Alarm Control Panels

INTEGRA

Firmware Version 1.08

PROGRAMMING

Satel
GDAŃSK

integra_p_en 08/10

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 at:
http://www.satel.eu

<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>RTTE</b> 1999/5/EC
<b>EMC</b> 2004/108/EC
<b>LVD</b> 2006/95/EC</td></tr>
<tr><td colspan="3"><b><i>The product meets the requirements of harmonized standards:</i></b>
EMC/Immunity EN 50130-4:1995+A1:1998+A2:2003, EN 61000-6-1:2007
EMC/Emissions EN55022:2006+A1:2007, EN 61000-6-3:2007, EN 61000-3-2:2006
Electrical safety EN 60950-1:2006
Telephone TBR 21</td></tr>
<tr><td>Gdańsk, Poland 2009-11-05</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.eu</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 INTEGRA control panels in version 1.07 and 1.08

Partitions	Option VALID WITHIN 60 SEC.
Zones	Option to use resistors of different values in 2EOL loops. Wiring types ROLLER 2EOL and VIBRATION 2EOL for mainboard zones of INTEGRA 128-WRL control panels with electronics version 2.01. Zone types: – 63. TROUBLE – 91. DETECTOR MASK Option NO RESTORE EVENT for zone type 47: NO ALARM ACTION. Option DISABLED IN ARM STATE for zone type 91: DETECTOR MASK. Option ALARMING for zone type 91. DETECTOR MASK.
Outputs	Output type 118. KEYFOB BATTERY LOW. Output type 119. WIRELESS SYSTEM JAMMING. Option ACTIVE DURING VIOLATION for output type 24. MONO SWITCH.
GSM telephone	Selection of GSM band to be used by the GSM phone, for INTEGRA 128-WRL control panels with electronics version 2.01.
LCD keypads	New, more intuitive way to enter data (hexadecimal values, telephone numbers and names). Keypad restart does not result in exiting the service mode. Sensitivity control for the built-in proximity card reader in INT-KLCDR-GR and INT-KLCDR-BL keypads with firmware version 1.06 or later. Support for a new keypad: INT-KSG (touch sensor keypad).
Expansion modules	Communications testing by ETHM-1 modules with firmware version 1.05 by means of PING commands. Support for new modules: – INT-CR – proximity card arm/disarm device, for arming / disarming and alarm clearing in many partitions by means of proximity cards, key fobs and other passive transponders; – INT-TXM – reporting interface for connecting a radio monitoring transmitter to the control panel.
Wireless devices	Support for new wireless devices: – AMD-102 – wireless magnetic contact with input for roller shutter detector, – ARD-100 – wireless reorientation detector.
Users	Defining a minimum length of user codes.

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.

This manual covers information on programming all the INTEGRA series control panels. When reading the manual please bear in mind that there are some differences between these panels. Information relating to the INTEGRA 128-WRL only is additionally highlighted.

2. Control Panel Firmware Replacement

Available on the **www.satel.eu** website is the current version of control panel firmware and the FLASHX program enabling to write it to the control panel. The firmware replacement, which is carried out through the control panel RS-232 port, does not require any panel dismantling. The mainboard RS-232 port and the computer port should be connected as shown in Fig. 1 (you can purchase a ready-made cable, available from SATEL).

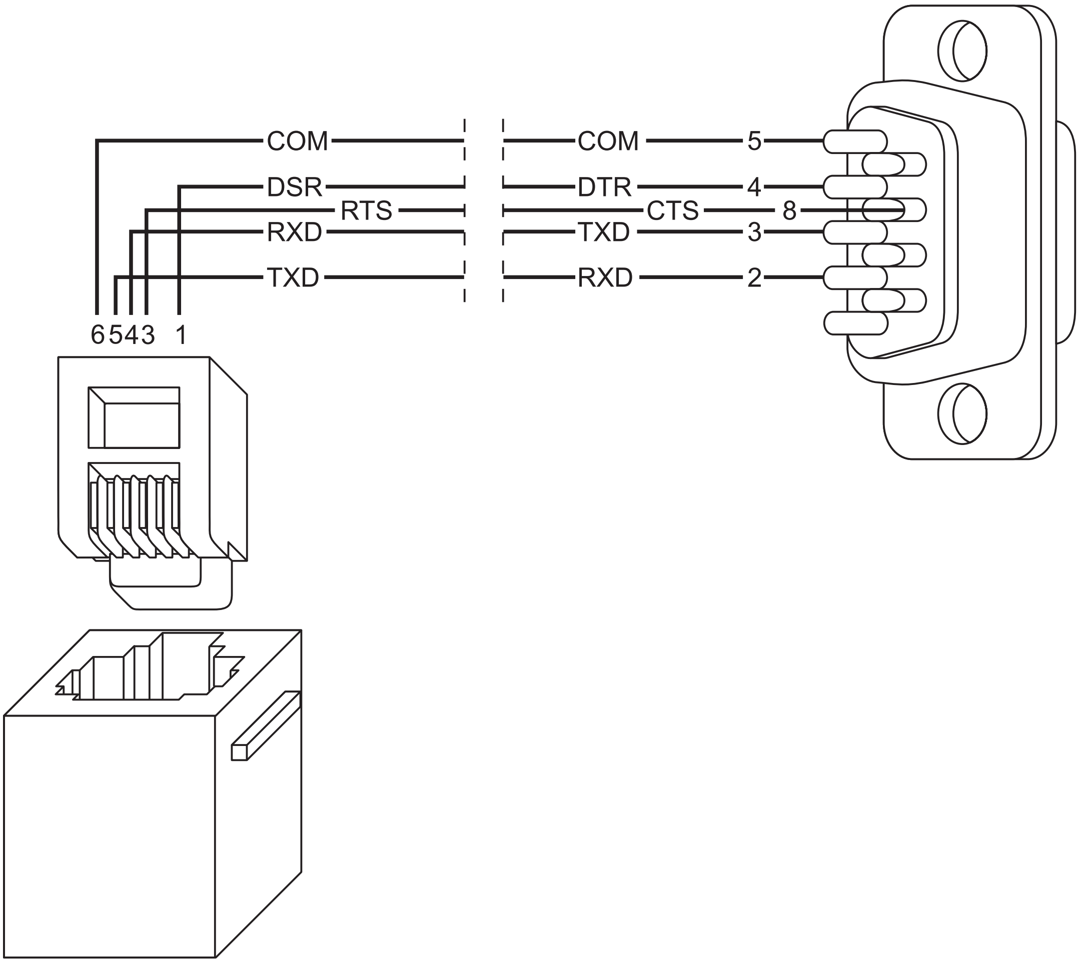


Fig. 1. Connecting computer to the serial port of control panel. Shown on the left is RJ connector on control panel mainboard. Shown on the right is DB-9 female plug, as seen from solder side.

Note: *It is recommended that the cable be connected first to the control panel connector, and then to the computer connector.*

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, 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 installation of the MobileKPD application), or a palmtop (PDA or MDA, after a suitable application is installed).

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. Using the ▲ or ▼ key, 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 (see: description of the HIDE SERVICE MODE AFTER parameter, section SERVICE OPTIONS).

When exiting the service mode, the alarm control panel checks whether the data in RAM memory have changed as compared with those stored in non-volatile FLASH memory. If the data in RAM memory have changed, a prompt will be displayed, asking whether the new settings are to be written to the FLASH memory. 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 discovery of errors or data loss from RAM memory.

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 the service mode cannot be entered in normal way (e.g. the control panel for some reason does not support the keypad), you can use the so-called "from pins” method – an emergency control panel starting procedure by hardware means. In such a case it is recommended that the control panel factory default settings be restored and the system reconfigured.

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 (in INTEGRA 24, INTEGRA 32, INTEGRA 64 and INTEGRA 128 control panels, the DIALER LED will start blinking).
4. Wait about 10 seconds (in INTEGRA 24, INTEGRA 32, INTEGRA 64 and INTEGRA 128 control panels, the DIALER LED will go off), then remove the jumper from pins. The control panel should automatically enter the service mode menu (in LCD keypads, the [SERVICE] LED will start blinking). The service mode menu will be displayed on the keypad having the lowest address.

   If no service mode menu will be displayed on the keypad, but a prompt will appear asking whether to delete the control panel data, it means that the access to the service mode “from pins" has been disabled in the control panel program (→SERVICE MODE →CONFIGURATION →BLOCK SM). Pressing the key with number 1 will amount to resetting all the control panel settings (restarting to factory default settings), but will enable entering the service mode.
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" with the DISABLE SERVICE MODE option (see: section SERVICE OPTIONS).*

3.1.3 Service mode menu

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

Note: *Functions relating to INTEGRA 128-WRL control panel only are highlighted by white font on black background.*

- **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
      - New object
      - Delete object
    - **Partitions**
      - **Settings**
        - [select partition by name]
          - Type
          - Dep. partitions
          - Timers 1..32
          - Timers 33..64
          - **Options**
            - 2 cds to arm
            - 2 cds to d-arm
            - Codes on 2 arm
            - Timer priority
            - Fin. exit time
            - Infin. ex. time
          - Exit delay
          - Auto-arm delay
          - Al. verify time
          - Al. verify time

- Guard – armed
- Guard – disarm.
- Time for guard.
- C. mach. blk.del.
- C. mach. blk. time
- **Zones**
- Name

Names

- [select partition by number]

Hardware

- **LCD keypads**
  - **Settings**
    - [select device by name – see: section SERVICE MENU FOR DEVICES TO BE CONNECTED TO KEYPAD BUS]
  - **Names**
    - [select device by type and address]
  - DTM short
  - Loud tamp.DTM
- **Expanders**
  - **Settings**
    - **ABAX - INTEGRA**
      - Response period:
      - New device
      - Active mode
      - Configuration
      - Filter
      - Remove device
      - Synchronization
      - Test mode on
      - Test mode off
    - [select device by name – see: section SERVICE MENU FOR DEVICES TO BE CONNECTED TO EXPANDER BUS]
  - ABAX confirmat.
  - INT-IT-wt.2cd.
  - Rem. RX key fobs
  - Copy RX keyfobs
  - Rem. ABAX kfobs
  - Copy ABAX kfobs
  - **Names**
    - [select device by type and address]
  - DT1 short
  - Loud tamp.DT1
  - DT2 short
  - Loud tamp.DT2
- **Identification**
  - LCD keypads id.
  - Expanders id.
  - **Keypads addr.**
- EOL R1 resistor
- EOL R2 resistor
- **GSM**
  - Use GSM phone
  - PIN code

- PUK code
- Modem format
- SMS centre
- SMS DloadX
- SMS GuardX
- GPRS
  - APN
  - User
  - Passwd
  - DNS
  - Addr. D
  - Addr. G
  - Key D
  - Key G
  - Port D
  - Port G
- GSM band
- Sound

Options

- **Tel. options.**
  - Mon. TELEPHONE
  - Mon.GPRS
  - Mon.SMS
  - 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
  - CR+LF
  - Parity bit
  - Parity: EVEN
  - Zone alarms
  - Part/mod. al.
  - Arming/disarm.
  - Bypasses
  - Access control
  - Troubles
  - User functions

  - System events
- **Active rights**
- **Various options**
  - Simple codes
  - Notify of code
  - Confirm with 1
  - Autoabort msg.
  - SM -> menu
  - Tests -> menu
  - No AC-no blght
  - Fast exp. bus
  - No rest. mon.
  - Inf. aft. tamper
  - Zones bef. arm
  - Arm, trb. warn.
  - Blk aft. w. code
  - Troubl. memory
  - Hide alarms
  - Events limit.
  - View clear.al.
- **Do not arm**
  - If verif. al.
  - If tamper
  - If monit. trbl.
  - If batt. trbl.
  - If outs. trbl.
  - If other trbl.
- **Times**
  - Global entry delay
  - Global alarm time
  - Suppr.arm status after
  - AC loss report delay
  - Tel. loss report delay
- Rings to answer
- Min. code length
- Prefix length
- Clock adjustm.
- Daylight saving
- Summer time
- Winter time
- Time server
- Time zone
- PING test
  - PING
  - PING period
  - PING tries

Zones

- **Details**
  - [select zone by name]
    - EOL
    - Sensitivity [x20ms] / Pulses duration / Sensitivity. [ms] / Output
    - Pulses count
    - Type

