outputs. If the observation time is not programmed, the alarm will be generated upon the first violation.

9. 24H TAMPER - permanently armed zone, intended for the tamper circuits. Violation of the zone is additionally signaled as a trouble.

10. 24H VIBRATION - 24h zone intended for working with vibration detectors: during arming (from LCD keypad), an automatic test of these detectors is performed - prior to starting the "exit delay" countdown, the VIBRATION DETECTORS TEST type output is activated and countdown begins of testing time, during which all vibration type zones in the given partition should be violated.

11. 24H CASH MACHINE - zone intended for protection of a cash machine (see: Partitions).

12. PANIC-AUDIBLE - permanently armed zone, intended for operating the panic buttons.

13. PANIC-SILENT - permanently armed zone; its violation starts reporting to the monitoring station and activates the SILENT ALARM type outputs without activating the audible alarm signaling (it also refers to audible signaling in the keypad).

14. MEDICAL - BUTTON

15. MEDICAL - REMOTE CONTROL - violation of the medical zones will trigger an alarm signaled in keypads and on the SILENT ALARM type outputs. The zone names and the codes of events from those zones are compatible with the Contact ID monitoring standard.

16÷31 COUNTING L1÷16 – the counting zones will signal an alarm when the number of violations counted during a specified time period exceeds the set value. The control panel offers the possibility to program 16 different counters, which define how the counting zones will operate. Several zones can be assigned to each counter, thus creating a group of counting zones. Violations of the counting zones in armed mode can be signaled at the 9. DAY ALARM, 12. SILENT ALARM and 116. INTERNAL SIREN type outputs.

The following information should be specified for each group of counting zones (counters) (→*Service mode* →*Zones* →*Counters* →*Counter n* [n = counter number]):

- Max. value - number of zone violations which, if exceeded, will trigger the alarm,
- Counting time - the time in which violations are counted
- Counter type
  - *normal* - all violations of counter group zones are counted
  - *omits recurs* - consecutive violations of the same zone are not counted (alarm will be triggered if the number of violations from different zones exceeds the maximum value).

Note: *If the counter skips repeats, the programmed maximum counter value must be lower than the number of zones in counter group.*

32. 24H FIRE

33. 24H FIRE – SMOKE

34. 24H FIRE – COMBUSTION

35. 24H FIRE – WATER FLOW (FIRE)

36. 24H FIRE – HEAT

37. 24H FIRE – BUTTON

38. 24H FIRE – DUCT

39. 24H FIRE – FLAME

All the fire zones (type 32÷39) trigger alarms signaled on the FIRE ALARM type outputs. They differ in the alarm code being sent to the monitoring station in the Contact ID format. The names of these zones are compatible with the names of event codes in the CID format. The fire outputs (except for the 24H FIRE – BUTTON) can work with alarm verification.

40. 24H FIRE SUPERVISORY

41. 24H LOW WATER PRESSURE

42. 24H LOW CO2

43. 24H WATER GATE DETECTOR

44. 24H LOW WATER LEVEL

45. 24H PUMP ACTIVATED

46 24H PUMP FAILURE

47. NO ALARM ACTION - zone intended for activating the outputs (e.g. ZONE VIOLATION, READY STATUS etc.). If the WRITE VIOLATIONS TO EVENT LOG option is activated for this zone, every violation will be recorded in the event log.

48. 24H AUXILIARY – PROTECTION LOOP

49. 24H AUXILIARY - GAS DETECTOR

50. 24H AUXILIARY - REFRIGERATION

51. 24H AUXILIARY - LOSS OF HEAT

52. 24H AUXILIARY - WATER LEAKAGE

53. 24H AUXILIARY - FOIL BREAK

54. 24H AUXILIARY - LOW BOTTLED GAS LEVEL

55. 24H AUXILIARY - HIGH TEMPERATURE

56. 24H AUXILIARY - LOW TEMPERATURE

The zone types from 40 to 56 (auxiliary) signal alarms on the TECHNICAL ALARM type outputs. The names of zones and the codes of events from those zones are compatible with the Contact ID monitoring standard.

57. TECHNICAL - DOOR OPEN - zone intended for supervising the status of the door defined as *Dependent door* in the access control module (which controls the electromagnetic door lock).

58. TECHNICAL - DOOR BUTTON - zone intended for opening the door controlled via a partition keypad, code lock (or another access control module). The value of *entry delay* time entered for such a zone means the address of a door control module (from 0 to 31 – modules of bus 1, from 32 to 63 - modules of bus 2, 32 - address 00, 33 - address 01, etc.). Violation of such a zone will switch over the selected module relay and open the door (e.g. entering a room requires the access code to be entered from the keypad installed outside the door, while for exiting it is enough to press the button situated at the door inside the room).

59. TECHNICAL - AC LOSS - intended for control of devices working together with the alarm control panel e.g. additional power supply units. Violation of this zone will trigger the trouble alarm in the control panel.

60. TECHNICAL - BATTERY LOW - intended for the battery control in additional power supply units working together with the control panel. Violation of this zone will trigger the trouble alarm in the control panel.

61. TECHNICAL - GSM LINK TROUBLE - intended for control of the external GSM communication module. Violation of this zone will trigger the trouble alarm on the control panel.

62. TECHNICAL – OVERLOAD – intended for control of an additional power supply unit used together with the control unit. If the power supply unit is overloaded, violation of this zone will cause the control panel to signal a trouble.

63. RESERVED

64÷79 BYPASSING - GROUP: 1÷16 – violation of this type of zone will bypass a specified group of zones. The control panel enables up to 16 zone groups to be defined. The group is created by selecting the zones and defining how they will be bypassed:

- *Bypass only* - violation of the zone bypassing a particular group will bypass the zones. If the bypassing zone has a fixed BYPASS TIME, the group will be bypassed for such a time. If the BYPASS TIME is equal to zero, unbypassing of the group will follow automatically when the partitions to which the zones belong are disarmed.
- *Bypass on/off* - violation of a bypassing zone will bypass the zones, while end of violation will result in unbypassing the same.

Additionally, the following **options** are available to this type of zone, which are activated when, after arming, the control panel records an exit from the partition to which the bypassing zone is assigned (violated the control panel zone with function 0 or 6 - EXIT):

- **No bypass if armed** – with this option enabled, the zone will not perform the bypassing function, if the partition to which the zone belongs is armed.

- **Alarm in arm state** - with this option enabled, violation of the bypassing zone in the armed mode will **trigger an alarm**.

80. ARMING – violation of the zone will arm the selected group of partitions or the partition to which the zone belongs.

81. **DISARMING** – violation of the zone will disarm the selected group of partitions or the partition to which the zone belongs, and can also clear the alarm and cancel the messaging.

82. **ARM/DISARM** - the zone controls the arming status of the partition it belongs to. Additionally, activating the PRIORITY option enables the user to choose the control mode:
    - option deactivated: violation of the zone will arm, and end of violation will disarm the partition ("switch"),
    - option activated: consecutive violations will arm/disarm the partition ("button").

    Disarming may simultaneously clear the alarm and cancel the messaging.

83. **CLEARING ALARM** - violation of the zone will clear alarm in the selected group of partitions or the partition to which the zone belongs, and can also cancel messaging.

84. **GUARD** - violation of the zone is recognized as recording the guard's round in the partition to which the zone belongs. The partition can be bypassed for the guard round time.

85. **ENTRY/EXIT - CONDITIONAL** - ENTRY/EXIT zone (as type 0) with an extra feature: the zone becomes an instant one upon arming, but without leaving the protected area (i.e. without violating of this zone during exit delay).

86. **ENTRY/EXIT - FINAL** – as type 0, but after arming and detecting the violation end of this zone, the control panel ends the exit delay countdown and enters the armed mode.

87. **EXIT - FINAL** - as type 6, but after arming and detecting the violation end of this zone, the control panel ends the exit delay countdown and enters the armed mode.

88. **24H BURGLARY** - a permanently armed zone, violation of which will trigger the burglary alarm.

89. **FINISHING EXIT DELAY** – violation of the zone will reduce the time for leaving the partition. It is possible to program a shorter exit delay time, which will be counted down from the moment of zone violation. If this value remains not programmed, the exit time will be reduced to 4 seconds from the zone violation. There will be no effect if the zone is violated and the just running exit delay is shorter than that programmed for the zone.

90. **DISABLING VERIFICATION** – violation of the zone will disable verification of alarms in the partition. All alarms will be unverified until next arming.

4.4 Outputs

The control panel outputs are intended for switching on / off external devices (signaling, lighting, air conditioning, etc.) connected to corresponding terminals of the mainboard or expander. Each of the outputs can serve one of a few dozen functions or can be activated through a combination of other outputs functions (the LOGICAL AND and LOGICAL OR type of outputs). Triggering sources for each output are defined separately. All the outputs (in mainboard and/or expanders) are fitted with LEDs to indicate their current status. The numbers of system outputs are determined in much the same way as the zone numbers. The outputs not assigned to expanders can be used to perform logical functions.

4.4.1 Parameters

Output name - up to 16 characters.

Output type (see the list of *output types*)

Cut off time – refers to the outputs responding to events (alarm, video control outputs, etc.), for the status indicating outputs this time is irrelevant.

4.4.2 Options

Polarization – defines the output operating mode; selecting the option means:

- for high-current outputs: active state +12V, inactive state 0V (common ground);

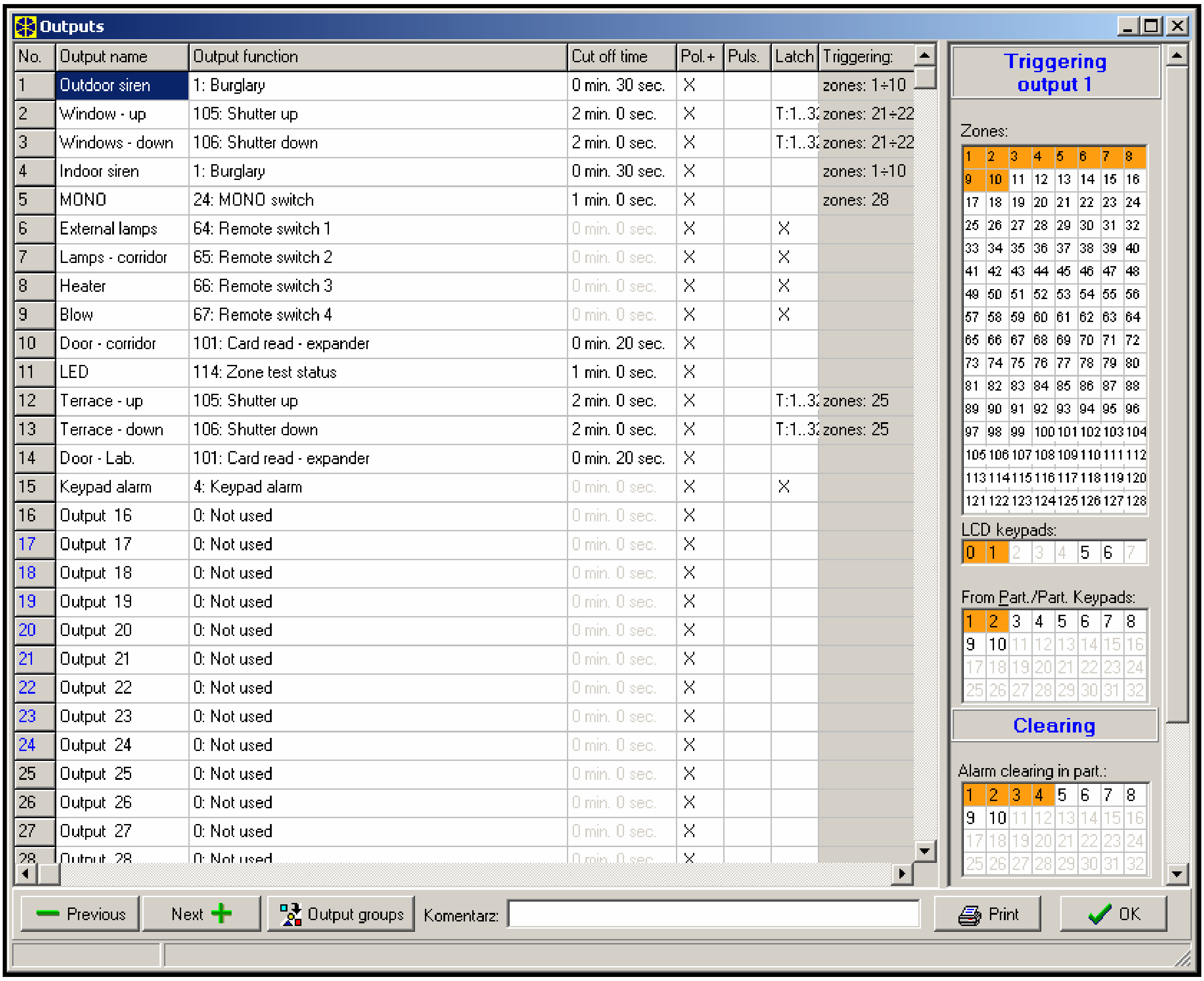
– for OC type outputs: active state - shorted to common ground; inactive state - cut off from common ground.

***Note:** If the option is not set (selected) the output will act in the opposite way.*

Pulsation - sets whether the output signal is to be continuous or pulsating (0.5/0.5 sec.) - the option only applies to the timed outputs;

Latch - (refers to the alarm outputs only) with this option active, the output will be signaling until alarm is cancelled by entering a code.

Comment – this field is intended for entering important information regarding the particular zone. Length of the comment is limited to 256 characters.



Outputs

No.	Output name	Output function	Cut off time	Pol.+	Puls.	Latch	Triggering:
1	Outdoor siren	1: Burglary	0 min. 30 sec.	X			zones: 1÷10
2	Window - up	105: Shutter up	2 min. 0 sec.	X		T:1..3	zones: 21÷22
3	Windows - down	106: Shutter down	2 min. 0 sec.	X		T:1..3	zones: 21÷22
4	Indoor siren	1: Burglary	0 min. 30 sec.	X			zones: 1÷10
5	MONO	24: MONO switch	1 min. 0 sec.	X			zones: 28
6	External lamps	64: Remote switch 1	0 min. 0 sec.	X		X	
7	Lamps - corridor	65: Remote switch 2	0 min. 0 sec.	X		X	
8	Heater	66: Remote switch 3	0 min. 0 sec.	X		X	
9	Blow	67: Remote switch 4	0 min. 0 sec.	X		X	
10	Door - corridor	101: Card read - expander	0 min. 20 sec.	X			
11	LED	114: Zone test status	1 min. 0 sec.	X			
12	Terrace - up	105: Shutter up	2 min. 0 sec.	X		T:1..3	zones: 25
13	Terrace - down	106: Shutter down	2 min. 0 sec.	X		T:1..3	zones: 25
14	Door - Lab.	101: Card read - expander	0 min. 20 sec.	X			
15	Keypad alarm	4: Keypad alarm	0 min. 0 sec.	X		X	
16	Output 16	0: Not used	0 min. 0 sec.	X			
17	Output 17	0: Not used	0 min. 0 sec.	X			
18	Output 18	0: Not used	0 min. 0 sec.	X			
19	Output 19	0: Not used	0 min. 0 sec.	X			
20	Output 20	0: Not used	0 min. 0 sec.	X			
21	Output 21	0: Not used	0 min. 0 sec.	X			
22	Output 22	0: Not used	0 min. 0 sec.	X			
23	Output 23	0: Not used	0 min. 0 sec.	X			
24	Output 24	0: Not used	0 min. 0 sec.	X			
25	Output 25	0: Not used	0 min. 0 sec.	X			
26	Output 26	0: Not used	0 min. 0 sec.	X			
27	Output 27	0: Not used	0 min. 0 sec.	X			
28	Output 28	0: Not used	0 min. 0 sec.	X			

Triggering output 1

Zones:

1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
65 66 67 68 69 70 71 72
73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88
89 90 91 92 93 94 95 96
97 98 99 100 101 102 103 104
105 106 107 108 109 110 111 112
113 114 115 116 117 118 119 120
121 122 123 124 125 126 127 128

LCD keypads:

0 1 2 3 4 5 6 7

From Part./Part. Keypads:

1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32

Clearing

Alarm clearing in part.:

1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32

Fig. 11. Details of output settings.

4.4.3 Source of output triggering

Depending on its type, the output can be triggered in various ways. The control panel makes available lists to select triggering sources suitable for particular types of outputs. For example, you can program zones, keypads, partitions/partition keypads to control zone for the alarm outputs; master users (administrators) and users for the CODE ENTERED SIGNALING / CODE USED SIGNALING outputs; control timers for the TIMER type outputs, etc.

Triggering from zones – selection of the zones, violation of which will activate the output.

Triggering from LCD keypads – selection of the keypads, triggering alarm in which will activate the output.

Triggering from partitions / partition keypads – selection of the partitions and partition keypads, triggering alarm in which will activate the output.

Triggering from control timers – selection of the timers which will activate the output.

Triggering by administrators – indication of the administrators, in case of which entering the password / reading the card or chip will activate the output.

Triggering by users – indication of the users, in case of which entering the password / reading the card or chip will activate the output.

Triggering from control outputs – indication of the outputs, activation of which will activate the output.

Triggering from expansion modules – indication of the expanders which under specified circumstances will activate the output.

Triggering by telephone line trouble – selection of the type of failure to be signaled at the output.

Triggering from reset zones - indication of the zones which will temporary disable the output (verification of fire alarms).

Triggering by synthesizer – selection of the synthesizer messages which will activate the output

Triggering by remote switches – selection of the remote switches the activation of which will trigger the output.

Triggering by wireless zones – selection of the zones (to which wireless devices are assigned), which under specified circumstances will activate the output.

Triggering by wireless outputs – selection of the outputs (to which wireless devices are assigned), which under specified circumstances will activate the output.

Triggering by reporting troubles – selection of reporting troubles, the occurrence of which will activate the output.

Triggering by partitions where burglary zones are tested – selection of partitions in which starting the test of burglary zones will activate the output.

Triggering by partitions where fire / technical zones are tested – selection of partitions in which starting the test of fire or technical zones will activate the output.

Triggering when selected armed mode activated – selection of the armed mode, the activation of which will activate the output.

4.4.4 Clearance availability

Alarm canceling - the list of partitions makes it possible to determine which event will disable the alarm output: the output will only be deactivated if the alarm signaling is cleared in one of selected partitions.

Note: *Clearance of the alarm output should be assigned to the partition by which the output is triggered. If the particular partition is signaling no alarm, clearance of the alarm will be impossible.*

4.4.5 Output disabling

Disabling timers – the output will not be activated within the timer preset time.

Blocked in partitions – the output will not be activated from the installer indicated partitions, if the user will block the signaling of zone violations from those partitions (see USER MANUAL →DESCRIPTION OF USER FUNCTIONS →CHANGE OPTIONS →OUTPUTS CHIME).

4.4.6 Output types

0. NOT USED

1. **BURGLARY ALARM** - signals all burglary and panic alarms (from zones, keypad / expander tamper, keypad Panic, etc.).
2. **FIRE / BURGLARY ALARM** - signals the burglary and panic alarms (continuous sound) and the fire alarms (intermittent sound).
3. **FIRE ALARM** - signals the fire alarms (from fire zones and triggered from keypads).
4. **KEYPAD ALARM** - signals alarms (fire, panic, auxiliary) triggered from keypad.
5. **KEYPAD FIRE ALARM** - signals the fire alarms triggered from keypad.
6. **KEYPAD PANIC ALARM** - signals the panic alarms triggered from keypad.
7. **KEYPAD AUXILIARY ALARM** - signals the medical assistance call alarm triggered from keypad.
8. **TAMPER ALARM** - signals the tamper alarms.
9. **DAY ALARM** – the output signals the following:
   - alarms from zones type 13. PANIC-SILENT,
   - alarms of call for medical help from zones type 14. MEDICAL - BUTTON and 15. MEDICAL - REMOTE CONTROL,
   - alarms from zones type 7. DAY/NIGHT, if the partition to which the zone belongs is disarmed,
   - alarms from zones type 8. EXTERIOR, if the armed mode which assumes that the user will stay inside the protected facility is enabled in the partition (see: USER MANUAL →SYSTEM ARMED MODE),
   - alarms from zones type 4. PERIMETER, if the SIGNALING DELAY has been programmed for them,
   - alarm from zones 5. INSTANT and 6. EXIT, if the SIGNALING DELAY option has been enabled and the ALARM DELAY has been programmed for them,
   - alarms from zones, for which the REPORTING DELAY option has been enabled, provided they were violated during the ENTRY DELAY countdown,
   - unverified alarms (prealarms) from zones with the PREALARM option enabled, provided the AUDIBLE ALARM AFTER VERIFICATION is enabled for the partition,
   - the first violation of the zones type 8. EXTERIOR when they are armed, provided the SURVEILLANCE TIME has been programmed for the zone,
   - violation of the counting zones (type 16 – 31) when armed.
10. **DURESS ALARM** - signals that a DURESS type code (or prefix) has been used in the system.
11. **CHIME** – signals violation of the selected zones when they are disarmed. The installer can indicate partitions, the signaling from which can be blocked by the user by means of the OUTPUTS CHIME function (see USER MANUAL). The function can be automatically blocked for a specified period of time after violation of the selected zone.
12. **SILENT ALARM** – the output becomes activated in the same situations as the output type 9. DAY ALARM. Additionally, it can signal silent panic alarms from keypads, partition keypads and code locks.
13. **TECHNICAL ALARM** - signals violation of the 24H AUXILIARY zones (zone types 40 - 56).
14. **ZONE VIOLATION** - the output activated by violation of selected zones.
15. **VIDEO ON DISARMED** - the output activated by violation of selected zones with the *Video on disarmed* option active (when the zone is disarmed).
16. **VIDEO ON ARMED** - the output activated by violation of selected zones with the *Video on armed* option active (when the zone is armed).
17. **READY STATUS** - signals "readiness" of selected zones for arming (all zones are free from violations).

18. **BYPASS STATUS** - signals that some selected zones have been bypassed.
19. **EXIT DELAY WARNING** - signals that *Exit delay* is running in selected partitions.
20. **ENTRY DELAY WARNING** - signals that *Entry delay* is running for selected zones or in selected partitions.
21. **ARM STATUS** - the output activated when at least one of the selected partitions is armed.
22. **FULL ARM STATUS** - the output activated if all of the selected partitions are armed.
23. **ARM/DISARM ACKNOWLEDGE** - signals arming / disarming of one selected zone (1 signal 0.3 sec. - arming, 2 signals - disarming, 4 signals - alarm canceling /disarming with alarm canceling).
24. **MONO SWITCH** - the output is activated for a specified time with a *MONO output control* type code. The output should be assigned to specific partitions and/or zones. It will be activated by a code entered from keypad / partition keypad serving that partition, or when the selected zone is violated.
25. **BI SWITCH** - the output is activated / deactivated by a *BI output control* type code. The output should be assigned to specific partitions and/or zones. It will be activated by a code entered from keypad / partition keypad serving that partition, or when the selected zone is violated.

Notes:

- *In order to make the MONO SWITCH or BI SWITCH type of output available for control from the LCD keypad, it must be assigned to a selected group of outputs.*
- *The output status can be presented as per the zone state. This is useful, if the control panel output is to only pass a control pulse to switch the device on/off, and the information on the current state of the device is supplied to the control panel zone.*

26. **TIMER** - the output is armed and disarmed by selected timers.
27. **TROUBLE STATUS** - signals detection of a trouble condition (mains power supply failure, low battery, defect of zones, expander buses, etc.).
28. **AC LOSS - CONTROL PANEL MAINBOARD** - signals mains power failure of the control panel mainboard.
29. **AC LOSS (FROM ZONES)** - signals violation of the selected TECHNICAL-AC LOSS type zones.
30. **AC LOSS (FROM EXPANDERS)** - signals mains power failure of the selected expanders with power supply units (expander selection: from 0 to 31 - bus 1 modules, from 32 to 63 - bus 2 modules) and the mimic boards.
31. **BATTERY TROUBLE - CONTROL PANEL MAINBOARD** - signals low voltage condition of the backup battery of the control panel mainboard.
32. **BATTERY TROUBLE (FROM ZONES)** - signals violation of the selected TECHNICAL-BATTERY LOW type zones.
33. **BATTERY TROUBLE (FROM EXPANDERS)** - signals low voltage condition of the backup battery of the selected expanders (as well as the mimic board).
34. **ZONE TROUBLE** - signals exceeding the *Maximum violation time* or the *Maximum no violation time* of the selected zones.
35. **TELEPHONE USAGE STATUS** - signals that the telephone line is captured by the control panel.
36. **GROUND START** - the output generates a control pulse necessary for work with some types of telephone exchange.
37. **MONITORING ACKNOWLEDGE** - the output activated after successful completion of connection with the monitoring station.
38. **SERVICE MODE INDICATOR** - signals activation of the service mode on one of the control panel LCD keypads.