-
  -
    -
      - Entry delay / Alarm delay / Surveillan. time / Signal. delay / Bypass time / Kpd number / Arming mode / Group
      - 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.
      - Chime in exp. / No al. in kpds.
      - Video, disarmed
      - Video, armed
      - Bypass disabl.
      - Bypass no exit
      - Bell delay / Alarm if armed / Clear alarm / Restore=disarm / Alarm
      - Auto-reset 3
      - Auto-reset 1
      - Auto-rst. clr
      - Pre-alarm / Attend verif. / No restore ev.
      - Abort delay / Part. tmp. block / No viol.monit. / Arm-inactive
      - Rest. after bell
      - Rest. aft. disarm
      - Al. on exit end / Log events / No bp. if armed / Abort voice m.
      - Al. aft.unbps. / Event in arm
      - Tamp. alw. loud
      - Monitor. delay / Chk. if can arm / Restore=bps.v. / Bypass verif.
      - Name
  - **Parameters**
    - Partition
    - EOL
    - Sensit. [x20ms]
    - Type
    - Entry delay
    - Max. violat. time
    - Max. no-viol.t.
    - **Zone options**
      - [select option]
  - **Counters**
    - **Counter n** [n – counter number: 1...16]
      - Max. value
      - Counting time
      - Omit recurs
  - **Bypasses**
    - **Group n** [n – number of bypassed group of zones: 1...16]
      - Zones
      - Bypass on/off
  - **Test**
    - SIGNAL. OUTPUT
    - [select zone]
  - **Names**
    - [select zone by number]
- **Outputs**
  - **Details**
    - [select output by name]

- Function
- Cut-off time
- Polarization +
- Pulsating
- Latch / Timers 9..16 / Timers 17..32 / Timers 33..64
- Arm - no ctrl.
- Zones / Timers / Expanders / Outputs / Users / Doors / Voice mess. / Tel. switches (triggering)
- LCD keypads / Master users / Arm mode sel. / Dialing mode (triggering)
- Partitions / Burg. tst. part. (triggering)
- Fire. tst. part. (triggering)
- Bypass. timers
- Clear in parts.
- Troubles
- Name

- **Parameters**
  - Function
  - Cut-off time
  - **Options**
    - [select option]
- Test
- **Names**
  - [select output by number]

Outputs groups

- Group n outputs [n – number of group of outputs: 1...4]
- Group n name [n – number of group of outputs: 1...4]
- Outs state by

Timers

- **Times**
  - [select timer by name]
- **Names**
  - [select timer by number]

User schedules

- **Settings**
  - [select schedule by name]
- **Names**
  - [select schedule by number]

Monitoring

- Mon. TELEPHONE
- Mon. GPRS
- Mon. SMS
- Mon. ETHM-1
- Dont rep. rsts.
- Stations
- **Advanced**
  - Long hsk.s1t1
  - Long hsk.s1t2
  - Long hsk.s2t1
  - Long hsk.s2t2
  - Long hsk. wait.
  - Need ack.id.s1
  - Id. 6-chars s1
  - Source name s1

  - Partit.name s1
  - SIA evr.bl.s1A / TELIM 0ton s1A
  - SIA evr.bl.s1B / TELIM 0ton s1B
  - Need ack.id.s2
  - Id. 6-chars s2
  - Source name s2
  - Partit.name s2
  - SIA evr.bl.s2A / TELIM 0ton s2A
  - SIA evr.bl.s2B / TELIM 0ton s2B
- **Station 1**
  - Tel. 1 number
  - Tel. 2 number
  - Tel. 1 format
  - Tel. 2 format
  - Server address
  - Server port
  - Key (server)
  - Key (GPRS)
  - Key (ETHM-1)
  - Tel.num.for SMS
  - SMS format
  - Repetition cnt.
  - Suspension time
  - TELIM/SIA prefix
  - Identifier n [n – identifier number: 1...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)
  - Key (ETHM-1)
  - Tel. num. for SMS
  - SMS format
  - Repetition cnt.
  - Suspension time
  - TELIM/SIA prefix
  - Identifier n [n – identifier number: 1...8]
  - Identifier sys.
  - Event assign.
- **Id. assignment**
  - **Partitions**
    - [select partition]
  - **Zones**
    - [select zone]
  - **LCD keypads**
    - [select keypad]
  - **Expanders**

        - [select expander]
  - TELIM codes
  - **Event codes**
    - **Identifier n** [n – identifier number: 1...8]
      - **Zones**
        - [select zone]
      - **Partitions**
        - [select partition]
      - **LCD keypads**
        - [select keypad]
      - **Expanders**
        - [select expander]
    - **Identifier sys.**
      - Troubles
      - Troubles rst.
      - Other
  - Test at
  - Test MS1 every
  - Test MS2 every
- **Messaging**
  - Messaging
  - Double v. mess.
  - Repetition cnt.
  - Tel. names
    - [select telephone by number]
  - **Tel. settings**
    - [select telephone by name]
      - Tel. number
      - Messaging type
      - Rounds count
      - Any code
      - Code
  - **Assignment**
    - Zone alarms
      - Synthesizer
      - Pager message
      - Telephones
    - Zone tampers
      - Synthesizer
      - Pager message
      - Telephones
    - Burglary alarms
      - Synthesizer
      - Pager message
      - Telephones
    - Fire alarms
      - Synthesizer
      - Pager message
      - Telephones
    - Medical alarms
      - Synthesizer
      - Pager message
      - Telephones

        - Duress alarms
            - Synthesizer
            - Pager message
            - Telephones
        - Tampers
            - Synthesizer
            - Pager message
            - Telephones
        - AC (230V) loss
            - Synthesizer
            - Pager message
            - Telephones
        - Outputs
            - Synthesizer
            - Pager message
            - Telephones
    - **Messages**
        - [select message]
    - **Pager types**
        - [select pager]
    - **Msg. abort in P.**
        - [select telephone by name]
    - **Msg. abort on T.**
        - [select telephone by name]

- **Tel. answ./ctrl.**
    - Answering
    - Double call
    - Rings count
    - On armed part.
    - Remote control
    - Users (all)
        - [select user from the list of all users]
    - Users (t.code)
        - [select user from the list of users with telephone code]
- **SMS control** [n – number of SMS message: 1...32]
    - SMS -> z.viol.
        - SMS n
        - SMS n – wej.
    - SMS -> function
        - SMS n
        - SMS n – fun.
        - SMS n – part.
        - SMS n – zones
        - SMS n – outs.
        - SMS n – name
    - SMS check state
    - Partitions list
    - Authorized tel.
    - Tel.cod.in SMS
    - Case sensitive
    - Confirm by SMS
    - SMS control

Note

- Text
- Valid
- From
- For
- Who can erase

System status

- Partitions
- Zones
- Troubles
- Supply voltage
- Radio devices
- ST prog. version
- GSM IMEI/v/sig.
- IP/MAC ETHM-1
- Modules version

Restarts

- Clear all
- Clear settings
- Clear codes
- Settings<-FLASH
- **Starter**

Service menu for devices to be connected to keypad bus

[SERVICE CODE][*][9] →Structure →Hardware →LCD keypads →Settings

INT-KLCD / INT-KLCDR / INT-KLCDK / INT-KLCDL / INT-KLCDS / INT-KSG

- Partitions
- Alarms
- Fire alarms
- Chime zones
- Chime bps. zone
- Chime bps. time
- Quickarm part.
- Fin. exit time
- Entry time p.
- Exit time part.
- Date Time format
- Name (2nd row)
- LCD backlight
- Keys backlight
- Auto backlight
- **Alarm messages**
  - Part. al. mess.
  - Zone al. mess.
- **Alarms**
  - Fire alarm
  - Medical alarm
  - Panic alarm
  - Silent panic
  - 3 wrong codes
- **Options**
  - Entry time s.
  - Exit time sig.
  - Alarm signal.

    - New trbl. sign.
    - Key sounds
    - Trbl. in p.arm.
    - Zone violation
    - Auto-arm delay
    - Unkn. card sig.
    - Ev.3 unk. cards
    - Al.3 unk. cards
    - Dspl. mode chg.
    - Show code ent.
    - Show disarming
    - Control (8#)
    - **RS communicat.** (does not apply to INT-KSG)
  - Sound volume (only INT-KLCD-GR/BL, INT-KLCDR-GR/BL and INT-KSG)
  - **Reviews**
    - Zones
    - Partitions
    - Alarms log
    - Troubles log
    - Troubles
    - Chime changing
  - State part.
  - Zone characters
  - Part. characters
  - **Code+arrows**
  - Sensitivity (only INT-KLCDR-GR/BL with firmware version 1.06 or newer)
  - Card close
  - Card close long
  - Door to open
  - Tamper in part.
  - Z1 (n) in kpd [n – number of zone in the system]
  - Z2 (n) in kpd [n – number of zone in the system]
- **CA-64 PTSA**
  - Zones
  - Partitions
  - Alarms
  - What to show
  - AC delay
  - RS communicat.
  - Tamper in part.
- **ETHM-1**
  - Use DHCP
  - Address IP
  - Netmask
  - Gateway
  - DHCP-DNS
  - DNS
  - Port (WWW)
  - Port (DloadX)
  - Port (others)
  - Key (DloadX)
  - Key (others)
  - Connect DloadX

- Connect GuardX
- Connect Intern.
- Connect GSM
- PING test
- Tamper in part.
- Fail. – event
- Fail. – alarm

INT-RS

- DSR control
- RX control
- Tamper in part.

Service menu for devices to be connected to expander bus

[SERVICE CODE][*][9] →Structure →Hardware →Expanders →Settings

INT-CR / INT-IT

- Partit. LED R
- Partit. LED G
- Partit. LED Y
- Master users
- Users
- **Signalling**
  - Alarm (latch)
  - Alarm (time)
  - Entry time
  - Exit time
  - Auto-arm delay
  - Hardw. signal
- Al. 3 unk .cards
- No autorst.3t.
- Tamper in part.

INT-S / INT-SK / INT-SCR

- Lock feature
- **Lock**
  - Lock feature
  - Relay ON time
  - Relay type (only INT-S and INT-SK)
  - Unauth. event
  - Unauth. alarm
  - Max. door open
  - Dependent door1
  - Dependent door2
- Doors on fire
- Master users
- Users
- **Alarms**
  - Fire alarm
  - Medical alarm
  - Panic alarm
  - Silent panic
  - 3 wrong 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

INT-SZ / INT-SZK

Lock

- Lock feature
- Relay ON time
- Relay type
- Unauth. event
- Unauth. alarm
- Max. door open
- Dependent door1
- Dependent door2

Doors on fire
Master users
Users

Alarms

- Fire alarm
- Medical alarm
- Panic alarm
- Silent panic
- 3 wrong codes

Options

- Part.blocking
- Guard control
- Changing code

Signaling

- Code entered
- Chime zones

Confirmation
Backlight
Auto backlight
No autorst.3t.
Partition

INT-ENT

Master users

- Users
- 3 wrong codes
- BI outs ctrl.
- MONO outs ctr.
- Guard control
- **Signalling**
  - Delay act. time
  - Code entered
- Confirmation
- Backlight
- Delay act. time
- No autorst.3t.
- Partition

CA-64 SR / CA-64 DR

- Lock feature
- **Lock**
  - Lock feature
  - Relay ON time
  - Unauth. event
  - Unauth. alarm
  - Max. door open
  - Dependent door1
  - Dependent door2
- Doors on fire
- Master users
- Users
- **Readers**
  - Reader A (only CA-64 SR)
  - Reader A sound
  - Reader A LED
  - Reader A arms
  - Reader B (only CA-64 SR)
  - Reader B sound
  - Reader B LED
  - Reader B arms
- Al. rdrs tamper (only CA-64 SR)
- 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

INT-RX

- No autorst.3t.
- Partition

ACU-100

- No autorst.3t.
- Tamper in part.
- Response period
- New device
- **Active mode**
  - [select zone to which wireless device is assigned]
- **Configuration**
  - [select zone to which wireless device is assigned]
- **Filter**
  - [select zone to which wireless device is assigned]
- **Remove device**
  - [select zone to which wireless device is assigned]
- Synchronization
- Test mode on
- Test mode off

CA-64 E / CA-64 O / INT-ORS / INT-IORS / CA-64 SM

- No autorst.3t.
- Tamper in part.

CA-64 Ei (v. 2.00/2.01)

- No autorst.3t.
- Tamper in part.
- EOL Rp resistor

CA-64 Ei (v. 4.00)

- No autorst.3t.
- Tamper in part.
- EOL R1 resistor
- EOL R2 resistor

CA-64 EPS / CA-64 ADR / CA-64 OPS / CA-64 PP

- No autorst.3t.
- Tamper in part.
- AC loss delay

CA-64 EPSi (v. 2.00/2.01)

- No autorst.3t.
- Tamper in part.
- EOL Rp resistor
- AC loss delay

CA-64 EPSi (v. 4.00)

- No autorst.3t.
- Tamper in part.
- EOL R1 resistor
- EOL R2 resistor
- AC loss delay

3.1.4 Entering data by means of the keypad

The method of programming depends on the type of data entered with the service function. The data will be written to the control panel on pressing [#] or [ok]. The [*] key enables exiting the function without saving any changes. Described below are general programming rules, however they can be different in case of some functions.