39. VIBRATION DETECTORS TEST - the output intended for testing the vibration detectors in one selected partition (see: Zone types – 24H VIBRATION). The output cut-off time defines the maximum duration of testing the vibration detectors in the selected partition.

40. CASH MACHINE BYPASS INDICATOR - signals bypassing the 24H CASH MACHINE type zones in selected partitions.

41. POWER SUPPLY - the output intended for supplying external devices; it is recommended that the control panel mainboard high-current outputs with electronic protection be used as power supply outputs.

42. POWER SUPPLY IN ARMED STATE - the power supply output is activated on arming some selected partitions (when the exit delay starts). It is intended for supplying e.g. ultrasound or microwave detectors, or infrared barriers, which should not be enabled if not used by the system.

43. RESETABLE POWER SUPPLY - the power supply output resetable from the user menu in LCD keypad. The reset (power cut-off) time for the resetable output is programmed as that output cut-off time.

44. FIRE POWER SUPPLY - the output intended for supplying the fire detectors with automatic alarm verification. The verification takes place in the following way: after detecting violation of one of the fire zones assigned to the given output the power supply is cut off (for a time programmed as the output cut-off time) and, in case next violation occurs after power supply is switched on again, the fire alarm will be triggered. The output can be also reset by the use of a suitable user function (as the RESETABLE POWER SUPPLY type output).

45. PARTITION BLOCKED INDICATOR - signals that the partition armed state is temporarily blocked. If CUT OFF TIME of this output is different from zero, the output will signal the ending of partition blocking: output will be activated for programmed period of time just before partition return to arm state.

46. LOGICAL AND – output is activated when all the outputs selected as the control ones are active.

47. LOGICAL OR - output is activated when at least one of the outputs selected as the control ones is active. An output is considered to be activated when it is energized with +12V voltage - which allows the output *Polarization* option to be used as logical negation.

Each control panel of the INTEGRA series supports all outputs, no matter whether they are physically available (i.e. expansion modules are connected) or not. This makes it possible to use any number of outputs as the control outputs of the LOGICAL AND or LOGICAL OR type.

Example of using outputs type 46, 47

Functions are assigned to outputs, which are not physically available:

- output 63 - BURGLARY ALARM (type 1),
- output 64 - ARM/DISARM ACKNOWLEDGE (type 23).

Output 1, to which the siren is connected, is programmed as LOGICAL OR type of output (type 47), while outputs 63 and 64 are selected to be control outputs.

Output 1 will be triggered if output 63 or 64 is activated.

Then a function should be assigned to the next output which is not physically available:

- output 62 – TIMER (type 26), controlled by a timer set to be daily switched "on" at 16:00 and "off" at 8:00.

Output 2, to which the siren is connected, is programmed as LOGICAL AND type of output, while outputs 1 and 62 are indicated as control outputs.

As a result, output 2 will signal alarms and confirm arming/disarming of the partition, but only between the hours 16:00 and 8:00, outside this time period the output being inactive.

48÷63 VOICE MESSAGE 1÷16 - the outputs activated by the telephone messaging function: it enables any external device to be used for playback of notification messages. When programming telephone notification one should select the message number (synthesizer) which is to be played back after connection is established. The messaging function will activate the corresponding output.

64÷79 REMOTE SWITCH 1÷16 - the output to be controlled via the telephone line by means of a telephone set and DTMF signals. The control is available to users with an assigned telephone code. Additionally, the outputs can be controlled by means of the LCD keypad and the user function OUTPUTS CONTROL (see USER MANUAL).

Notes:

- *To make the output available for control from the LCD keypad, it must be assigned to a selected group of outputs.*
- *If a cut-off time has been programmed for the REMOTE SWITCH type of output, the output will operate in the same way as the MONO SWITCH (i.e. it will be active for a programmed period of time).*
- *The output status can be presented by the zone state. This is useful, if the control panel output is to only pass a control pulse to switch the device on/off, and the information on the current state of the device is supplied to the control panel zone.*

80. NO GUARD ROUND - signals the lack of entering the *guard code* within the specified *round time* in selected partitions.

81. LONG AC LOSS - MAINBOARD - signals the mains power supply failure of the control panel mainboard with delay programmed as *Max. AC loss time* (Options - Global times).

82. LONG AC LOSS - MODULES - signals the mains power supply failure of the selected expansion modules (modules with power supply) with delay programmed as *Max. AC loss time* for each of the modules.

83. OUTPUTS OFF - the output is activated when all the selected outputs have been deactivated (the signaling is completed).

84. CODE ENTERED SIGNALING - the output is activated on entering the code of a selected user (and pressing the [*] or [#] key).

85. CODE USED SIGNALING - the output is activated on arming or disarming the system, using the code of one of selected users.

86. DOOR OPEN INDICATOR - the output is activated on opening the door supervised by the selected modules of access control.

87. DOOR OPEN TOO LONG INDICATOR - the output is activated on exceeding the maximum opening time of the door supervised by the selected modules of access control.

88. BURGLARY ALARM (NO TAMPER OR FIRE ALARMS) – the output only signals the *alarms from armed zones* and *the PANIC alarms from partition keypads and LCD keypads*.

89. EVENTS MEMORY 50% FULL - the output signals that the events memory area has been filled up to 50% (approx. 3000 events) since the last events readout using the DLOADX program. The output remains active until the event memory readout.

90. EVENTS MEMORY 90% FULL - the output signals that the events memory area has been filled up to 90% since the last events readout using the DLOADX program.

91. PARTITION AUTO-ARM DELAY COUNT SIGNALING - the output becomes active (for a specified time) on starting *auto-arming delay* countdown for the selected partitions.

92. PARTITION AUTO-ARM DELAY COUNT INDICATOR - the output indicates the fact of *auto-arming delay* countdown for the selected partitions.

93. UNAUTHORIZED DOOR OPENING – the output becomes active when the doors supervised by selected access control modules (partition keypads, code locks, transponders) are opened without access authorization (i.e. without entering the code or reading in the proximity card).

94. ALARM - UNAUTHORIZED DOOR OPENING – the output works in the same way as the type 93 output but only for the modules with the *Alarm when no authorization* option activated.

95. ETHM/GSM/ISDN REPORTING TROUBLE – the output signals trouble of reporting effected by means of TCP/IP, GSM or ISDN network.

96. TELEPHONE LINE TROUBLE - the output signals the state of:

1 - no voltage on tel. line.
2 - wrong dial tone
3 - no dial tone
4 - Monitoring Station 1 trouble
5 - Monitoring Station 2 trouble

97. VOICE MESSAGE – this output is similar to outputs 48-63. A message number is to be assigned to the output.

98. REMOTE SWITCH – this output is similar to outputs 64-79. A switch number is to be assigned to the output.

99. ACCESS CARD READ – the output signals that the card has been read in by selected users.

100. CARD HOLD - DOWN - the output signals that the card has been held by selected users.

101. CARD READ - EXPANDER – the output signals that the card has been read in indicated modules / keypads. It can be used to perform the function of access control and door control from the keypad. To this effect, indicate the keypad in which reading in the card will activate the output, and the partitions from which the users will be able to open the doors. In the keypad settings, you should indicate the control panel output as the door (see Fig. 15). It is necessary to define the door opening function for presenting / holding the card, and select whether this event is to be logged as an entry or an exit.

102. LINK TROUBLE – WIRELESS ZONE – the output signals lack of communication with wireless devices assigned to the indicated zones.

103. LINK TROUBLE - WIRELESS OUTPUT - the output signals lack of communication with wireless devices assigned to the indicated outputs.

104. WIRELESS DEVICE – LOW BATTERY – the output signals some problems with power supply of wireless devices (low battery, discharged (storage) battery, or lack of external power supply).

105. SHUTTER UP – the dedicated output for raising the roll shutters. It becomes active after violation of selected zones or disarming of selected partitions. It can also be triggered from the keypad, by means of the user menu function (→OUTPUTS CONTROL). Disabling timers can be indicated for the output. If disarming takes place within the time period defined for the timer, the output will not be activated. The cut-off time programmed for the output should be longer than that required for raising the roll shutters.

106. SHUTTER DOWN – the dedicated output for lowering the roll shutters. It becomes active after violation of selected zones or arming of selected partitions (on starting the exit delay countdown). It can also be triggered from the keypad, by means of the user menu function (→OUTPUTS CONTROL). Disabling timers can be indicated for the output. If arming takes place within the time period defined for the timer, the output will not be activated. The cut-off time programmed for the output should be longer than that required for lowering the roll shutters.

Notes:

- *The roll shutter control output, type 105 and 106, must be assigned to the consecutive physical exits.*
- *In order to make the SHUTTER UP and SHUTTER DOWN type of outputs available for control from the LCD keypad, they must be assigned to a selected group of outputs. The two outputs constituting a pair must be assigned to the same group of outputs.*

107. Card on reader A – the output signals that the card / chip has been read into the reader A of selected expanders. It can also signal the card reading into the indicated keypads.

108. Card on reader B - the output signals that the card / chip has been read into the reader B of selected expanders. It can also signal the card reading into the indicated keypads.

109. Zone logical AND - the output is activated when all zones selected as the control ones are violated.

110. Alarm – not verified – the output signals unverified alarms from indicated sources. The unverified alarms are generated by zones with enabled prealarm option and by zones with programmable entry delay (types: 0, 1, 85 and 86). Violation of the zones type 0, 1, 85 or 86 will start the entry delay time countdown. If the armed mode is not deactivated before the delay expires, an unverified alarm will be generated.

111. Alarm – verified – the output becomes active if, after violation of one of the indicated zones with enabled prealarm option, another zone is violated in the partition with enabled prealarm option during verification.

112. Verified – no alarm – the output becomes active if a zone with enabled prealarm option is violated in selected partitions, but no zone with enabled prealarm option is violated during verification.

113. Verification disabled status – the output signals disabling alarm verification in the partition.

114. Zone test status – the output activates after starting the zone test in the selected partitions. It can be used, e.g. to control operation of the LED in the detectors of GRAPHITE and SILVER types.

115. Arming type status – the output becomes active after chosen type of armed mode is activated in the selected partitions. The output can signal the following modes:

1 – fully armed;

2 – armed without interior lines, the Exterior type of outputs trigger a silent alarm, the other ones - audible;

3 – armed without interior, the Exterior type of outputs trigger a silent alarm, the other ones - audible; the delayed outputs, type 0, 1 and 2, act as the instant ones.

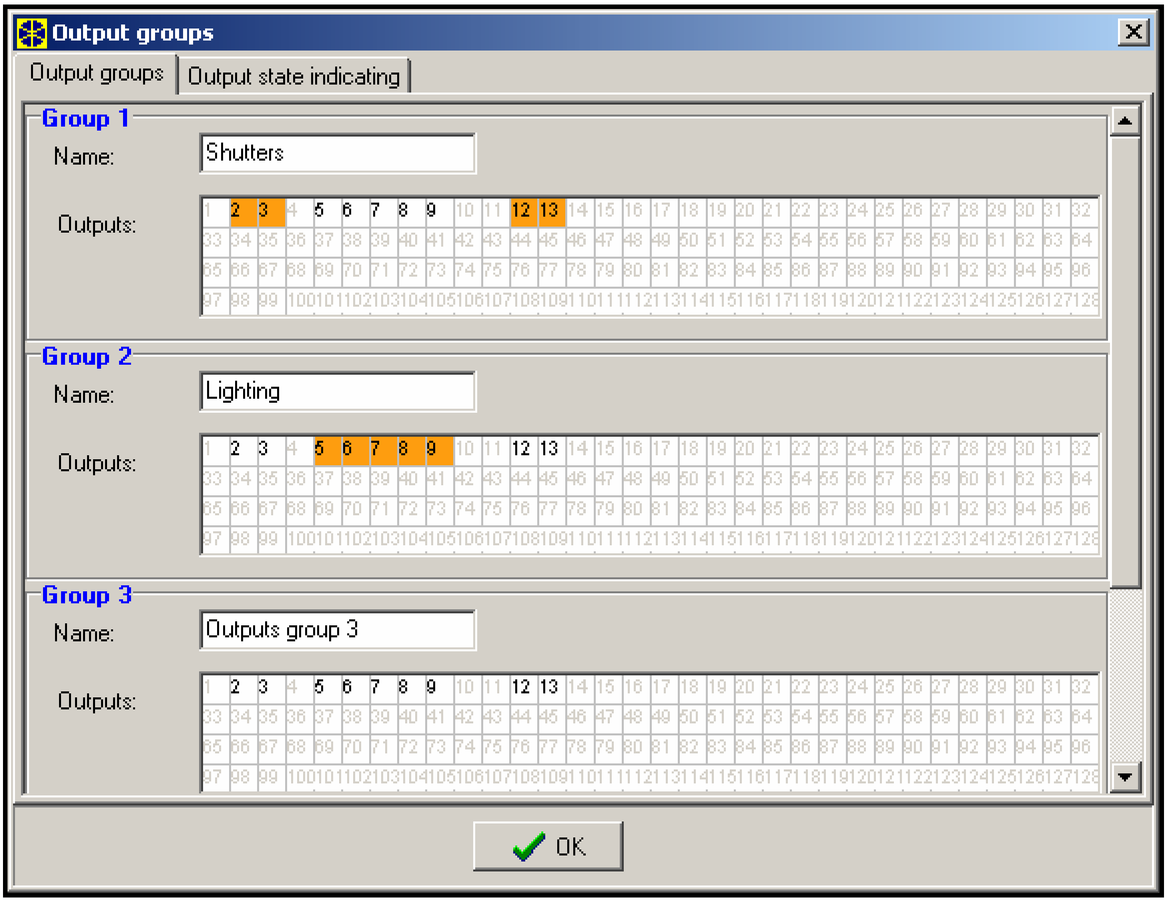
116. Internal siren – the output activates in the same situations as the outputs type 1. Burglary alarm or 9. DAY Alarm (logic product of the outputs type 1. Burglary alarm and 9. Day Alarm).

4.4.7 Output groups

The outputs type MONO switch, BI switch, Remote switch, Shutter up and Shutter down should be assigned to output groups, if they are to be controlled from LCD keypad by means of user functions. Each group may be given a name.

Note: *If the outputs are only assigned to one output group, starting the Outputs control function will not be followed by displaying the list of output groups in the keypad, but immediately by the list of controllable outputs.*

The output status can be presented as per the zone state. This is useful, if the control panel output is to only pass a control pulse to switch the device on/off, and the information on the current state of the device is supplied to the control panel zone.



Group 1

Name: Shutters

Outputs:

Group 2

Name: Lighting

Outputs:

Group 3

Name: Outputs group 3

Outputs:

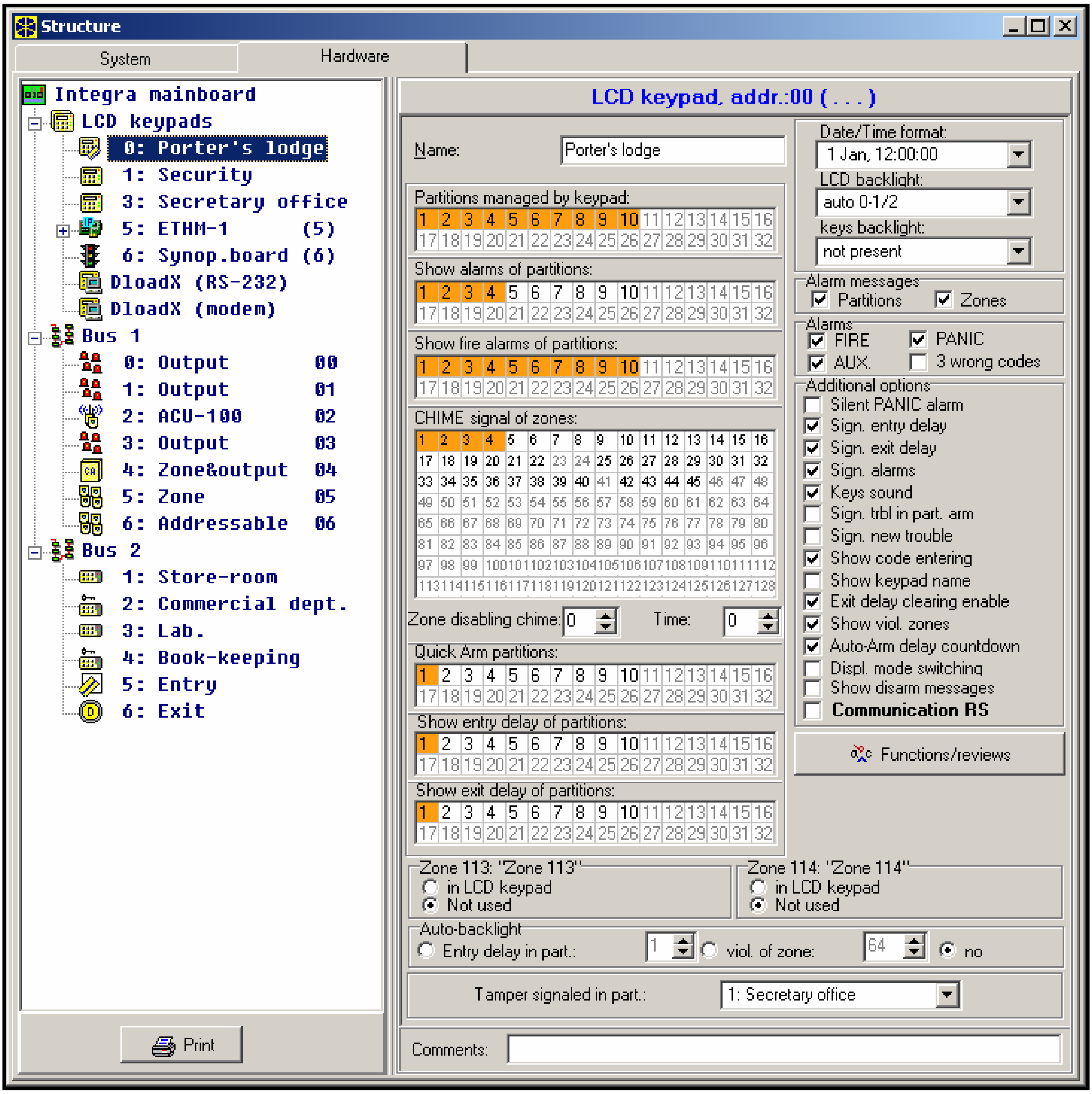
Fig. 12. Window for assignment of outputs to output groups.

5. LCD keypad

Each LCD keypad has an individual name and a set of parameters which determine its way of operation in the system. These are:

- **Partitions managed by keypad** – partitions which can be armed/disarmed or alarm in which may be cancelled from the keypad. Control will be possible for the users who have access to indicated here partitions. When any of the indicated partitions is armed, the keypad LED labeled 👁 [ARMED]. When all partitions specified here are armed, this LED lights steadily.
- **Alarm indication** – list of partitions for which a burglary/fire alarm will be indicated in the keypad by the LED labeled 🔊 [ALARM] and on the display (provided that the PARTITIONS ALARM MESSAGES option is active). An additional option determines whether the alarms are signaled audibly.
- **CHIME signal** – list of zones, violation of which generates audible keypad alarm. This signal can be automatically disabled after violation of selected zone for a time period not exceeding 255s.
- **Quick Arm** – partitions which will be armed after pressing [0][#] on the keypad.
- **Time indication** – the keypad can display the entry/exit delay countdown in the partitions served. Additional options make it possible to define whether the alarm is to be audibly signaled.
- **Keypad zones** - each LCD keypad is provided with two zones which can be used in the security system. These are zones 49 and 50 for the keypad with address 0, and zones 51 and 52 for the keypad with address 1, and so on, up to zones 63 and 64 for the keypad with address 7. These zones can be also accessible in a zone expansion module, if the

maximum number of zone modules are connected. Options make it possible for each of the keypad zones to determine whether or not it will be used in the keypad.



Integra mainboard
- LCD keypads
  - 0: Porter's lodge
  - 1: Security
  - 3: Secretary office
  - 5: ETHM-1 (5)
  - 6: Synop.board (6)
  - DloadX (RS-232)
  - DloadX (modem)
- Bus 1
  - 0: Output 00
  - 1: Output 01
  - 2: ACU-100 02
  - 3: Output 03
  - 4: Zone&output 04
  - 5: Zone 05
  - 6: Addressable 06
- Bus 2
  - 1: Store-room
  - 2: Commercial dept.
  - 3: Lab.
  - 4: Book-keeping
  - 5: Entry
  - 6: Exit

LCD keypad, addr.:00 (. . .)

Name: Porter's lodge

Partitions managed by keypad:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Show alarms of partitions:

1	**2**	**3**	**4**	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Show fire alarms of partitions:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

CHIME signal of zones:

1	**2**	**3**	**4**	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128

Zone disabling chime: 0 Time: 0

Quick Arm partitions:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Show entry delay of partitions:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Show exit delay of partitions:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Date/Time format: 1 Jan, 12:00:00

LCD backlight: auto 0-1/2

keys backlight: not present

Alarm messages: ☑ Partitions ☑ Zones

Alarms: ☑ FIRE ☑ PANIC ☑ AUX. □ 3 wrong codes

Additional options:
- □ Silent PANIC alarm
- ☑ Sign. entry delay
- ☑ Sign. exit delay
- ☑ Sign. alarms
- ☑ Keys sound
- □ Sign. trbl in part. arm
- □ Sign. new trouble
- ☑ Show code entering
- □ Show keypad name
- ☑ Exit delay clearing enable
- ☑ Show viol. zones
- ☑ Auto-Arm delay countdown
- □ Displ. mode switching
- □ Show disarm messages
- □ **Communication RS**

Zone 113: "Zone 113": ○ in LCD keypad ● Not used

Zone 114: "Zone 114": ○ in LCD keypad ● Not used

Auto-backlight: ○ Entry delay in part.: 1 ○ viol. of zone: 64 ● no

Tamper signaled in part.: 1: Secretary office

Comments:

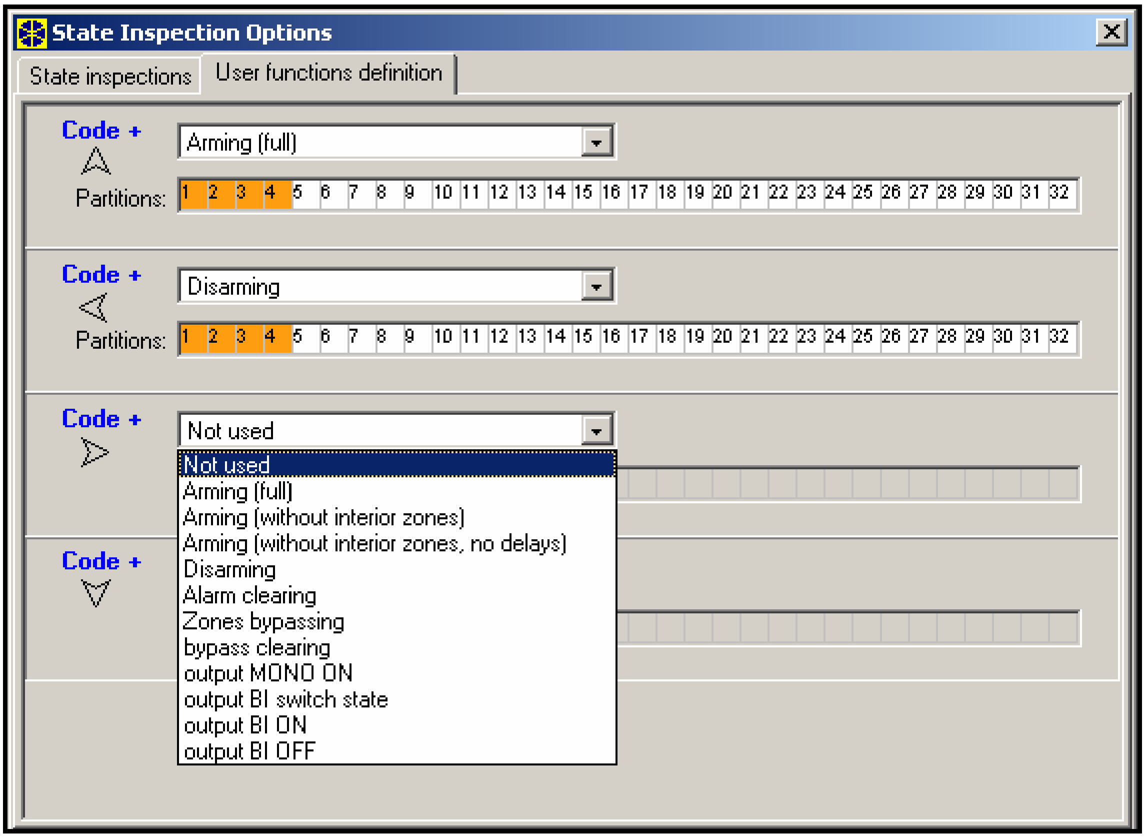
Fig. 13. Parameters defining LCD keypad operation.