Selection from the single-choice list

The upper line of display shows the function name, and the lower one – the currently selected item. To scroll through the item list, use the ▼ keys (down) and the ▲ keys (up). The ▶ and ◀ keys are not used.

Selection from the multiple-choice list

If the function enables several items to be selected (options, zones, outputs, etc.), two programming alternatives are possible:

1. Both lines of the display present items that can be selected. To scroll through the list, use the ▼ key (down) and the ▲ key (up). Situated at the end of the line, on the right-hand side, is a symbol indicating whether the item is selected - ▣, or not - · . Press any number key to change the currently displayed symbol to the other one for the item indicated by the arrow on the left-hand side of the display.
2. The upper line of display shows the function description, and the lower one – one of the items to choose from. To scroll through the item list, use the ▼ keys (down) and the ▲ keys (up). Shown in the upper right corner of the display is symbol indicating whether the item is selected - ▣, or not - · . Press any number key to change the currently displayed symbol to the other one. Press ▶ or ◀ to switch the keypad over to the **graphical programming mode**. The ▣ and · symbols are used to present on the display the current status of all items available within the given function. Use the ▶ key to move the cursor to the right, and the ◀ key to move it to the left. If the list of items is longer than 32, press ▶ when the cursor is on the last item to display the next group, or press ◀ when the cursor is on the first item – to display the previous (or the last) group. Press ▼ or ▲ for the keypad to return to the text mode.

Entering decimal and hexadecimal values

Digits are entered by pressing the suitable keys. Characters from A to F available under the [2] and [3] keys. Keep pressing the keys until the required character appears.

Programming telephone numbers

Keep pressing particular keys until the required character appears. Characters available in the keypad are presented in Table 1. Up to 16 characters can be programmed. Some of the special characters (a, b, c, d, # and ✻) are coded so that the character takes up two items, hence the maximum number of characters available for entering, if they are used, will be lower.

Characters available after next keystroke									
key	mode [ABC]				key	mode [abc]			
1	1	#			1	1	#		
2	2	B	C		2	2	a	b	c
3	3	D	E	F	3	3	d		
4	4				4	4			
5	5				5	5			
6	6				6	6			
7	7				7	7			
8	8				8				
9	9				9	8			
0	0	✻			0	0	✻		

Table 1. Characters available in the keypad when entering telephone numbers (to change the letter case, press ▼).

Shown on the left side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing the ▼ key, which changes the letter case, and will be visible for a few seconds after the last keystroke).

Special character	Function description
B	switch-over to pulse dialing
C	switch-over to tone dialing (DTMF)
D	waiting for additional signal
E	3 second pause
F	10 second pause
✱	signal ✱ in DTMF mode
#	signal # in DTMF mode
a b c d	other signals generated in DTMF mode

Table 2. Special character functions.

Entering names

Keep pressing particular keys until the required character appears. Characters available in the keypad are presented in Table 3. Hold down the key to display the digit assigned to the key.

Shown on the left side in the upper line of the display is information about the letter case: [ABC] or [abc] (it will be displayed after pressing any key and will be visible for a few seconds after the last keystroke).

The ▶ key moves the cursor to the right, and the ◀ key – to the left. The ▲ key deletes the character on the left side of the cursor.

Key	Characters available after next keystroke																	
1	!	?	'	`	↵	"	{	}	$	%	&	@	\	^	|	✎	#	1
2	a	b	c	2														
3	d	e	f	3														
4	g	h	i	4														
5	j	k	l	5														
6	m	n	o	6														
7	p	q	r	s	7													
8	t	u	v	·	▦	█	▯	↑	←	→	↓	8						
9	w	x	y	z	9													
0		.	,	:	;	+	-	✱	/	=	_	<	>	(	)	[	]	0

Table 3. Characters available when entering names. The lower case letters are available under the same keys (to change the letter case, press ▼ key).

3.2 DLOADX-INSTALLER PROGRAM

Note: *If the PERMANENT DLOADX ACCESS option is enabled (see: USER MANUAL), programming by means of the DLOADX program is possible even when the service has no access to the control panel.*

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.

The alarm control panel can be programmed locally or remotely.

1. **Local programming** requires connection of the RS-232 port on control panel mainboard (RJ type socket) to the computer COM port. The connection should be made as shown in Fig. 1 on page 4 (you can buy a ready-made cable, manufactured by SATEL).
2. In case of **remote programming,** communication with the control panel can be established in several ways:
   - by the built-in 300 bps modem through the telephone network (considering the transmission rate limited to 300 baud, the programming takes a longer time);
   - by the built-in GSM communicator, using CSD technology, through the GSM cellular telephone network **only INTEGRA 128-WRL**;
   - by the built-in GSM communicator, using GPRS technology **only INTEGRA 128-WRL**;
   - by the external modem connected to the RS-232 port of control panel mainboard through the telephone network;
   - by the GSM module, manufactured by SATEL, operating as an external modem with the use of CSD technology, through the GSM cellular telephone network;
   - by the ISDN module, manufactured by SATEL, operating as an external modem through the ISDN digital telephone network;
   - by the ETHM-1 module connected to the RS-232 port of control panel mainboard through the TCP/IP network (local networks and Internet).

Note: *The data transmission service with the use of CSD technology 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.*

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

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

1. Connect the RS-232 port of control panel to the computer port (see Fig. 1 on page 4).
2. Enter the **service code** from the keypad (by default 12345) and press [*].

3. Using the arrow keys, scroll the function list until the arrow indicates the function DOWNLOADING.
4. Press the [#] or [▶] key.
5. Select the item START DWNL-RS and press the [#] or [▶] key.
6. 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 button, and then on the window which will appear, and indicate the computer port through which communication is to be effected.
7. 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. The GSM communicator of INTEGRA 128-WRL control panel supports sending data with the use of CSD technology, i.e. at a rate of 9.6 kb/s. In case of the other control panels, higher transmission rates can be obtained after an external modem is connected. The INTEGRA control panels can interact with external analog, ISDN and GSM modems. Setting up a modem connection between the control panel and the PC will be possible, provided that there is a suitably selected modem on the computer side (see the table below).

Configuration on control panel side	Configuration on computer side
Built-in 300 bps modem	Analog modem
External analog modem	Analog modem
	GSM modem
External ISDN modem	ISDN modem
	GSM modem
External or built-in GSM modem	Analog modem
	ISDN modem
	GSM modem

Table 4. Ways to connect alarm control panel with computer for telephone communication.

The external modem or the communication module (GSM or ISDN) used as an external modem must be connected to the control panel RS-232 port (see Fig. 2 and 3).

The modem and alarm control panel must be suitably configured so that remote programming can be possible. Communication between control panel and modem can be established in several ways (shown in parentheses is information on the required configuration on the control panel side):

1. Connection initialized by the control panel (all configurations).
2. Connection initialized from the DLOADX program (built-in modem 300 bps, external analog modem or external ISDN modem).

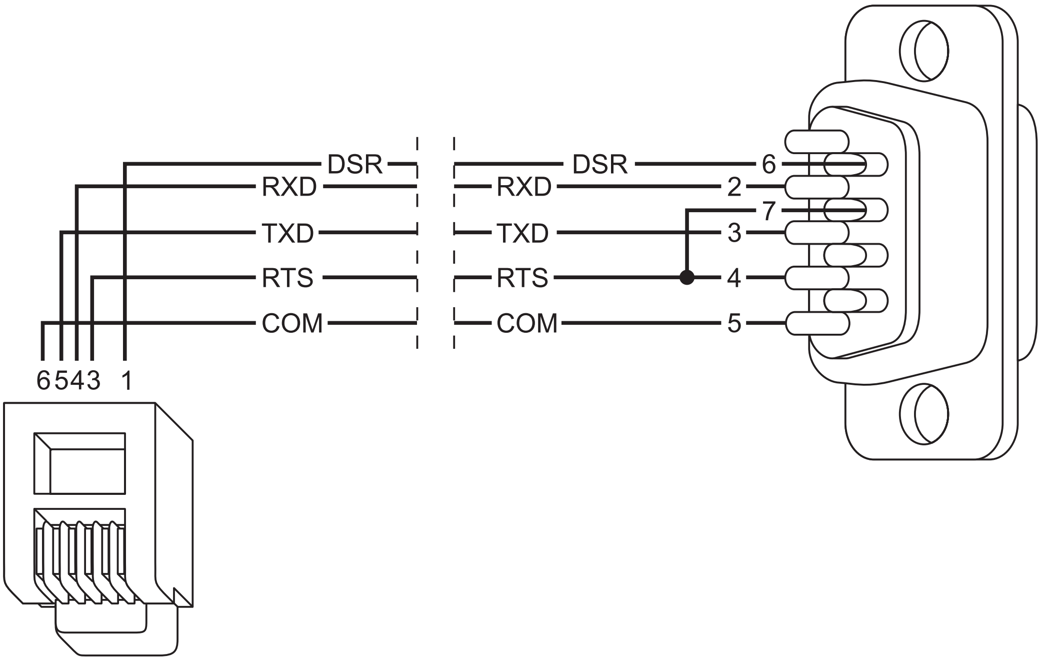


Fig. 2. Connecting the external modem with DB-9 socket to the control panel RS-232 port. Shown on the left is RJ plug, to be connected to the socket on control panel mainboard. Shown on the right is DB-9 male plug (seen from solder side).

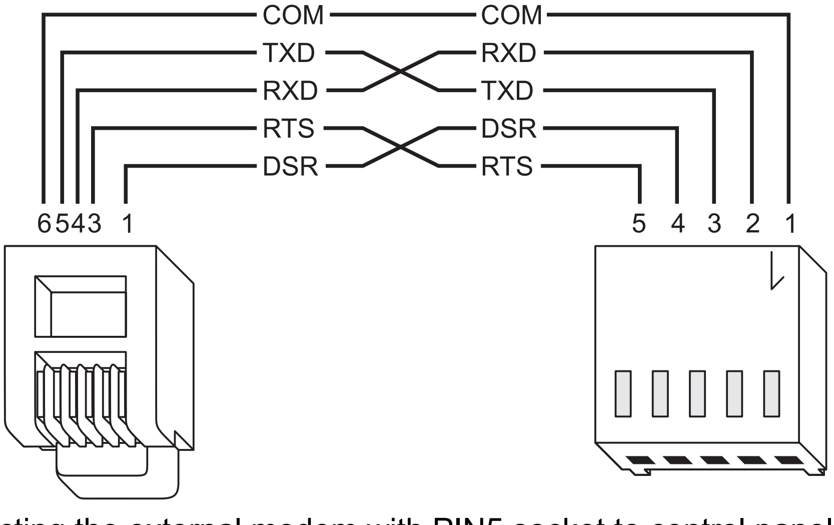


Fig. 3 Connecting the external modem with PIN5 socket to control panel RS-232 port (GSM, ISDN and ETHM-1 modules are similarly connected). Shown on the left side is RJ plug, to be connected to control panel on-board socket. PIN5 connector is shown on the right.

3. Connection initialized from the DLOADX program, but the control panel calls back and sets up the connection (built-in 300 bps modem, external analog modem or external ISDN modem).

4. Connection initialized by means of SMS, after reception of which the control panel sets up the connection (GSM module operating as an external modem, INTEGRA 128-WRL control panel).

In the modem 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.

Configuration of settings in modem to be connected to computer

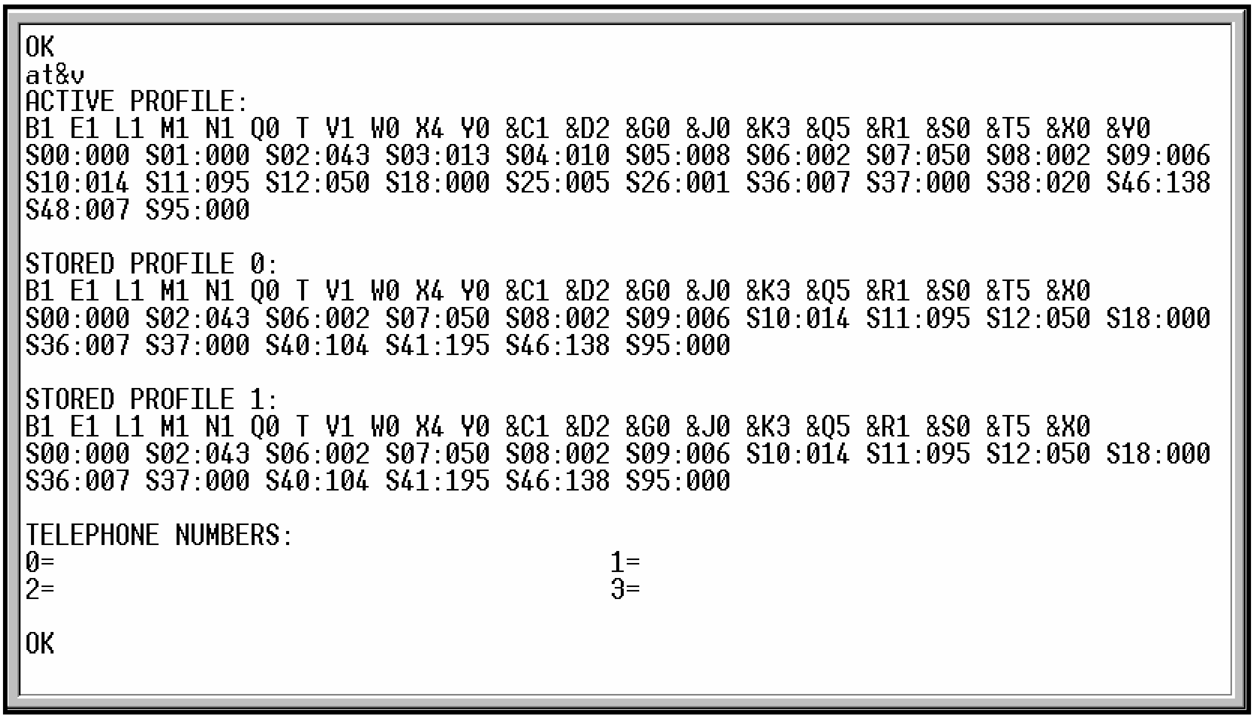
The modem connected to the computer can be configured by using the DLOADX program. For this purpose, click on the button to open the CONFIGURATION window. The MODEM tab makes it possible to define modem settings for three different configurations on the control panel side (built-in 300 bps modem, external analog modem or ISDN/GSM) modem. A click on the button will open for editing the parameters of modem communication port and initializing commands.

Configuration of settings in modem to be connected to control panel

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 Fig. 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 Fig. 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".*

Configuration of control panel settings

Depending on the modem type and the method of establishing communication, do the following in the control panel:

- If the control panel is to execute the connection, enter the telephone number of the computer from which the control panel is to be programmed (Service mode →Configuration TS →**Telephone DloadX**).
- If the connection is to be initialized by the computer or by means of SMS message, enable the **Answering – modem** option (Service mode →Options →Telephone options →Aswering. modem).
- If the connection is to be initialized by the computer, set the number of rings after which the control panel will answer the call (Service mode →Options →**Rings count**).
- If the connection is to be initialized by the computer and the control panel is to only go off hook after the second call, enable the **Double call** option (Service mode →Options →Telephone options →**Double call**).
- If an external modem is connected to the control panel, enable the **External modem** option (Service mode →Options →Telephone options →Ext. Modem).
- If a GSM or ISDN module is connected to the control panel as an external modem, enable the option **Modem ISDN/GSM** (Service mode →Options →Telephone options →Modem ISDN/GSM).
- If the control panel is to execute the connection after receiving an SMS message, define the code which will have to be included in the SMS message body to initialize communication with the DloadX program (Service mode →Structure →Hardware →GSM →**SMS DloadX**). **only INTEGRA 128-WRL**

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. In case of the INTEGRA 128-WRL control panel, they are*

only meaningful when communication is to be effected at a rate of 300 bps or an external analog modem is connected.

Connection initialized by the control panel through built-in 300 bps modem

1. Click the button in the DLOADX program and select "Modem 300 bps" from the drop-down menu. The window will then open where the modem initializing information will be shown.
2. Start the START DWNL-TEL function ([*code*][*] ➔DOWNLOADING ➔START DWNL-TEL) in the LCD keypad connected to the control panel. This function is available to the service technician and to the administrators/users having the DOWNLOADING STARTING authority level.
3. The control panel will call the programmed computer telephone number.
4. Establishing connection will be indicated by the DLOADX program with a suitable message.

Connection initialized by the control panel through external modem

1. Click the button in the DLOADX program and select "Modem - INTEGRA with ext. modem" from the drop-down menu. The window will then open where the modem initializing information will be shown.
2. Start the START DWNL-MOD function ([*code*][*] ➔DOWNLOADING ➔START DWNL-MOD.) in the LCD keypad connected to the control panel. This function is available to the service technician and to the administrators/users having the DOWNLOADING STARTING authority level.
3. The control panel will call the programmed computer telephone number.
4. Establishing connection will be indicated by the DLOADX program with a suitable message.

Connection initialized by the control panel through built-in GSM communicator (using CSD technology) only INTEGRA 128-WRL

1. Click the button in the DLOADX program and select "Modem - INTEGRA with ext. modem" from the drop-down menu. The window will then open where the modem initializing information will be shown.
2. Start the START DWNL-CSD function ([*code*][*] ➔DOWNLOADING ➔START DWNL-CSD) in the LCD keypad connected to the control panel. This function is available to the service technician and to the administrators/users having the DOWNLOADING STARTING authority level.
3. The control panel will call the programmed computer telephone number.
4. Establishing connection will be indicated by the DLOADX program with a suitable message.

Connection initialized from the DLOADX program

1. Click the button in the DLOADX program and select in the drop-down menu the modem type corresponding to that on the control panel side (for CSD communication in the INTEGRA 128-WRL control panel, select "Modem - INTEGRA with ext. modem"). The window will then open where the modem initializing information will be shown.
2. Click with your mouse pointer on the „Connect" button.
3. After the programmed number of rings (or after the second number call, if the DOUBLE CALL option has been enabled) the control panel will answer the call and the connection will be established. It will be indicated by the DLOADX program with a suitable message.

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

1. Click the button in the DLOADX program and select in the drop-down menu the modem type corresponding to that on the control panel side (for CSD communication in the

INTEGRA 128-WRL control panel, select "Modem - INTEGRA with ext. modem"). The window will then open where the modem initializing information will be shown.

2. Click with your mouse pointer on the „Connect” button.
3. After the programmed number of rings (or after the second number call, if the DOUBLE CALL option has been enabled) the control panel will answer the call, acknowledge receiving the call, and disconnect. Then it will call back the computer telephone number programmed in the control panel.
4. Establishing connection will be indicated by the DLOADX program with a suitable message.

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

1. Click the button in the DLOADX program and select "Modem - INTEGRA with ext. modem" from the drop-down menu. The window will then open where the modem initializing information will be shown.
2. Send an SMS message to the INTEGRA 128-WRL control panel / to the GSM module connected to the alarm control panel. In case of the INTEGRA 128-WRL control panel the SMS message should look as follows:

   „**xxxx=csd=**” („xxxx” denotes the code defined in control panel which triggers communication with DLOADX program) – the control panel will call the programmed telephone number of the computer; the data will be sent using CSD technology;

   „**xxxx=yyyy=**” („xxxx” denotes the code defined in control panel which triggers communication with DLOADX program; "yyyy" denotes telephone number of the computer with which the control panel is to establish communication) – the control panel will call the telephone number sent in the SMS message (the computer telephone number programmed in control panel will be ignored); the data will be sent using CSD technology.

   If the GSM module is connected to the control panel as an external modem, the SMS message should look as follows:

   „**xxxx**” („xxxx” denotes the code defined in module which triggers communication with DLOADX program) – the control panel, using the module, will call the programmed computer telephone number; the data will be sent using CSD technology;

   „**xxxx=yyyy.**” („xxxx” denotes the code defined in module which triggers communication with DLOADX program; "yyyy" denotes telephone number of the computer with which the control panel is to establish communication) – the control panel, using the module, will call the telephone number sent in the SMS message (the computer telephone number programmed in control panel will be ignored); the data will be sent using CSD technology.
3. Having received the SMS message, the control panel will call the computer telephone number (the INTEGRA 128-WRL control panel will, additionally, send an SMS acknowledgement message). Establishing connection will be indicated by the DLOADX program with a suitable message.

3.2.3 Remote programming with the use of GPRS technology only INTEGRA 128-WRL

The SIM card installed in the control panel must have the GPRS service activated!

The computer on which the DLOADX program will be running must have an IP address which is visible on the Internet (so-called public IP address) or the network server port must be redirected to that computer, so as to make connection with that computer possible.

The following items are to be programmed in the control panel:

- Access point name (APN) for Internet GPRS connection (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**APN**).

- User name for Internet GPRS connection (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**USER**).
- Access code for Internet GPRS connection (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**CODE**).
- IP address of the DNS server which is to be used by the control panel (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**DNS**). The DNS server address is not to be programmed if the computer address is entered in numerical form (4 decimal numbers separated by dots).

Note: *APN, user name, code and DNS server address can be obtained from the GSM network operator.*

- Address of the computer (or the network server whose port has been redirected to the computer) with which the control panel is to establish communication (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**ADDRESS D**). The address can be entered in numerical form or as a name.
- Number of the network port through which communication with the DLOADX program will be effected (SERVICE MODE →STRUCTURE →HARDWARE →GSM →GPRS →**PORT D**).
- If the control panel is to establish GPRS communication after receiving an SMS message: the code which has to be included in the SMS message body to initialize communication with the DLOADX program (SERVICE MODE →STRUCTURE →HARDWARE →GSM →**SMS DLOADX**).

Communication between the control panel and the computer can be established in two ways:

1. Initializing connection by the control panel.
2. Initializing connection by means of an SMS message, after receiving of which the control panel will establish a connection.

Irrespective of the chosen method of establishing communication, the DLOADX program must be running on the computer, and receiving GPRS connections from the control panel must be enabled (the server must be activated):

1. Click on the button to open the menu.
2. Select the "TCP/IP: DloadX <- GPRS" command. The server activation window will open.
3. Define the number of network port through which the server (the computer with DLOADX program) will communicate with the control panel. The number must correspond to that programmed in the control panel.
4. Click on the "Start" button. This will activate the server which will be waiting for establishing a connection by the control panel.

Connection initialized by control panel

Having activated the server on your computer, start the START DWNL-GPRS function on the LCD keypad ([*code*] [*] →DOWNLOADING →START DWNL-GPRS). This function is available to the service personnel and to the administrators/users having the DOWNLOADING authority level.

Connection initiated by SMS message, after reception of which the control panel establishes connection

An SMS message should be sent to the INTEGRA 128-WRL control panel. The message should look as follows:

„**xxxx=gprs=**" („xxxx" denotes the code defined in control panel which triggers communication with DLOADX program) – the control panel will connect to the computer whose IP address was preprogrammed beforehand;

„**xxxx=aaaa:p=**" („xxxx" denotes the code defined in control panel which triggers communication with DLOADX program; "aaaa" stands for address of the computer with which the control panel is to establish communication, entered in numerical form or as a name; "p" is number of the network port through which communication with the DLOADX program is to be effected) – the control panel will connect to the computer whose address was given in the SMS message (the computer IP address and port which are programmed in the control panel will be ignored).

3.2.4 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.

1. Locally:
   - through RS-232 port of LCD keypad;
   - through RS-232 port of INT-RS converter;
   - through RS-232 port on control panel mainboard.
2. Remotely:
   - through TCP/IP network (local networks and Internet) by means of a locally connected computer on which the GUARDSERV program is running;
   - through built-in GSM communicator with the use of CSD technology, by means of GSM cellular telephone network **only INTEGRA 128-WRL**;
   - through built-in GSM communicator with the use of GPRS technology **only INTEGRA 128-WRL**;
   - through external modem connected to the RS-232 port on control panel mainboard, by means of telephone network;
   - through SATEL made GSM module, operating as an external modem with the use of CSD technology, by means of GSM cellular telephony network;
   - through SATEL made ISDN module, operating as an external modem, over ISDN digital telephony network;
   - through the ETHM-1 module connected to control panel, over TCP/IP network (local networks and Internet).

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. GSM Phone only INTEGRA 128-WRL

The GSM phone enables the INTEGRA 128-WRL control panel to execute the functions of monitoring, messaging, call answering and control, and makes remote programming possible (GSM or GPRS). Settings of the control panel GSM telephone can be programmed by means of LCD keypad (SERVICE MODE →STRUCTURE →HARDWARE →GSM) or DLOADX program (window STRUCTURE, tab HARDWARE, branch GSM PHONE).

GSM using – this option must be enabled if the control panel is to support the GSM communicator. The option may be disabled if the GSM communicator is not to be used (e.g. SIM card is not installed, etc.). Disabling the option will thus prevent any GSM related troubles from being unnecessarily reported.

PIN Code – PIN code of the SIM card. Entering a wrong code may result in blocking the SIM card.