- **Auto-backlight** – determines whether the automatic illumination of the keypad is to come on after the particular system event, i.e. start of the entry delay countdown in the selected partition, or violation of the selected zone.
- **Date/Time format** - permits selecting the format of time and date display on the keypad.
- **LCD Backlight** - selection of the display backlighting type.
- **Keys backlight** - selection of the keypad backlighting type.
- **Alarm messages** - the options define whether text messages on alarms in partition and zones are to be shown (the message contains name of partition/zone).
- **Alarms** – the options determine if the following alarms can be called from the given LCD keypad:
  - FIRE - fire alarm triggered by holding down the key with 🔥 symbol,
  - PANIC - panic alarm triggered by holding down the key with 🛡 symbol,

  - AUX. – auxiliary (medical) alarm triggered by holding down the key with (!) symbol.

- - 3 wrong codes - alarm triggered by entering wrong access codes three times.
- **Additional options** – a set of additional options for activating some functions of the keypad (shown in square brackets is the name displayed on keypad):
  - *Silent PANIC alarm [Silent panic]* - determines if the panic alarm called from the LCD keypad will be indicated as a silent alarm (with no signaling on alarm outputs) or as a normal, audible alarm
  - *Signaling entry delay [Entry time s.]* - determines whether the entry delay counting will be signaled by sound on the keypad
  - *Signaling exit delay [Exit time sig.]* - determines whether the exit delay counting will be signaled by sound on the keypad
  - *Signaling alarms [Alarm signal.]* - determines whether the LCD keypad will signal the alarm by sound
  - *Key sounds [Key sounds]* - determines whether pressing the keypad keys will be confirmed by sounds
  - *Signaling troubles in partially arm [Trbl.in p.arm.]* - determines whether the keypad will indicate system troubles (yellow LED) if some of the served partitions are armed (when all partitions are armed, troubles are not indicated)
  - *Signal new trouble [New trbl. sign.]* – with this option enabled, the keypad will audibly signal occurrence of a new trouble. For the option to operate it is necessary to enable the option TROUBLE MEMORY UNTIL REVIEW in the control panel.
  - *Show code entering [Show code ent.]* – determines whether code entry will be shown in the form of asterisks on the keypad display.
  - *Show keypad name [Name (2nd row)]* – determines whether keypad name will be displayed in the second line.
  - *Exit delay clearing enable [Fin. exit time]* – determines whether entering the [9][#] sequence will make it possible to shorten the exit delay time in partitions with the option EXIT DELAY CLEARING.
  - *Show violated zones [Zone violation]* – enabling the option means that the zones signaling CHIME in the keypad will be shown together with their name
  - *Auto-Arm delay countdown signaling [Auto-arm delay]* - activates audible signaling of the countdown to arming the partitions by timer (the signaling continues for the partition auto-arming delay time)
  - *Display mode switching [Dspl.mode chg.]* – enabling the option makes it possible to switch over the display mode from system status to all-partition status by holding down the key "9"
  - *Show disarm messages [Show disarming]* – disarming one of the keypad operated partitions can be signaled by sounds or displayed messages. The option refers to situations when the partition is disarmed by means of another keypad or without the use of a keypad.
  - *Communication RS-232* - determines whether the keypad RS-232 port is enabled to interface with the GUARDX program - with this option enabled, it is possible to program the settings of the computer “virtual" keypad accessible from the GUARDX program
- **Functions/reviews** – options which make it possible to:
  - program the access to key functions ("press and hold down" type) – for scrolling through system memory and status;
  - define the characters to signal the status of zones and partitions in the viewing functions;
  - select partitions the status of which will be permanently shown on the display;

- assign the user functions to arrow keys (to be performed after entering the code and pressing the corresponding arrow).



State Inspection Options

State inspections | User functions definition

Code + △ — Arming (full) — Partitions: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Code + ◁ — Disarming — Partitions: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

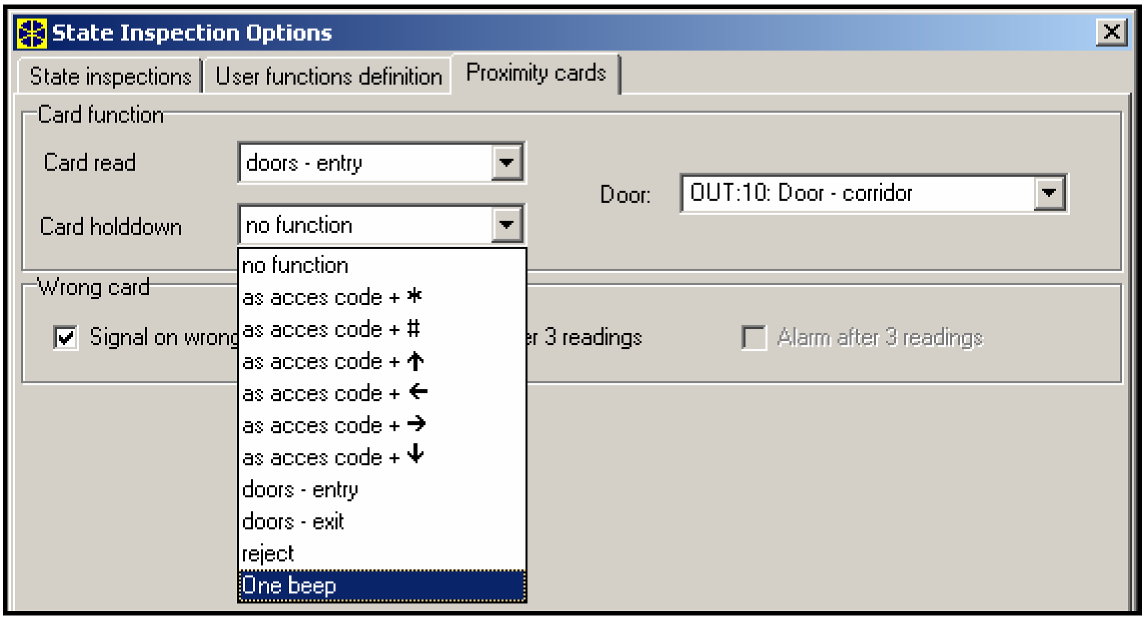
Code + ▷ — Not used

Code + ▽

Not used
Arming (full)
Arming (without interior zones)
Arming (without interior zones, no delays)
Disarming
Alarm clearing
Zones bypassing
bypass clearing
output MONO ON
output BI switch state
output BI ON
output BI OFF

Fig. 14. Programming arrow functions.

- define reaction of a keypad with built-in reader to bringing closer / holding a card, or to an attempt to read in an unregistered card
- select doors to be opened by presenting or holding the card. You can indicate the doors controlled by expander or the control panel output type 101 (see description of the output type 101).



State Inspection Options

State inspections | User functions definition | Proximity cards

Card function

Card read: doors - entry

Card holddown: no function

Door: OUT:10: Door - corridor

Wrong card

☑ Signal on wrong … r 3 readings

□ Alarm after 3 readings

no function
as acces code + *
as acces code + #
as acces code + ↑
as acces code + ←
as acces code + →
as acces code + ↓
doors - entry
doors - exit
reject
One beep

Fig. 15. Handling proximity cards.

- **Tamper signaled in partition** – defines the partition where alarm will be signaled after violation of the keypad tamper circuit and disconnection of the keypad from the system.

- **Sound volume** – the function makes it possible to control loudness level of the keypad sounder. It refers to the keypads type INT-KLCD-GR, INT-KLCD-BL, INT-KLCDR-GR and INT-KLCDR-BL. The function is unavailable in the DLOADX program.

6. Codes and users

The INTEGRA control panel distinguishes three code types, i.e. service, master user (administrator), and user codes. The service and master codes are stored in the EEPROM memory, thus they are not erased after removal of the MEMORY jumper. Jumper removal will disconnect the 3.6V battery used for backup of settings / events memory, as well as the clock if there is a failure of the control panel AC supply. The codes of other users are saved in the RAM memory with a battery backup and will be lost after removal of the MEMORY jumper. Each user of the system has a code to allow him to operate the control panel (including arming/disarming, clearing alarms, controlling outputs, and having access to other functions). The code identifies the user, his authority level in the system and access to partitions and selected parts of the facility (the access is controlled with locks controlled by the INTEGRA control panel). The types of codes, their properties and methods to enter into the system are described in detail in the user manual.

Provision is made for the installer to create in the service mode a "template (mask) of basic authority" to be granted to each new user (or master user). Such a template should be created by means of the function called ACTIVE USER AUTHORITY (→*Service mode* →*Options* →*Active authority*). An extra authority level, not included in the template, may be individually granted to the user (or master user) when they are being entered or edited.

Each user is assigned a consecutive number in the system, which in case of monitoring is sent to the monitoring station in the events which, apart from the event code, also contain the user number (when monitoring in Contact ID format is enabled). After deletion of the user, the control panel may assign the available number to a new user entered into the system.

6.1 Prefixes

Control of the system may require entering additional digits called a **prefix** directly before the access code. The prefix length (1 to 8 digits) is determined by the installer with the service function: →*Options;* →*Prefix length* (only from LCD keypad), while the prefix value (contents) is determined by the administrator with the →*Change prefix* user function. There are two kinds of prefixes:

Normal– the prefix normally entered before each use of the code, by default programmed as 0 or 00, or 000 ... (the number of zeros depends on the length of prefix).

Duress– the prefix normally entered before use of the code in emergency, e.g. when the user is forced by third parties to disarm the system, bypass the zones, etc., by default programmed as 4 or 44, or 444 ... (the number of fours depends on the length of prefix). Using this prefix before the code results in the ***duress*** alarm code being sent to the monitoring station and activation of the DURESS ALARM output.

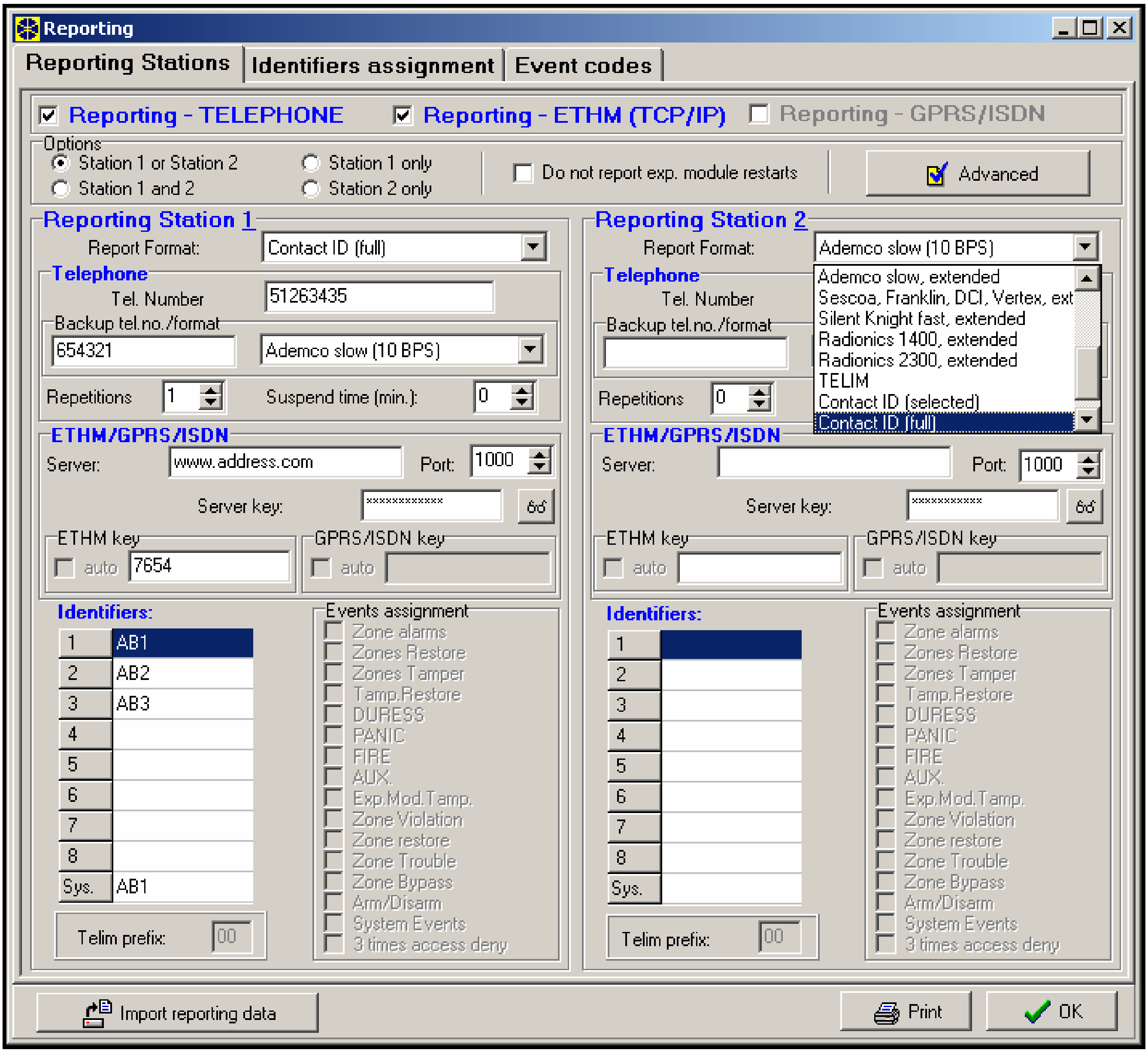
Using the installer code does not require knowledge of the prefix - it is sufficient to enter any digits instead of the prefix. What is important is that the number of entered digits should correspond to the length of prefix.

Notes!

- *Changing the length of prefixes is possible only from real keypads.*
- *Changing the length of prefixes restores their default values.*

7. Monitoring

The communicator of the control panel enables the monitoring function to be performed via the telephone line. By connecting additional modules to the control panel, events can be monitored with the use of Ethernet (TCP/IP), GSM (GPRS technology) or ISDN networks.



☑ Reporting - TELEPHONE ☑ Reporting - ETHM (TCP/IP) □ Reporting - GPRS/ISDN

Options
● Station 1 or Station 2 ○ Station 1 only
○ Station 1 and 2 ○ Station 2 only
□ Do not report exp. module restarts

Reporting Station 1
Report Format: Contact ID (full)
Telephone
Tel. Number: 51263435
Backup tel.no./format: 654321 Ademco slow (10 BPS)
Repetitions: 1 Suspend time (min.): 0
ETHM/GPRS/ISDN
Server: www.address.com Port: 1000
Server key: ***********
ETHM key: □ auto 7654
GPRS/ISDN key: □ auto
Identifiers:

1	AB1
2	AB2
3	AB3
4	
5	
6	
7	
8	
Sys.	AB1

Telim prefix: 00

Events assignment
□ Zone alarms
□ Zones Restore
□ Zones Tamper
□ Tamp.Restore
□ DURESS
□ PANIC
□ FIRE
□ AUX.
□ Exp.Mod.Tamp.
□ Zone Violation
□ Zone restore
□ Zone Trouble
□ Zone Bypass
□ Arm/Disarm
□ System Events
□ 3 times access deny

Reporting Station 2
Report Format: Ademco slow (10 BPS)
Ademco slow, extended
Sescoa, Franklin, DCI, Vertex, ext
Silent Knight fast, extended
Radionics 1400, extended
Radionics 2300, extended
TELIM
Contact ID (selected)
Contact ID (full)
Telephone
Tel. Number
Backup tel.no./format
Repetitions: 0
ETHM/GPRS/ISDN
Server: Port: 1000
Server key: ***********
ETHM key: □ auto
GPRS/ISDN key: □ auto
Identifiers:

1	
2	
3	
4	
5	
6	
7	
8	
Sys.	

Telim prefix: 00

Events assignment
□ Zone alarms
□ Zones Restore
□ Zones Tamper
□ Tamp.Restore
□ DURESS
□ PANIC
□ FIRE
□ AUX.
□ Exp.Mod.Tamp.
□ Zone Violation
□ Zone restore
□ Zone Trouble
□ Zone Bypass
□ Arm/Disarm
□ System Events
□ 3 times access deny

Fig. 16. Window for format selection and definition of identifiers.

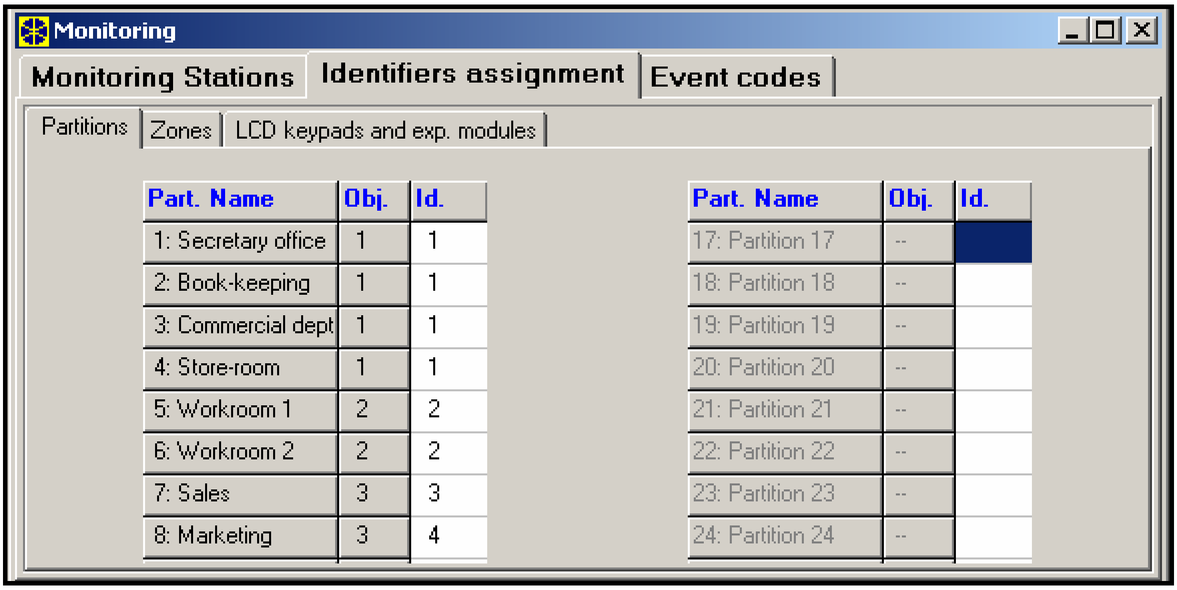
Events can be transmitted to two monitoring stations. For each station, it is possible to program two telephone numbers (main and reserve), and if other forms of monitoring are used apart from the telephone, also the address of monitoring station server. If all forms of monitoring are programmed, the control panel will first make an attempt of monitoring through the Ethernet (TCP/IP), then the GSM (GPRS) or ISDN network, and only finally by means of the telephone (using the main and reserve telephone numbers). The procedure will be terminated when the event is successfully sent to the monitoring station by means of one of above mentioned transmission methods. Otherwise, the control panel will make repeated monitoring attempts as many times, as programmed by the installer. If the event cannot be sent despite completion of the preprogrammed number of retries, the control panel will hang up until a next event occurs, or for a specified period of time. After the time expires, the control panel will make further attempts to send the event.

Note: *8 is the typical value for the* REPETITIONS *parameter, and 30- for the* SUSPEND TIME *parameter (occurrence of a new event resumes sending all the events not yet transmitted).*

Events in the system are divided into eight classes:

1. alarms from zones and tampers,
2. alarms occurring in partitions (e.g. PANIC, fire alarm from the LCD keypad),
3. arming and disarming,
4. zone bypass,
5. access control,
6. system troubles,
7. functions used,
8. other events in the system (e.g. start of the service mode).

Events of class 5 and 7 are not monitored. Other events are transmitted depending on the selected transmission format.



Part. Name	Obj.	Id.	Part. Name	Obj.	Id.
1: Secretary office	1	1	17: Partition 17	--	
2: Book-keeping	1	1	18: Partition 18	--	
3: Commercial dept	1	1	19: Partition 19	--	
4: Store-room	1	1	20: Partition 20	--	
5: Workroom 1	2	2	21: Partition 21	--	
6: Workroom 2	2	2	22: Partition 22	--	
7: Sales	3	3	23: Partition 23	--	
8: Marketing	3	4	24: Partition 24	--	

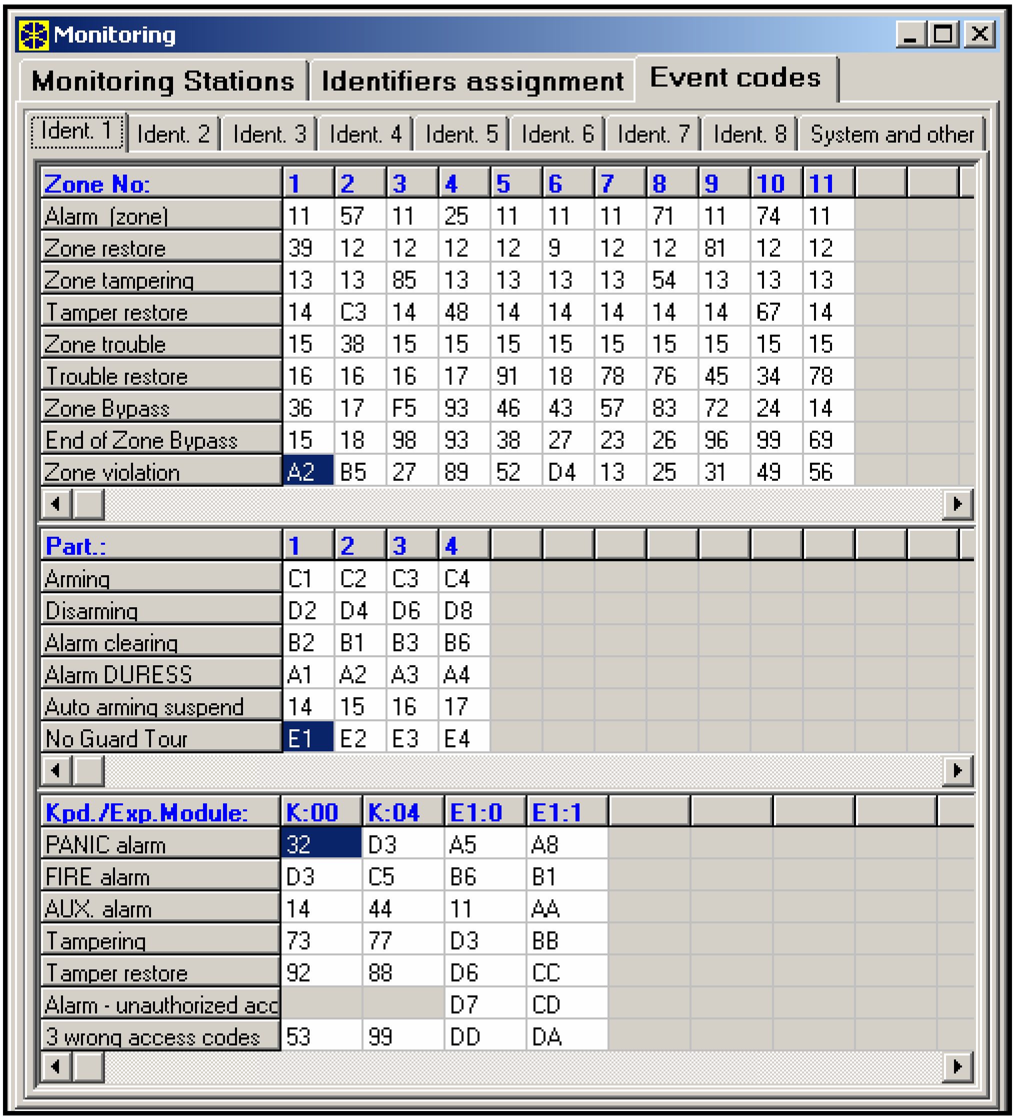
Fig. 17. Window for assigning partition events to identifiers.