Note: *If the PIN code of SIM card is inconsistent with that entered in the control panel settings, the control panel will inform of it by means of a suitable message and an audible signal in the LCD keypad. After 255 seconds the control panel will retry to use the PIN code. If the PIN code is wrong, the control panel will signal it again. After the third attempt to use a wrong PIN code, the card will be blocked. In such a case, the PUK code will have to be entered.*

PUK code – this option is only available in LCD keypads (SERVICE MODE →STRUCTURE →HARDWARE →GSM →PUK CODE), when as a result of entering invalid PIN code the SIM card has been blocked. After entering a correct PUK code, confirmed by pressing the [#] key, the SIM card will by unblocked, receiving a new PIN code (the one entered in the PIN CODE function).

Modem format – GSM modem transmission format. The modem format should be selected, with consideration for the type of modem used with the computer and the scope of services provided by the cellular network operator.

SMS center number – telephone number of the SMS message management center, which acts as an agent in sending SMS messages. Entering the number is necessary if the GSM communicator is to send SMS messages. The number entered in the control panel must correspond to the network in which the GSM communicator is used (this depends on the SIM card installed in the control panel).

SMS DloadX – password that must be included in the SMS message sent to the control panel, so that it can start the procedure of establishing communication with the DLOADX program (communication through modem or by means of GPRS technology).

SMS GuardX – password that must be included in the SMS message sent to the control panel, so that it can start the procedure of establishing communication with the GUARDX program (communication through modem or by means of GPRS technology).

APN – name of the access point for Internet GPRS connection. You should obtain it from your GSM network operator.

User – name of the user for Internet GPRS connection. You should obtain it from your GSM network operator.

Code – code for Internet GPRS connection. You should obtain it from your GSM network operator.

Note: *For sending data with the use of GPRS technology, you must define the APN, user name and code.*

DNS server – IP address of DNS server to be used by the control panel. It can be obtained from the GSM network operator. It is necessary, when IP address of the device with which the control panel is to communicate using GPRS technology (computer with DLOADX or

GUARDX program, monitoring station) has been entered as a name. It is not required when the addresses have been entered in the numerical form (4 decimal numbers separated by dots).

DloadX Address – address of the computer with DLOADX program with which the control panel is to communicate using GPRS technology. It can be entered in numerical form (4 decimal numbers separated by dots) or in the form of a name.

Port (DloadX) – number of the network port through which communication with DLOADX program will be effected.

GuardX Address – address of the computer with GUARDX program with which the control panel is to communicate using GPRS technology. It can be entered in numerical form (4 decimal numbers separated by dots) or in the form of a name.

Port (GuardX) – number of the network port through which communication with GUARDX program will be effected.

GSM band – selection of the GSM bands to be handled by the GSM telephone. The function is available for electronics version 2.1 or newer. If no band is selected, the telephone will handle all bands.

Additionally, advanced options of programming sound settings in GSM telephone are also available. In most cases, the factory settings of the audio path are optimal for correct communication.

5. Wireless System only INTEGRA 128-WRL

The INTEGRA 128-WRL control panel can directly support (without connecting any additional modules) up to 48 wireless devices (up to 48 wireless zones/outputs) and 248 key fobs of ABAX system. The ABAX system uses two-way communication in 868.0 MHz – 868.6 MHz frequency band. Reception of messages and commands is acknowledged, which guarantees that they have reached the recipient and, additionally, makes possible control of presence of wireless devices in the system. Configuring parameters and testing wireless devices is effected by radio, without dismounting of their enclosures.

The mainboard wireless system can be programmed by means of LCD keypad (SERVICE MODE →STRUCTURE →HARDWARE →EXPANDERS →SETTINGS →ABAX - MAIN BOARD, and in case of the APT-100 key fobs, also SERVICE MODE →STRUCTURE →HARDWARE →EXPANDERS) or DLOADX program (window STRUCTURE, tab HARDWARE, branch WIRELESS SYSTEM, and in case of the APT-100 key fobs, also the KEYFOBS ABAX window, which can be opened by clicking on the KEYFOBS ABAX command in USERS menu). The procedures of adding and deleting the ABAX wireless devices are described in the installation guide. The procedures of adding and deleting the ABAX key fobs, as well as configuring them, are described in the user manual.

Response period – communication with wireless devices takes place in specified intervals. The control panel is then gathering information on the status of wireless devices and, if necessary, sending commands to the devices, e.g. switching the detectors to their active/passive state, switching on/off the test mode and/or changing configuration of the devices. The polling period can be **12**, **24** or **36** seconds. The less frequent is communication between the control panel and the wireless devices takes place, the greater is the number of wireless devices can work with their operating ranges mutually overlapped (for 12 s – maximum 150, for 24 s – 300, and for 36 s – 450). Outside the polling period, information on tampers of devices and violations of active detectors is sent to the control panel. The RESPONSE PERIOD has also impact on the level of energy consumption by the wireless devices. The less frequently communication between the control panel and the wireless devices takes place, the lower energy consumption and the longer battery life is.

Filter – the number of consecutive response periods, during which communication with the device failed to be established, before no communication with the device is reported. Values from the 0 to 50 range can be entered. Entering the digit 0 will disable control of the device presence in the system.

Configuration – some of the wireless devices make additional parameters and options available, which can be configured by radio.

In the LCD keypad, having started the CONFIGURATION FUNCTION (SERVICE MODE →STRUCTURE →HARDWARE →EXPANDERS →SETTINGS →ABAX – MAIN BOARD. →CONFIGURATION) select the zone to which the device you want to configure is assigned, and press the [#] or ▶ key. Even if the device takes up several zones, only the name of the first of them can be displayed. The number of displayed zones depends on the type of device. Having programmed the parameters, confirm the new settings using the [#] key. Automatic return to the zone selection list will follow.

In the DLOADX program, click in the "Configuration" column in the field pertaining to the chosen device and parameters you want to change. Using the keyboard, enter new settings. Having programmed the parameters, write the new settings to the control panel (use the button).

Always active – with this option enabled, the device will be always active (see section: WIRELESS DETECTORS).

Synchronization – this function starts the procedure of synchronization, i.e. checking whether other ABAX wireless systems are working within the control panel range. The control panel will adapt the polling period so as to prevent radio transmissions from being mutually jammed. Synchronization takes place automatically when starting the control panel, and after each operation of adding/deleting devices which are supported by it.

Test mode – when in the test mode, wireless devices will signal communication with the control panel by LED blinking, and detectors will inform about tampers and violations by means of indicator LEDs. During normal work, the LED signaling is off for energy saving reasons. In the test mode, the signaling of sirens is blocked. The test mode is switched on and off during polling, thus causing a delay, the duration of which depends on the programmed polling period. The test period will be switched off automatically 30 minutes after:

- starting the test mode by means of the DLOADX program (the 30 minutes are running from the moment of quitting the WIRELESS SYSTEM branch),
- terminating the service mode in control panel.

Note: *According to the requirements of EN50131 standard, the level of radio signal sent by wireless devices is lowered when the test mode is running.*

Confirming outputs [ABAX confirmation] – you can select up to 8 alarm system outputs, the status of which will be sent to the ABAX system key fobs (the status of up to 3 outputs being sent to a single key fob). See the USER MANUAL for description of how the outputs should be assigned to the key fob LEDs.

Remove ABAX keyfobs – function only available in LCD keypad. It enables deletion of all data regarding the ABAX system key fobs in INTEGRA 128-WRL control panel (in ACU-100 controllers connected to the control panel). It also applies to information on the zones assigned to buttons of individual users' key fobs. Removal of the key fob in any other will not reset settings of the buttons.

Copy ABAX keyfobs – function only available in LCD keypad. If additional ACU-100 controllers (with firmware version 2.0 or later) are connected to the control panel, the function enables copying the key fob related data from the INTEGRA 128-WRL control panel (or ACU-100 controller) to the ACU-100 controller (or INTEGRA 128-WRL control panel). Thus the key fob related data can be made uniform.

5.1 Hardwired zones/output expanders

The ACX-200 or ACX-201 expander takes up 4 zones and 4 outputs in the system. Parameters of the zones and outputs are to be programmed in the same way as those of the other hardwired zones and outputs of the control panel. However, it should be borne in mind that the actual sensitivity of the zones may be different from that programmed by means of the keypad or DloadX program:

– from 20 ms to 140 ms – corresponds to the sensitivity programmed in the control panel;

– above 140 ms – only some values are available: 300 ms, 500 ms, 700 ms etc. every 200 ms (the programmed value is rounded off to the one supported by the expander).

The expander indicates the zone status in real time. Also the expander outputs are controlled in real time. Only the zone programming takes place during the response time (data related to configuration of one zone are sent to the expander during one polling period, i.e. four response periods are required so as to send information on the settings of four zones).

Note: *If the communication with control panel is lost, all of the previously activated outputs will enter the inactive state after 20 response periods.*

Additionally, the ACX-201 expander will transmit information on:

– status of AUX1, AUX2 supply outputs – overload information is sent when the AUX1 or AUX2 output load exceeds 0.5 A.

– battery status – battery discharge information is sent when the battery voltage drops below 11 V for longer than 12 minutes (3 battery tests). This information will be sent to control panel until the battery voltage rises above 11 V for longer than 12 minutes (3 battery tests).

– AC supply status – power supply loss information is sent when the AC supply loss is lasting longer than 30 seconds. Power restore is reported with the same delay.

5.2 Wireless detectors

The wireless detectors send to the control panel information on violations, tampers and low battery status. Information on violations and tampers is transmitted to the zones to which the detectors are assigned. The system zones to which the detectors are assigned can be programmed as:

- NC, NO or EOL – the zone will only inform of detector violation;
- 2EOL/NC or 2EOL/NO – the zone will inform of detector violation and tamper.

Operating mode of the wireless detectors depends on the status of partition to which the zone with wireless detector belongs:

– **partition is disarmed** – the detector is operating in **passive mode**. It is the battery-saving mode during which communication with the control panel takes place mainly in the time intervals set by the Response period option. Information on violations and battery status is sent during that periods, however detector tamper events are sent immediately.

– **partition is armed** – the detector is operating in **active mode**. The detector sends all information to the control panel without delay.

Toggling the detectors from the passive to the active mode and conversely takes place during the polling time, hence it is done with a delay in relation to arming/disarming. Such a delay – depending on the selected polling frequency – can be up to 12, 24 or 36 seconds.

The wireless detectors which are assigned to the 24-h zones (i.e. armed round-the-clock), are always in the active mode. Also other wireless detectors can always work in the active mode, provided that the Always active option is enabled for them.

⚠ **The batteries ensure operation of the detectors for a period of about 3 years, provided that they remain in the passive state for some portion of that period,**

and the Response period is 12 seconds. A longer polling period (24 or 36 seconds) means extension of the battery life time. The battery life time in the detectors switched permanently into the active mode is shorter than in those which are periodically switched to the passive mode. However, if the specific character of a detector or its installation place is such that the number of violations is low, switching the detector permanently into the active mode will not adversely affect the battery life time.

5.2.1 APD-100 detector configuration

The APD-100 wireless passive infrared detector takes up 1 zone in the system. Sensitivity of the detector is remotely programmable, and in case of the firmware version 2.01, you can also enable/disable the option of immunity to pets with a weight of up to 15 kg.

In LCD keypad, the ◀ and ▶ keys enable navigation between programmable parameters. You can change sensitivity by means of the ▲ and ▼ keys. You can also enter suitable digit (see Table 5). The pet immunity option can be enabled/disabled by using numerical keys and the ▲ and ▼ keys. The pet immunity option can be enabled (the ▣ symbol on the display) or disabled by pressing any numerical key, ▲ or ▼.

In the DloadX program, a two-digit sequence is to be entered. The first digit refers to the sensitivity (see Table 5), and the other – to the pet immunity (0 – option disabled, 1 – option enabled).

Number	Detector sensitivity
1	low
2	medium
3	high

Table 5.

5.2.2 APMD-150 detector configuration

The APMD-150 wireless dual motion detector takes up 1 zone in the system. The following items are remotely programmable:

- infrared path sensitivity – within the range 1 to 4 (1 – minimum; 4 – maximum).
- microwave path sensitivity – within the range 1 to 8 (1 – minimum; 8 – maximum).
- test mode functionality i.e. when the violation is indicated – 0 (motion detected by both sensors), 1 (motion detected by the infrared sensor) or 2 (motion detected by the microwave sensor).

In the LCD keypad, the ◀ and ▶ keys enable navigation between programmable parameters, and the ▲ and ▼ keys allow you to modify them. You can also enter digits.

In the DloadX program, enter 3 digits corresponding to the selected parameters.

For example, entering 4-4-0 means that the sensitivity of IR path is set at 4, the sensitivity of the microwave path is set at 4 too, and, in the test mode, the detector will signal violation (the LED will go on) after motion is registered by both detectors.

5.2.3 AMD-100 and AMD-101 detectors configuration

The AMD-100 wireless magnetic detector with an additional zone takes up 1 zone in the system, and the AMD-101 wireless magnetic detector with an additional independent zone – 2 zones (the first: magnetic detector, the second: the additional input of the detector). For detectors with the electronics version 3.5 D or newer, you should select the active reed switch. In the LCD keypad you can do it by means of the ▲ and ▼ keys. In the DlaodX program, enter the digit 0 (the lower reed switch) or 1 (the side reed switch).

5.2.4 AMD-102 detector configuration

The AMD-102 magnetic detector with input for roller shutter detector takes up 2 zones in the system (the first: magnetic detector, the second: additional input of the detector). You should select an active reed switch for the magnetic detector and program operating parameters for the input for roller shutter detector:

- number of pulses – within the 1 to 8 range. Registering the preset number of pulses will result in zone violation.
- pulse validity time – 30, 120 or 240 seconds or unlimited time (--- on keypad display). The time countdown runs from registering the pulse. Before the time expires, next pulses must be registered in sufficient number for the zone to be violated.

Note: *The pulse counter is reset after expiry of the pulse validity time and after arming the partition to which the zone belongs.*

In the LCD keypad, in order to define which of the two reed switches is to be active, select the first one of the two zones to which the detector is assigned (see description of the CONFIGURATION function). Use the ▲ and ▼ keys to select the reed switch. In order to configure operating parameters of the input for roller shutter detector, select the second one of the two zones to which the detector is assigned. The ◀ and ▶ keys allow you to navigate between the parameters, and the ▲ and▼ keys to modify them.

In the DLOADX program, in order to define which of the two reed switches is to be active, click in the "Configuration" column on the first of the two detector-related fields and enter the value 0 (the lower reed switch) or 1 (the side reed switch). In order to configure operating parameters of the input for roller shutter detector, click in the "Configuration" column on the second of the two detector-related fields and enter 2 digits corresponding to the selected parameters:

1 digit – number of pulses: from 1 to 8;

2 digit – pulse validity time: 0 (30 s), 1 (120 s), 2 (240 s) or 3 (unlimited time).

For example, if you enter the value 4-2, the zone will be violated after 4 pulses have been registered, 240 seconds being the maximum time that can elapse between the first and the last pulse.

5.2.5 AGD-100 detector configuration

The AGD-100 wireless glass break detector takes up 1 zone in the system. Sensitivity of the high-frequency channel is to be programmed for the detectors. The programming is done in the same way as in case of programming sensitivity of the APD-100 detectors.

5.2.6 AVD-100 detector configuration

The AVD-100 wireless vibration and magnetic detector takes up 2 zones in the system (the first: magnetic detector, the second: vibration detector). You should select the active reed switch for the magnetic detector and program the operating parameters of the vibration detector:

- sensitivity – within the range 1 to 8. Registering a single vibration which meets the sensitivity criteria will result in violation of the detector.
- number of pulses – within the range 0 to 7. Registering a predetermined number of vibrations within 30 seconds will result in violation of the detector. All vibrations are taken into consideration (they do not have to meet the sensitivity criteria). Pulses are not counted up for the value 0.

Note: *Parameters are being independently analyzed. As a result, the detector can signal violation after registering a strong single vibration, caused by a powerful impact, as well as after a few slight vibrations, caused by a series of weak strikes.*

In the LCD keypad, in order to determine which of the two reed switches is to be active, you should select the first of the two zones to which the detector is assigned (see description of the CONFIGURATION function). You can select the reed switch by using the ▲ and ▶ keys. In order to configure the operating parameters of the vibration detector, select the second zone of the two to which the detector is assigned. The ◀ and ▶ keys enable movement between the parameters being programmed, and the ▲ and ▼ keys allow you to modify the parameters. You can also enter the suitable digits at once.

In the DLOADX program, in order to determine which of the two reed switches is to be active, you should click in the "Configuration" column the first of the two fields corresponding to the detectors and enter the value 0 (the lower reed switch) or 1 (the side reed switch). In order to configure the operating parameters of the vibration detector, click in the "Configuration" column and enter 2 digits corresponding to the selected parameters. For example, entering the value 4-6 means that the sensitivity has been set at 4, and the number of pulses at 6.

5.2.7 ASD-100 detector configuration

The ASD-100 wireless smoke and heat detector takes up 1 zone in the system. The following items are remotely programmed for the detectors:

- working mode of heat sensor – you can disable the sensor or select the detection class (A1, A2 or B), in conformity with the EN 54-5 standard.
- buzzer functionality – you can disable the buzzer or select one of the three types of audible signaling.
- time of alarm signaling by the buzzer/LED – the following values can be programmed: 1, 3, 6 or 9 minutes.

In LCD keypad the ◀ and ▶ keys make it possible to navigate between the parameters to be programmed, and the ▲ and ▼ keys allow you to modify the parameters. You can also enter numerical values. The · symbol denotes that the heat sensor or buzzer is disabled.

In the DLOADX program, you should enter 3 digits corresponding to the selected parameters in accordance with Table 6. For example, entering the value 0-2-4 means that the heat sensor is disabled, type 2 audible signaling has been chosen, and duration of the buzzer/LED signaling will be 9 minutes.

1st digit		**2nd digit**		**3rd digit**	
digit	heat sensor	digit	audible signaling	digit	signaling duration
0	disabled	0	none	1	1 minute
1	A1	1	sound type 1	2	3 minutes
2	A2	2	sound type 2	3	6 minutes
3	B	3	sound type 3	4	9 minutes

Table 6.

5.2.8 ARD-100 detector configuration

The ARD-100 wireless reorientation detector takes up 1 zone in the system. Sensitivity should be programmed for the detector within the 1 to 16 range (1 – minimum; 16 – maximum).

In the LCD keypad, you can change the programmed sensitivity by using the ▲ and ▼ keys. You can also enter the numerical value at once. In the DLOADX program, enter a suitable number in the "Configuration" column.

5.3 Wireless sirens

⚠ **It is not recommended that reversed polarity be programmed for the alarm security system outputs to which wireless sirens are assigned, since signaling in such a case will be triggered for the inactive output, while activation of the output will stop the signaling.**

The wireless sirens send to the control panel information on power related troubles (low battery, loss of 12 V power supply) and on tampers. The tamper messages are sent immediately, while the trouble messages – during the polling period. The information is sent to the zones to which the sirens are assigned. The system zones to which the wireless sirens are assigned can be programmed as:

- NC, NO or EOL – the zone will only inform about power supply troubles;
- 2EOL/NC or 2EOL/NO – the zone will only inform about power supply troubles and tampers.

Note: *After starting the SERVICE MODE or TEST MODE as well as for 40 seconds after turning power on, the signaling in the siren is blocked. This enables carrying out installation operations. Opening the tamper contact will not trigger loud signaling, but information on the tamper will be sent (when in service mode, the control panel does not signal tamper alarms). The command to block/unblock signaling in connection with entering/quitting the test mode or service mode is sent during the polling period.*

5.3.1 ASP-105 siren configuration

The ASP-105 outdoor wireless siren takes up 2 outputs and 2 zones in the system. Information on low battery is transmitted to the first zone occupied by the siren, and information on loss of external 12 V DC power – to the second zone. Information on tampers is transmitted to both zones.

Two parameters are to be configured for the siren: the type of the audible signaling (there are 4 types available) and its maximum duration (1, 3, 6 or 9 minutes). The visual signaling is enabled throughout the cut-off time of control panel output.

In the LCD keypad, the ◀ and ▶ keys enable navigation between the programmable parameters, and the ▲ and ▼ keys allow you to modify them. You can also enter numerical values.

In the DLOADX program, enter a two-digit sequence as shown in Table 7.

1st digit		**2nd digit**	
digit	audible signaling	digit	signaling duration
1	sound type 1	1	1 minute
2	sound type 2	2	3 minutes
3	sound type 3	3	6 minutes
4	sound type 1	4	9 minutes

Table 7.

5.3.2 ASP-205 siren configuration

The ASP-205 external wireless siren takes up 2 outputs and 2 zones in the system. Information on low battery and tampers is transmitted to both zones.

Note: *A command to trigger the signaling is only send to the siren during the response time. Hence the cutoff time of the control panel outputs which control the ASP-205 wireless indoor siren must be longer than the response time. It is recommended that this time correspond to the signaling duration, as programmed in the siren.*

The siren makes it possible to configure two different, independently triggered ways of signaling. For each way of signaling you can:

- define maximum duration of signaling;
- select one of the three audible signals or disable the acoustic signaling;
- enable/disable the optical signaling.

Such a flexible solution allows the installer to determine whether there should be independently triggered optical and acoustic signaling in the siren, or various alarms (e.g. burglary and fire) should be signaled in a different way.

In LCD keypad, having started the Configuration function, you should configure both zones to which the siren is assigned, i.e. the two signaling methods. After selection of the zone, the ◀ and ▶ keys enable movement between the parameters being programmed:

– Operation manner of the acoustic signaling: it can be disabled (the · symbol is shown on the display) or one of the three types of acoustic signaling can be selected. Use the ▲ and ▼ keys to modify the parameters (you can also enter a digit from the 0 to 3 range).

– Maximum signaling duration: 1, 3, 6 or 9 minutes. Use the ▲ and ▼ keys to modify the parameters (you can also enter a suitable digit).

– Operation manner of the optical signaling: it can be disabled (the · symbol is shown on the display) or enabled (the ▯ symbol shown on the display). In order to modify the parameters, use any numerical key.

In the DloadX program, configuration of signaling parameters consists in entering 3 digits, as shown in Table 8. For example, entering the 4-3-1 value means that the signaling duration will be 9 minutes, sound type 3 has been selected and the optical signaling has been enabled.

1st digit		**2nd digit**		**3rd digit**	
digit	signaling duration	digit	acoustic signaling	digit	optical signaling
1	1 minute	0	none	0	disabled
2	3 minutes	1	sound type 1	1	enabled
3	6 minutes	2	sound type 2	-	-
4	9 minutes	3	sound type 3	-	-

Table 8.

Violation of the siren tamper contact will generate tamper alarm, which will last 3 minutes (sound type 1 and optical signaling).

5.4 230 V AC wireless controllers

The ASW-100 E or ASW-100 F 230V AC wireless controller takes up 1 output and 1 zone in the system. One of the three operating modes should be selected for the controller (shown in square brackets is description of the mode in LCD keypad):

– mode 0 [button: inactive] – the electric circuit is only remotely controlled;

– mode 1 [button: interim control] – the electric circuit can be controlled remotely or manually;

– mode 2 [button: combined control] – the electric circuit can be controlled remotely or manually, but remote control can be manually overridden.

To select the operating mode in the LCD keypad, use the ▲ and ▼ keys. In the DloadX program enter 0 for mode 0, 1 for mode 1 or 2 for mode 2. The new settings are sent to the controller during the response time (see: Response period).

Activation of the output to which the controller is assigned will result in energizing the 230 V electric circuit (in case of programming reversed polarity of the output, the circuit will be deenergized).

Depending on the operating mode, information on the button status (mode 0) or on the electric circuit (mode 1 and mode 2) is supplied to the control panel zone to which the controller is assigned). Information on the button status is sent in real time. Information on the electric circuit status is sent during response time Pressing the button/making the electric circuit will activate the zone to which the controller is assigned.

For the ASW-100 E or ASW-100 F controller, carefully select the FILTER value, i.e. the number of response periods with no response, after which loss of communication with the ASW-100 controller will be reported. The 230 V sockets are installed at low position, hence the ASW-100 controllers mounted in them are exposed to the risk of being covered by personnel moving around the premises.

6. System options

If the name of option in LCD keypad has been abbreviated, the short name is shown in square brackets next to the full name.

6.1 Telephone options

Reporting - TELEPHONE [Mon. TELEPHONE] – with this option enabled, the control panel can send event codes to the monitoring station by means of the telephone line.

Reporting – GPRS [Mon.GPRS] – with this option enabled, the control panel can send event codes to the monitoring station, using GPRS technology. The GPRS reporting can be performed by the INTEGRA 128-WRL control panel or any other control panel, after connecting the GSM/GPRS module. The GSM/GPRS module must be connected to the RS-232 port of the control panel (operation as an external modem). The GPRS technology enables sending events in all formats, except for the TELIM format.

Reporting – ETHM (TCP/IP) [Mon. ETHM-1] – if the ETHM-1 module is connected to the control panel and this option is enabled, the control panel will be able to send event codes to the monitoring station via the Ethernet network, using the TCP/IP protocols. The Ethernet network enables sending events in all formats, except for the TELIM format.