- For pulse formats and Ademco Express it is necessary to program event codes. Only those events are transmitted which are assigned to a valid identifier (i.e. those which have at least three characters different from “0") and whose code is different from “00".
- When the “Contact ID (selected)" format is selected, the events are sent which would have been transmitted in pulse formats, the programmed code being of no relevance, since the control panel transmits codes according to the format specification.
- When the “Contact ID (full)" format is selected, there is no need for the installer to program any event codes and/or assign events to identifiers. The control panel transmits codes according to the format specification and the defined division into objects.

Notes:

- *When the “Contact ID (selected)" format is selected, the control panel will only transmit the events which can be transmitted in pulse formats. Not all possible events have their equivalents in pulse formats. Programming of codes for all possible events in the system would require dozens of identifiers to be reserved for the control panel.*
- *For the Contact ID formats, each object has its own identifier. Therefore, the identifiers of non-existing objects need not to be programmed. In the system event identifier field (events of class 6 and 8), you should re-enter the identifier of the object which “is responsible" for the system (for example, the object, where the control panel is installed).*

- *For the “Contact ID (selected)" format, the assignment of partitions, zones, keypads and expanders to identifiers does not need to reflect the division of the system into objects. But it is essential that a value different from “0" be programmed. The control panel transmits all events in the object with a single identifier according to division of system components among the objects.*
- *For the STATION 1 OR STATION 2 operating mode (and STATION N ONLY, with dialing both numbers), it is not possible to select the “Contact ID (full)" format for just one number and another format for the remaining numbers, because it may occur that the event transmitted in format “Contact ID (full)" cannot be converted into the type 4/2 code.*



Zone No:	1	2	3	4	5	6	7	8	9	10	11
Alarm (zone)	11	57	11	25	11	11	11	71	11	74	11
Zone restore	39	12	12	12	12	9	12	12	81	12	12
Zone tampering	13	13	85	13	13	13	13	54	13	13	13
Tamper restore	14	C3	14	48	14	14	14	14	14	67	14
Zone trouble	15	38	15	15	15	15	15	15	15	15	15
Trouble restore	16	16	16	17	91	18	78	76	45	34	78
Zone Bypass	36	17	F5	93	46	43	57	83	72	24	14
End of Zone Bypass	15	18	98	93	38	27	23	26	96	99	69
Zone violation	A2	B5	27	89	52	D4	13	25	31	49	56

Part.:	1	2	3	4
Arming	C1	C2	C3	C4
Disarming	D2	D4	D6	D8
Alarm clearing	B2	B1	B3	B6
Alarm DURESS	A1	A2	A3	A4
Auto arming suspend	14	15	16	17
No Guard Tour	E1	E2	E3	E4

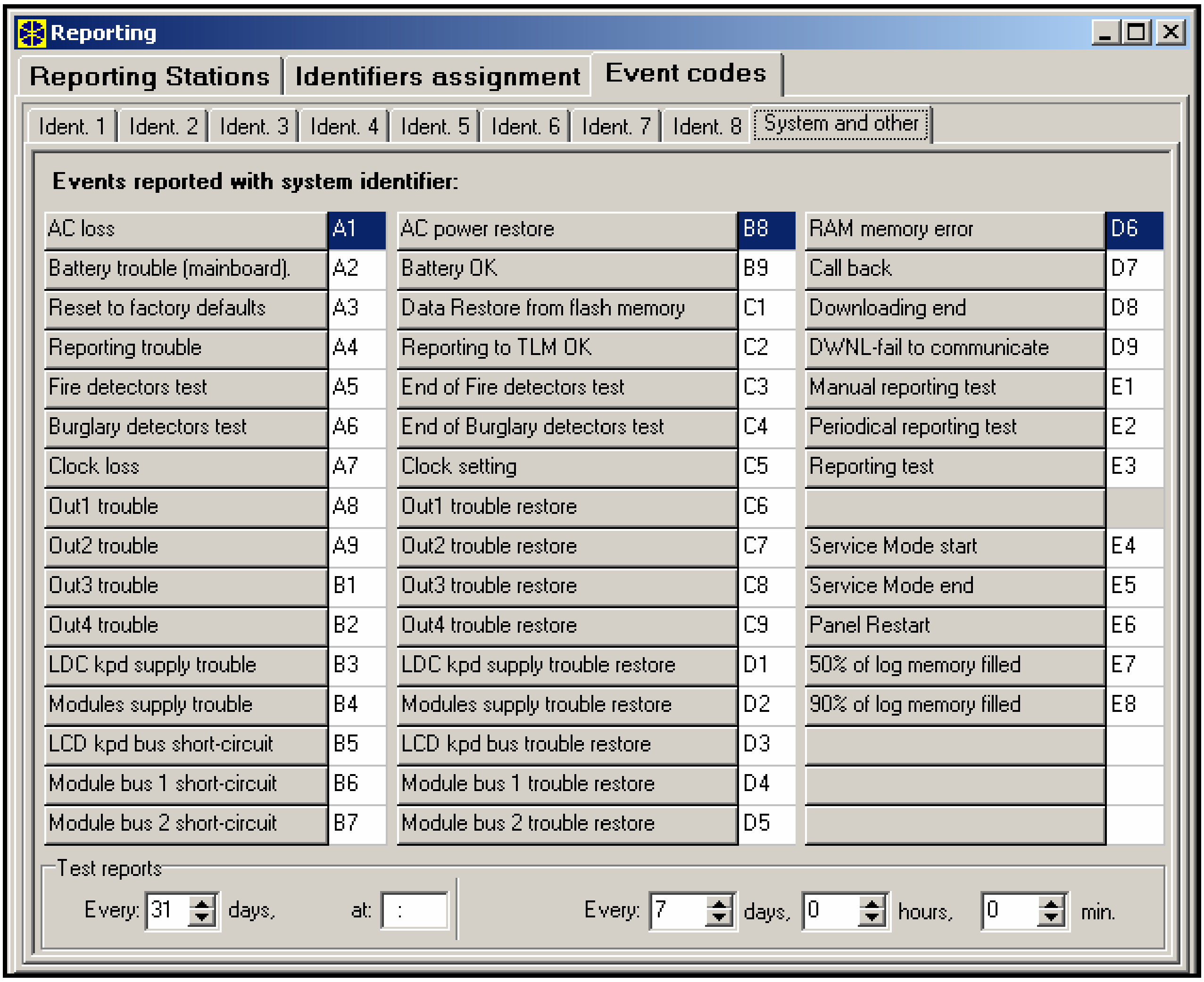
Kpd./Exp.Module:	K:00	K:04	E1:0	E1:1
PANIC alarm	32	D3	A5	A8
FIRE alarm	D3	C5	B6	B1
AUX. alarm	14	44	11	AA
Tampering	73	77	D3	BB
Tamper restore	92	88	D6	CC
Alarm - unauthorized acc			D7	CD
3 wrong access codes	53	99	DD	DA

Fig. 18. Programming of monitoring codes for pulse formats.

For the pulse formats, individual events are assigned to identifiers. This enables the available space to be optimally used for codes (8 x 225 codes = 1800 codes) – events from smaller objects may be grouped with a single identifier, and several identifiers may be assigned for larger objects.

Event codes are programmed after the division is made. The DLOADX program (and corresponding service functions) shows all events assigned to the identifier, which facilitates correct programming of codes (the event code window shows only the fields for those codes which will be transmitted with the given identifier – see Figure 18).

System events and troubles are transmitted with their own identifier. Figure 19 shows the events assigned to this identifier.



Events reported with system identifier:

AC loss	A1	AC power restore	B8	RAM memory error	D6
Battery trouble (mainboard).	A2	Battery OK	B9	Call back	D7
Reset to factory defaults	A3	Data Restore from flash memory	C1	Downloading end	D8
Reporting trouble	A4	Reporting to TLM OK	C2	DWNL-fail to communicate	D9
Fire detectors test	A5	End of Fire detectors test	C3	Manual reporting test	E1
Burglary detectors test	A6	End of Burglary detectors test	C4	Periodical reporting test	E2
Clock loss	A7	Clock setting	C5	Reporting test	E3
Out1 trouble	A8	Out1 trouble restore	C6		
Out2 trouble	A9	Out2 trouble restore	C7	Service Mode start	E4
Out3 trouble	B1	Out3 trouble restore	C8	Service Mode end	E5
Out4 trouble	B2	Out4 trouble restore	C9	Panel Restart	E6
LDC kpd supply trouble	B3	LDC kpd supply trouble restore	D1	50% of log memory filled	E7
Modules supply trouble	B4	Modules supply trouble restore	D2	90% of log memory filled	E8
LCD kpd bus short-circuit	B5	LCD kpd bus trouble restore	D3		
Module bus 1 short-circuit	B6	Module bus 1 trouble restore	D4		
Module bus 2 short-circuit	B7	Module bus 2 trouble restore	D5		

Test reports

Every: 31 days, at: :

Every: 7 days, 0 hours, 0 min.

Fig. 19. System event codes.

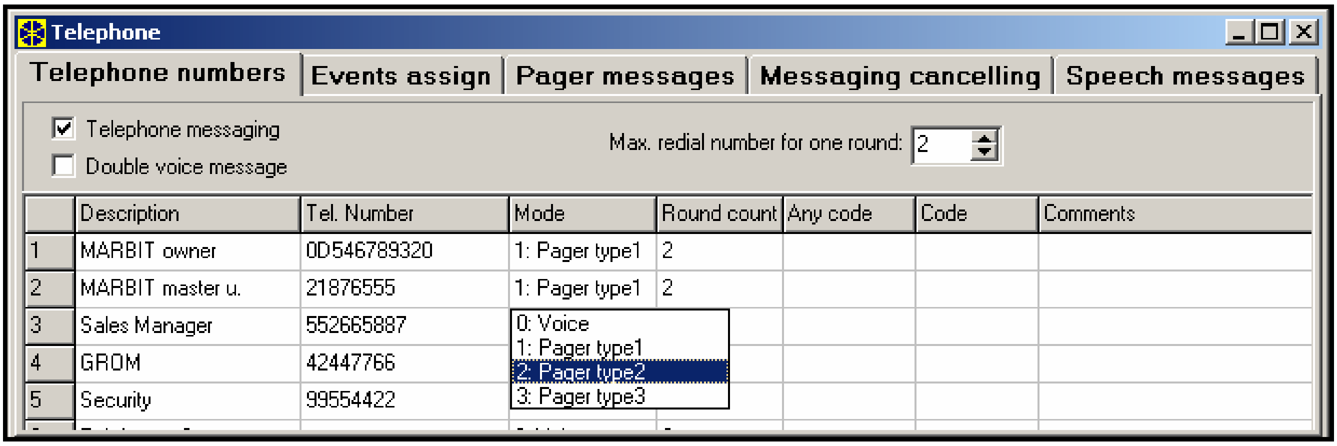
Notes:

- *The "Settings reset" event is caused by the service functions, which restore the factory settings of the system. A number transmitted in the Contact ID format informs which settings are reset (0 – control panel settings reset, 1 – reset of codes).*
- *The "RAM memory error" event informs of error(s) in the settings memory that is backed-up with a 3.6V battery. If the settings are stored in the FLASH memory, detection of this error forces "Module restart" that will be followed by "Settings restore".*
- *"Module Restart" appears at each power supply connection.*
- *The INTEGRA control panel offers two types of a monitoring test: transmitting the "Periodical test of monitoring" event at a specified time and/or at preprogrammed time intervals. An additional transmission may be initiated with the user function, provided the "Manual transmission test" code is programmed.*
- *Checking communication with the station is facilitated by the "Station XX test" function (in the TESTS menu of the user functions), accessible after programming the station phone numbers, system event identifier and "Monitoring test" code. Calling of this function initiates monitoring, when the control panel displays on the keypad information on the current transmission phase and the test result.*
- *The event codes shown in Figures 18 and 19 are taken at random to illustrate an example of programming. They should be programmed as recommended by the monitoring station operating personnel.*

8. Messaging

The messaging function built in the INTEGRA control panel makes it possible to notify of alarms with messages reproduced from voice synthesizers or transmitted to pagers. Messaging is performed independently from monitoring but monitoring has the priority. If in the course of messaging some events occur which must be reported to the monitoring station by the control panel, monitoring will be included in between the messages sent.