SMS reporting [Mon. SMS] – with this option enabled, the control panel can send event codes to the monitoring station in the form of SMS messages. This option is only available in the INTEGRA 128-WRL control panel.

Telephone messaging [Tel. messaging] – with this option enabled, the control panel can notify about the occurrence of specific events by means of voice messages or text messages using the telephone links.

Answering – modem [Modem answer.] – with this option enabled, external initiation of the communication between modem and control panel is possible.

Answering – audio [Voice answer.] – with this option enabled, the control panel will carry out the function of call answering, i.e. the users who have a telephone code will be able to obtain by phone information on the status (armed/disarmed, alarms) of partitions to which they have access.

Remote control – with this option enabled, the control panel allows the users having a telephone code to operate the REMOTE SWITCH type of outputs by using a phone. The option is available if the ANSWERING – AUDIO is enabled.

External modem – with this option enabled, the control panel will support an external modem connected to the control panel RS-232 port.

Modem ISDN/GSM/ETHM [ISDN/GSM modem] – enable this option where the GSM, ISDN or ETHM-1 module is connected as the external modem. The option is available if the EXTERNAL MODEM option has been enabled.

Tone dialing – with this option enabled, the control panel will tone dial the telephone numbers (pulse dial, if this option is disabled).

Ground Start – with this option enabled, the control panel will use the Ground Start method to obtain signal on the telephone line (by grounding temporarily the telephone line wires). Enable this option, if required by your phone service provider.

No dial tone test [No dialton.tst] – with this option enabled, the control panel will not perform the test for dial tone before dialing the number and will start dialing the number 5 seconds after going "off hook". This makes it possible for the control panel to dial the number when some non-standard tones occur on the telephone line after going off hook (e.g. interrupted tone). When this option is disabled, the control panel will start dialing the number 3 seconds after going off hook, provided that the dial tone is present.

No answer tone test [No answer test] – with this option enabled, in case of notifying by means of voice messages, the control panel will not perform the test for "off hook" condition. The voice message will be played back 15 seconds after completion of the number dialing. In case of reporting, the control panel will ignore any signals (including the busy tone) received from the telephone exchange after dialing the telephone number, and will wait for the handshake from the monitoring station. Enable this option if, after dialing the number, non-standard signals are received from the telephone exchange or in case of very poor quality connections.

Double voice message [Dbl. voice msg.] – with this option enabled, the voice message is played back twice during telephone messaging.

Double call – with this option enabled, the control panel must be called twice for the modem communication to be established. The first time you must wait for the preprogrammed number of rings and hang up. Then you must call back within three minutes and the control panel will answer the call immediately. This solution makes it possible to connect after the control panel some additional devices which will be activated after a preset number of rings (e.g. answering machine, fax, etc.).

Pulse 1/1.5 (off 1/2) – this option applies to dialing the telephone numbers by using the pulse mode. Before you enable it, make yourself familiar with the valid standard of pulse dialing.

6.2 Printer options

Printing – the option enables on-line events printout by the printer connected to the RS-232 port of control panel mainboard.

6.2.1 Printout options

Include reporting status [Monitor.status] – with this option enabled, on the printout will appear the information if the particular event was sent to the monitoring station (printout of the event information will take place not immediately but after transmission to the station has been completed).

Print names / descriptions [Names/descript] – determines if, besides the numbers of zones, outputs, modules and users, also their names and descriptions are to be printed.

Wide paper – printout width will be 132 columns (if the option is disabled: 80 columns).

2400 bps (off:1200 bps) – data will be sent to RS-232 port at a rate of 2400 bps (if the option is disabled - at a rate of 1200 bps).

CR+LF (off: CR) – parameter determining the control mode of paper feed in the printer.

Use parity bit – the parity check of data transferred from the control panel to the printer is enabled.

Parity EVEN (off: ODD) – option determines the mode of parity check of data transferred from the control panel to the printer. The option is relevant only if the USE PARITY BIT option is active.

Notes:

- *The other parameters of RS-232 transmission are permanently programmed: 8 data bits and 1 stop bit.*
- *All the parameters regarding transmission through RS-232 (i.e. transmission rate, CR+LF, parity, data bits and stop bits) are to be set identically on the control panel and on the connected printer - otherwise the printer will not operate at all, or the printout will be illegible.*

6.2.2 Printout contents

The options define what kind of information will be contained in the printout.

6.3 Other options

Permitted "simple" access codes [Simple codes] – with this option enabled, the users can use access codes containing less than three different digits (e.g. 1111 or 1212) or contain consecutive digits (3456).

Notify of necessity to change access code [Notify of code] – with this option enabled, the LCD keypad will notify the user of the necessity to change access code (e.g. if the code is a newly created one, or if other users, when changing their code, happen to “hit” the code of the user in question).

Confirm commands with "1" [Confirm with 1] – with this option enabled, the LCD keypad will require for some functions that commands be additionally confirmed by using the [1] key.

Clear messaging on alarm clearing [Autoabort msg.] – clearing the alarm can automatically cancel messaging about this alarm, if the user clearing the alarm has the TELEPHONE MESSAGING CANCELING right.

Return to menu from Service Mode [SM -> menu] – quitting the service mode can result in return to the user menu, instead of to the basic mode of keypad operation.

Return to menu from menu "Test" [Tests -> menu] – ending the TEST function can result in return to the user menu, instead of to the basic mode of keypad operation.

Fast module bus communication [Fast exp. bus] – it is recommended to enable this option to speed up communication with the modules. The option should only be disabled in case of extended security alarm systems, where electric interference may cause problems with communication.

No module restart reports [No rest. mon.] – when this option is enabled and the Contact ID or SIA format is used for reporting, no event codes referring to module restarts will be sent to the monitoring station.

Service message after tamper alarm [Inf.aft.tamper] – after any tamper alarm, the keypads can display on LCD display the message informing that service maintenance is necessary. The message will be cleared after entering the service code and confirming it with the [#] key.

Backlight off on AC loss [No AC-no blght] – the backlighting in keypads can be automatically switched off in case of 230 V AC power loss.

Block keypad after 3 wrong codes [Blk aft.w.code] – with this option enabled, after entering an invalid code / reading in an invalid card three times, the keypad / reader will be blocked for 90 seconds. After this period of time has expired, each subsequent entry of an invalid code / read-in of an invalid card will block the keypad / reader at once. The counter of invalid codes / cards will be reset after a correct code is used.

Trouble memory until review [Troubl. memory] – the trouble memory can be signaled until it will be cleared (erasing the trouble memory is possible when exiting the function of viewing troubles in the keypad or in the “Troubles” window).

Do not show alarm if armed [Hide alarms] – with this option enabled, no alarms will be indicated in keypads during the armed mode.

Limit events [Events limit.] – with this option enabled, while armed events from the same source will be saved into the event log and reported to the monitoring station 3 times only.

Alarming zones review [View clear.al.] – with this option enabled, you can view the zones that triggered the alarm in the LCD keypad immediately after alarm clearing.

6.4 Arming options

Warn while arming if trouble [Arm, trb.warn.] – suitable information about troubles, if any, can be displayed during the procedure of arming by means of the LCD keypad, so that the user can review them.

Display violated/bypassed zones on arming [Zones bef. arm] – information about violated/bypassed zones can be displayed during the procedure of arming by means of the LCD keypad, so that the user can review them.

Do not arm if tampered [If tamper] – arming can be impossible if tamper is detected.

Do not arm if battery trouble [If batt. trbl.] – arming can be impossible if there is a battery trouble.

Required system reset after verified alarm [If verif. al.] – arming can be impossible after a verified alarm.

Do not arm if trouble [If other trbl.] – arming can be impossible if there is a trouble.

Do not arm if output battery trouble [If outs. trbl.] – arming can be impossible when the control panel detects overloading of the mainboard outputs or disconnection of devices connected to these outputs.

Do not arm if reporting trouble [If monit.trbl.] – arming can be impossible if there are any problems with reporting.

6.5 Times

Global entry delay – parameter taken into account in the delayed zones, for which the programmed ENTRY DELAY is equal to 0.

Global alarm time – time of signaling alarm in keypads, proximity card arm/disarm devices, proximity card readers and DALLAS chip readers.

No armed indication after [Suppr.arm status after] – time counted from the moment of partition arming, after which the LED indicating armed status in the keypad/partition keypad goes off.

AC loss report delay – time during which the control panel must be without AC power before the trouble is reported. A delay in reporting the trouble prevents sending information about short-time voltage decays, having no effect on normal operation of the system.

Telephone line loss report delay – time during which abnormal voltage must be on the telephone line for the control panel to report the telephone line trouble. A delay in reporting the trouble prevents sending information about short-time voltage dips (e.g. during a phone call) or decays.

6.6 Service options and parameters

In the keypad the options are available in SM SETTINGS submenu.

Disable service mode [Block SM] – with this option enabled, entering the service mode "from pins" (by hardware means) will be impossible (entering the service mode "from pins" will only be possible if the control panel factory settings are restored).

Disable downloading [Block DWNL] – with this option enabled, starting communication with the DLOADX program "from pins" will be impossible.

Hide service mode after [Hide SM after] – you can define the time that must elapse after the last operation performed on the keypad before the service mode is hidden. The control panel will remain in the service mode, but the keypad will exit the service mode. The service mode will continue to be indicated in the keypad by the corresponding LED as well as beeps (provided that the option of service mode acoustic signaling is enabled). Return to the service mode in the keypad will follow after re-entering the service code and selecting the SERVICE MODE in the user menu. If value 0 is programmed, hiding the service mode is disabled.

Service mode beep [SM sounds] – with this option enabled, the service mode will be acoustically signaled in the keypad.

6.7 Other parameters

Rings before answer [Rings to answer] – number of rings after which the control panel will go off hook.

User code min. length [Min. code length] – you can set the minimum required number of digits for the user code. The parameter will be taken into account when creating and editing the codes (but it has no effect on the codes already existing in the system).

Prefix length – you can set the required number of digits for the prefix. Entering a number different from 0 means that from now each code will have to be preceded by a prefix. See also: section PREFIXES.

Note: *Each change of the prefix length restores the factory default prefixes.*

RTC clock correction [Clock adjustm.] – if the accuracy of control panel clock is inadequate, the clock settings may be adjusted once per 24 hours (at midnight) by a defined time. The correction time is programmed in seconds. The maximum correction can be ±19 seconds per 24 hours.

Summer/winter time [Daylight saving] – the control panel can automatically adjust the clock settings due to a change from the summer time to the winter time according to the selected schedule.

Summer time from – if the control panel clock is to be corrected by 1 or 2 hours according to dates, you should enter the dates (day, month) after the clock is changed to the summer time (moved forward).

Winter time from – if the control panel clock is to be corrected by 1 or 2 hours according to dates, you should enter the dates (day, month) after the clock is changed to the winter time (moved back).

Time server – enter in this field the address of a time server with support for NTP protocol, if the control panel is to synchronize the time with the server (automatically and after suitable function is enabled by the installer or master user). Time synchronization is possible for the INTEGRA 128-WRL control panel and any other panel to which the ETHM-1 module is connected.

Time zone – select in this field the time zone, which is a difference between the Greenwich Mean Time (GMT) and the zone time.

PING test – the ETHM-1 modules with firmware version 1.05 can test communications by using the PING command sent to the indicated network device. The ETHM-1 module will be testing communication after the parameters described below are configured and the PING TEST option is enabled in the module itself. In the DLOADX program, you can program the communication test parameters by using the PING command in the "Structure" window, "Hardware" tab, after you click on the keypad bus.