Messages may be transmitted to 4, 8 or 16 phone numbers (depending on the control panel type). It is possible to send up to 32 various voice messages and up to 64 different "pager" messages.



☑ Telephone messaging

□ Double voice message

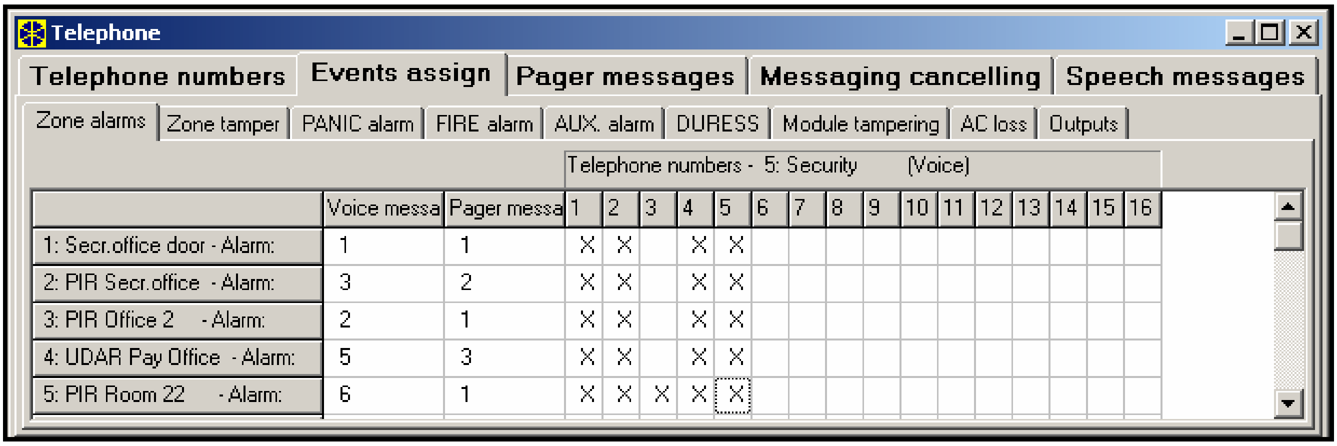
Max. redial number for one round: 2

	Description	Tel. Number	Mode	Round count	Any code	Code	Comments
1	MARBIT owner	0D546789320	1: Pager type1	2			
2	MARBIT master u.	21876555	1: Pager type1	2			
3	Sales Manager	552665887					
4	GROM	42447766					
5	Security	99554422					

0: Voice
1: Pager type1
2: Pager type2
3: Pager type3

Fig. 20. Programming phone numbers for messaging.

During voice messaging, it is possible to acknowledge the message receipt. A special code connected with a telephone number is used for this purpose (it is possible to set any code – four digits transmitted with DTMF denote receipt of a message). The control panel acknowledges the code receipt with a special signal. If there is a number of messages to transmit to a single phone number, all these messages are transmitted during a single connection. In this case, the signal confirming that the message is received is different (handshaking that informs that further messages are awaited).



Telephone numbers - 5: Security (Voice)

	Voice messa	Pager messa	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1: Secr.office door - Alarm:	1	1	X	X		X	X											
2: PIR Secr.office - Alarm:	3	2	X	X		X	X											
3: PIR Office 2 - Alarm:	2	1	X	X		X	X											
4: UDAR Pay Office - Alarm:	5	3	X	X		X	X											
5: PIR Room 22 - Alarm:	6	1	X	X	X	X	X											

Fig. 21. Defining the way of communicating alarms from zones.

Since it is possible to define in detail how each alarm is to be communicated, the INTEGRA control panel allows to organize an additional monitoring, based on the messaging function, that operates simultaneously with the basic monitoring. The way of defining the rules of reporting the alarms from zones is shown in Figure 21. The rules of communicating the other alarms are programmed in much the same way. The messaging may also include information on AC supply loss.

Note: *When reporting an alarm, the control panel performs a cycle of phone calls dialing all specific phone numbers in sequence. The numbers which confirmed alarm message* *receipt with a code are not dialed any more. The other phone numbers are continued to be notified according to the preset number of repeats.*

In order to activate the messaging function you should:

1. Select the TELEPHONE MESSAGING option and set the maximum number of redials in one queue (from 1 to 7) if the number is busy.
2. If, after voice connection is established, the message is to be repeated twice, select the DOUBLE VOICE MESSAGE option.
3. Program the telephone numbers to be notified, and set the following for each number:
   - description (up to 16 characters)
   - messaging mode (voice, pager)
   - number of queues (how many times the control panel will dial the given number - from **1** to **15**) – by default, zero is set, which means no telephone messaging
   - how the notification receipt is confirmed – select the ANY CODE option or enter the confirmation code (to cancel subsequent dialing of the given number)
4. Set the following parameters for corresponding events which will initiate messaging:
   - number of voice message synthesizer (from 0 to 16 or 31)
   - number of pager message for test messaging (from 0 to 32 or 64)
   - numbers of telephones to which the messages will be sent.
5. Select partitions for each telephone number, from which the user will be able to cancel messaging. You can also select telephone numbers, the acknowledgement of a message reception from which will cancel messaging to other indicated telephone numbers.
6. According to the circumstances, set the MESSAGING CANCELING option to enable the telephone messaging to be canceled together with alarm canceling.

9. Answering phone calls

The INTEGRA control panel is provided with the function of answering external phone calls. Only the users, who are assigned a special “**telephone code**" (see: *Codes and users*) have access to this function. The panel can answer calls in one of two modes:

- **single calling mode** - the panel answers the call after a specified number of rings (if the code is incorrect, the control panel will not answer any incoming calls for 4 minutes);
- **double calling mode** – having dialed the control panel number, wait for the specified number of rings, then hang up and (within 3 minutes) redial the control panel number. After the redialing, the control panel should immediately answer the call.

For detailed information on answering the phone calls see the USER MANUAL.

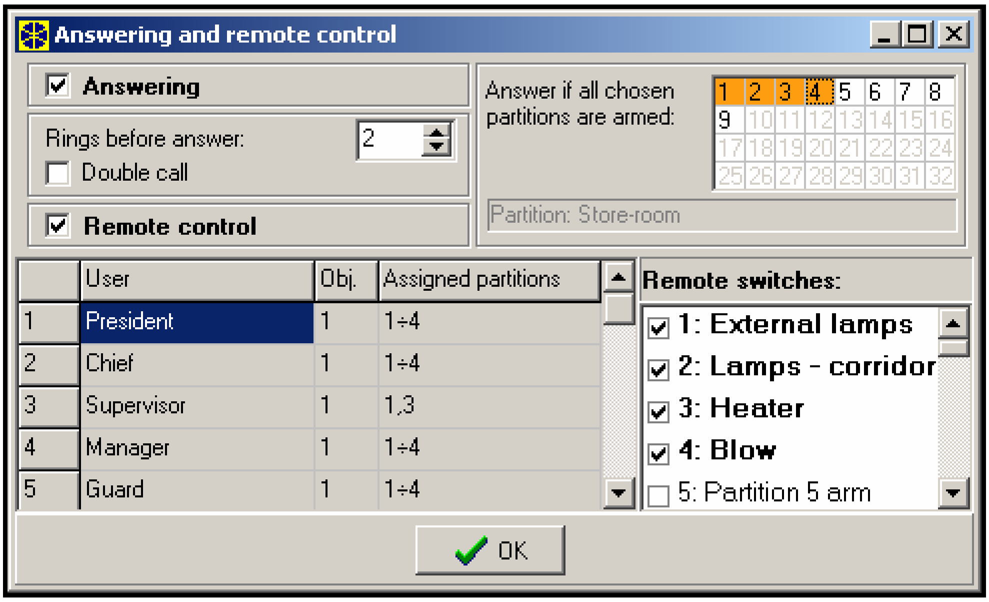
9.1 Control via telephone

The function of answering phone calls enables also the REMOTE SWITCH type outputs to be controlled (see: USER MANUAL). In order to start the CONTROL VIA TELEPHONE function do the following:

1. Select the ANSWERING and REMOTE CONTROL options.
2. Define how the connection to the control panel should be established:
   - double call (if this option is not selected, the control panel will answer the call after the telephone number is first dialed),
   - rings before answer.
3. Where appropriate, select the partitions which must be armed so that the control is available (with a possibility to restrict access to the control). You may also skip this selection.

4. Program telephone access codes for the users who are to perform the control function (USER EDITING).
5. Program suitable outputs as remote switches.
6. Assign the REMOTE SWITCH outputs to the users so that they can effect the control.

Note: *Not all cellular telephones allow DTMF control.*



Answering and remote control

☑ Answering

Rings before answer: 2

□ Double call

☑ Remote control

Answer if all chosen partitions are armed:

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Partition: Store-room

	User	Obj.	Assigned partitions
1	President	1	1÷4
2	Chief	1	1÷4
3	Supervisor	1	1,3
4	Manager	1	1÷4
5	Guard	1	1÷4

Remote switches:

☑ 1: External lamps
☑ 2: Lamps - corridor
☑ 3: Heater
☑ 4: Blow
□ 5: Partition 5 arm

Fig. 22. Defining which remote switches may be controlled by users.

10. Control of outputs from LCD keypad

The control panel makes it possible to control from the LCD keypad the following types of outputs: MONO SWITCH, BI SWITCH and REMOTE SWITCH (see: USER MANUAL). To start the control function you should:

1. Program the parameters of control outputs (type, cut-off time, polarization).
2. Select how the output status will be indicated (standard or selected zone status).
3. Connect suitable devices to the outputs, and supply suitable signals to the zones indicating the equipment status.
4. Assign control outputs to the groups (4 groups can be created) and to the partitions from which triggering will be possible (telephone relays are not assigned to partitions).
5. Grant the CONTROL authority to the users who are to hale access to this function, and assign partitions to trigger the controlling outputs.

11. Conformance to CLC/TS 50131-3 requirements

In order to meet the CLC/TS 50131-3 requirements, follow the instructions below:

- use at least 6-digit codes, which will ensure minimum 100 000 possible passwords for each system user. When using the 6-digit codes, the total number of combinations amounts to 1 000 000, however it is usually lower due to combinations chosen by other users, as well as because simple codes (like 123456, 111111 or 111222) are not permitted. The total number of available codes is determined in the following way: $t=10^n$, where n=number of digits in a code.
- enable the option BLOCK KEYPAD AFTER 3 WRONG CODES
- enable the option ALARM AFTER 3 WRONG CODES for each keypad /partition keypad

- program all the burglary zones not belonging to the entry/exit path as type 4 PERIMETER
- for detectors provided with antimasking function, connect the detector alarm output in parallel with the signaling output of masking attempt and program the MAXIMUM VIOLATION TIME of the zone to be slightly longer than the signaling of violation on the detector alarm output
- enable the PRIORITY option for all zones, excluding the entry/exit path
- enable the options WARN WHILE ARMING IF TROUBLE, VIOLATED / BYPASSED ZONES PREVIEW WHEN ARMING, DO NOT ARM IF TAMPER, DO NOT ARM IF BATTERY TROUBLE, DO NOT ARM IF TROUBLE, DO NOT ARM IF OUTPUTS TROUBLE and DO NOT ARM IF REPORTING TROUBLE
- enable the options TROUBLE MEMORY UNTIL REVIEW, DO NOT SHOW ALARM IF ARMED and LIMIT EVENTS
- the entry delay time should not exceed 45 seconds
- enable the options AUTO-RESET 3 and REPORTING DELAY for all burglary zones
- enable the BYPASS DISABLED option for the tamper, panic and trouble alarm zones
- disable the ALWAYS LOUD TAMPER ALARM option for all zones, keypad / expander buses
- armed mode information blanking should take place not later than after 180 seconds
- enter a suitable value of clock correction
- make quick arming of the system partitions impossible
- program the signaling time within the limits of 90 seconds to 15 minutes
- program the delay of AC power trouble reporting so as not to exceed 60 minutes

SATEL sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
POLAND
tel. + 48 58 320 94 00
info@satel.pl
www.satel.pl