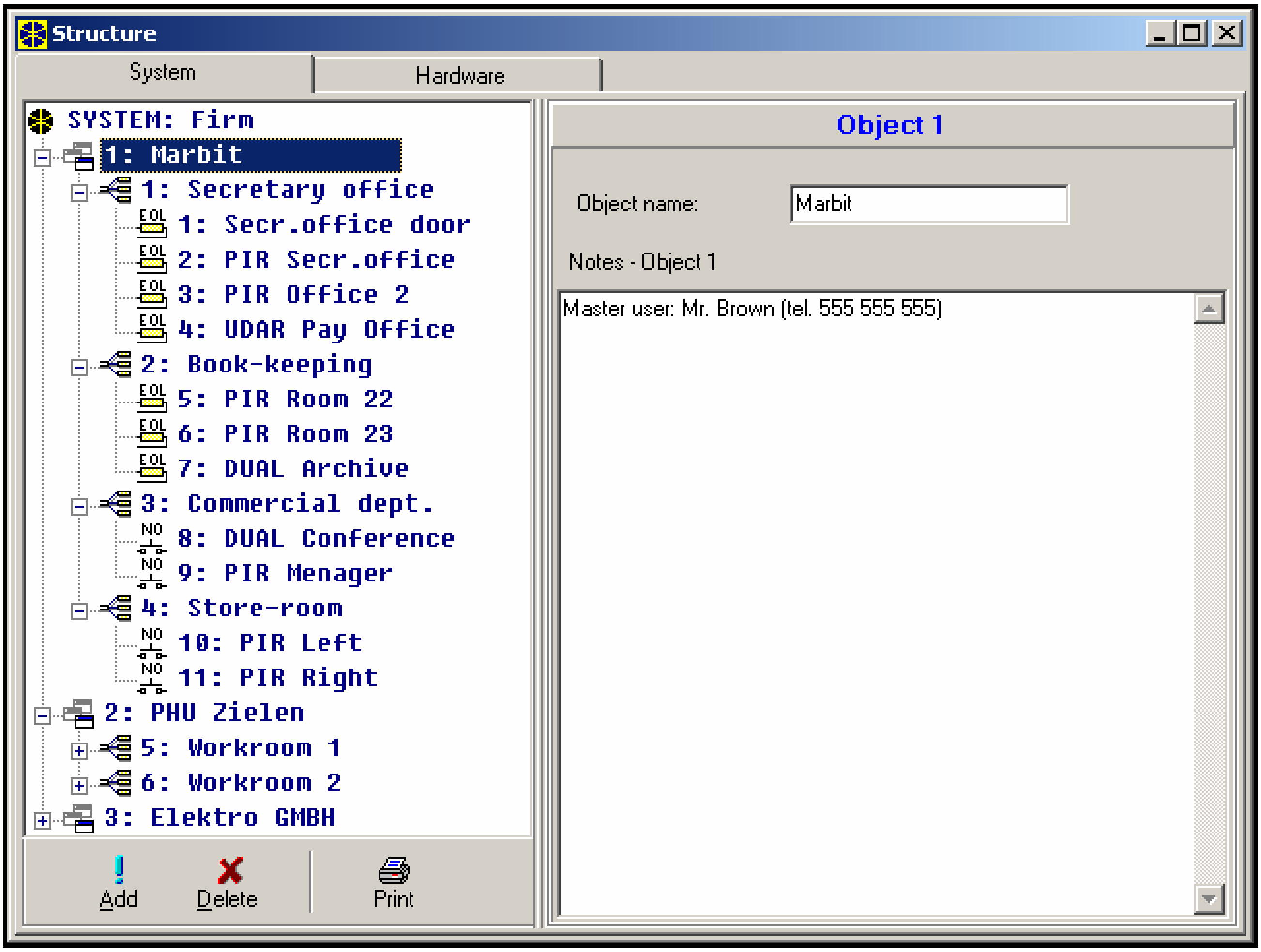
Address to test [PING] – address of the device to which the module is to send the PING command to test communications. It can be entered as an IP address (4 decimal numbers separated by dots) or as a name.

Period [PING period] – the interval between consecutive communication tests by using the PING command. If value 0 is programmed, the communication test will be disabled.

Tries no. before trouble – the number of unsuccessful communication tests (the module has received no answer to the PING command sent) after which trouble will be reported. If value 0 is programmed, the communication test will be disabled.

7. System structure

7.1 Objects



```
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.

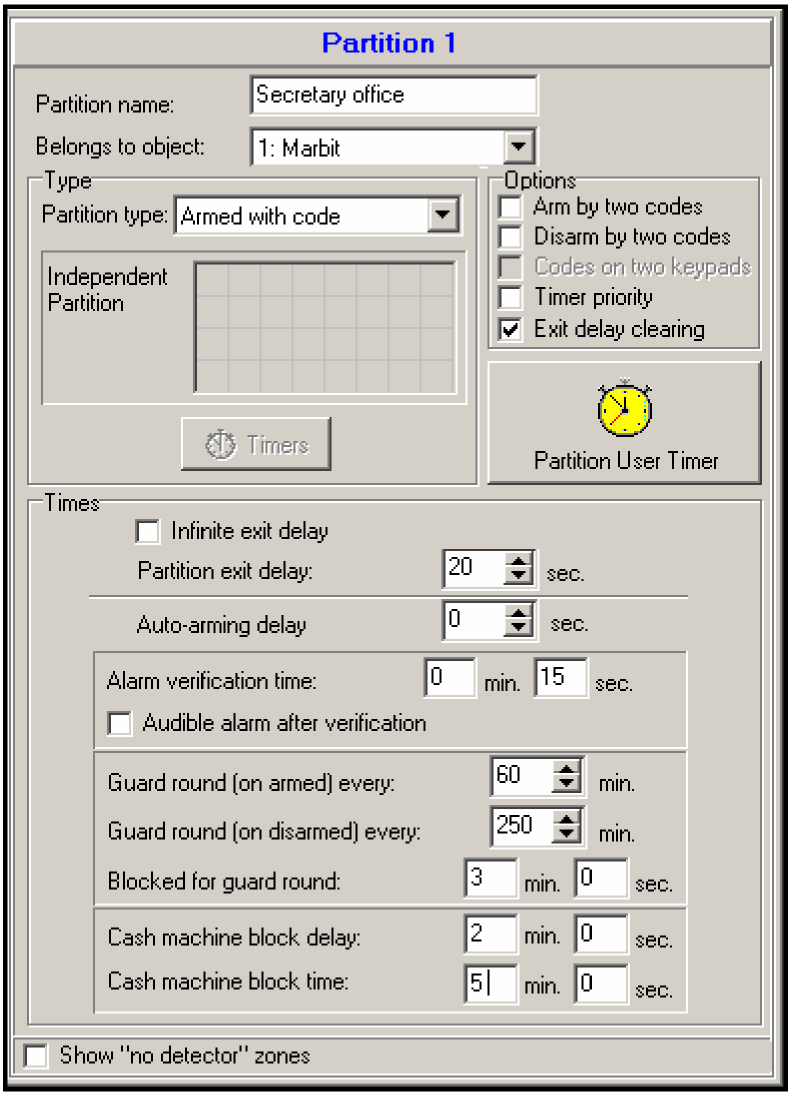
Depending on its size, the INTEGRA control panel makes it possible to create 1, 4 or 8 objects. The objects are created in the service mode by using the EDIT OBJECT function or the DLOADX program. They are recognized as separate alarm systems. It is possible to configure the control panel so that individual 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).

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.

7.2 Partitions



Partition 1

Partition name: Secretary office

Belongs to object: 1: Marbit

Type

Partition type: Armed with code

Independent Partition

Options

☐ Arm by two codes

☐ Disarm by two codes

☐ Codes on two keypads

☐ Timer priority

☑ Exit delay clearing

Times

☐ Infinite exit delay

Partition exit delay: 20 sec.

Auto-arming delay 0 sec.

Alarm verification time: 0 min. 15 sec.

☐ Audible alarm after verification

Guard round (on armed) every: 60 min.

Guard round (on disarmed) every: 250 min.

Blocked for guard round: 3 min. 0 sec.

Cash machine block delay: 2 min. 0 sec.

Cash machine block time: 5 min. 0 sec.

☐ Show "no detector" zones

Fig. 6. Partition settings.

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 Fig. 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.

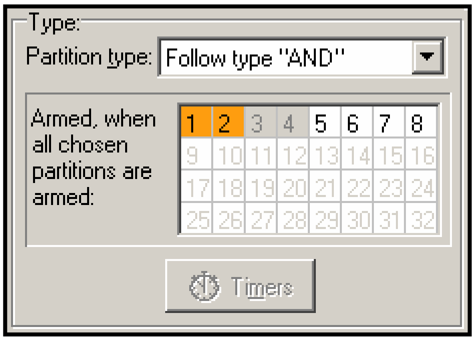
A partition can be created in the service mode with the use of the EDIT OBJECT function, by assigning it to the selected object. When creating a partition, it can be given a **name** (up to 16 characters). Also, the **partition type** should be defined (by default: ARMED WITH CODE). The function also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

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.

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 installer 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. Fig. 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 "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.



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

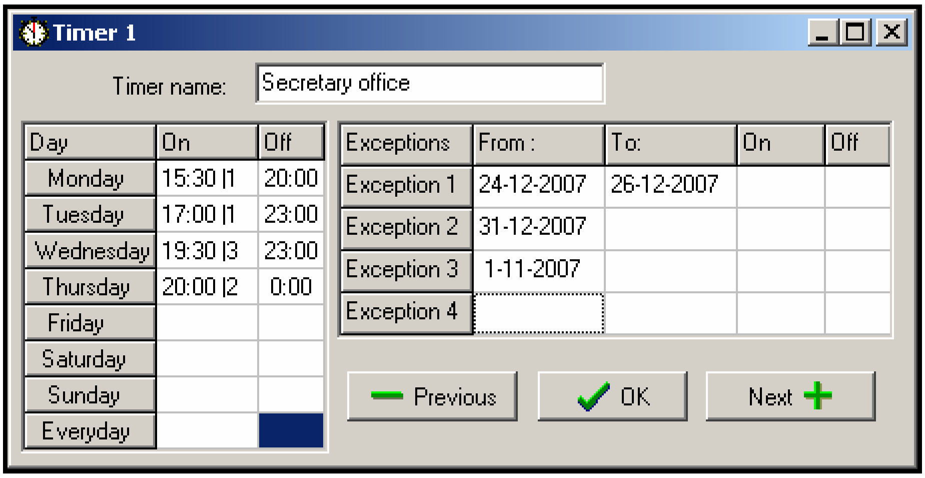
Fig. 7. Definition of FOLLOW TYPE "AND" partition.

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 Fig. 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.*



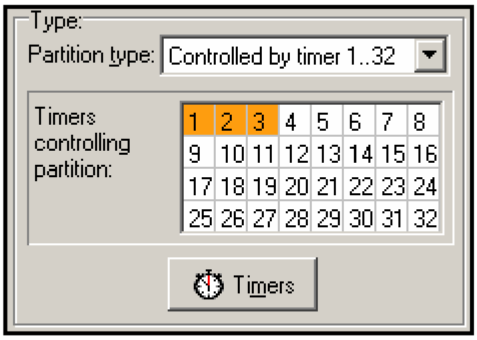
Timer name: Secretary office

Day	On	Off
Monday	15:30 |1	20:00
Tuesday	17:00 |1	23:00
Wednesday	19:30 |3	23:00
Thursday	20:00 |2	0:00
Friday		
Saturday		
Sunday		
Everyday		

Exceptions	From :	To:	On	Off
Exception 1	24-12-2007	26-12-2007		
Exception 2	31-12-2007			
Exception 3	1-11-2007			
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". When defining the timer, specify the type of armed mode to be activated by the timer: 0 – fully armed, 1 - fully armed+bypasses, 2 – armed without interior, 3 – armed without interior and without entry delay. By default, the control panel assumes that each new timer will activate the full armed status (type 0).



Type:

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 „Auto-arm" event is logged. When the partition is disarmed by the timer, the „Auto-disarm" event is logged. The event details include the number of timer which armed / disarmed 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).

Valid within 60 sec – where arming / disarming requires entering two codes, the first of them is valid for 60 seconds (the validity period of the first code cannot be programmed by the user).

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 – the partitions (except for the dependent ones) may be controlled by a separate timer, whose mode of operation is to be programmed by means of the function available in the user menu (→CHANGE OPTIONS →PARTITION TIMERS). In the DLOADX program, the PARTITION USER TIMER is only available when communication with the control panel is in progress. The timer controls the control panel in much the same way as the other timers. When programming the timer, define the type of armed mode to be activated by the timer: 0 – fully armed, 1 – fully armed+bypasses, 2 – armed without interior, 3 - armed without interior and without entry delay. By default, the control panel assumes that each new timer will activate the full armed status (type 0).

Note: *In case of the PARTITION USER TIMER, 0 is indicated as the timer number in the details of „Auto-arm” / „Auto-disarm” event which is logged after the partition is armed / disarmed by the timer.*

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. Delay up to 255 seconds can be programmed. The exit delay time can be reduced in the following cases:

- violation of zones type: 85. ZONES/OUTPUTS – CONDITIONAL, 86. ZONES/OUTPUTS – FINAL or 89. FINISHING EXIT DELAY in the partition;
- entering the [9][#] sequence in the LCD/partition keypad (see the EXIT DELAY CLEARING option).

Infinite exit delay [Infin.ex.time] – if this option is enabled, the partition will be armed after entering the code and then violating the zone type: 85. ENTRY/EXIT – CONDITIONAL, 86. ZONES/OUTPUTS – FINAL or 89. FINISHING EXIT DELAY. If this type of zone has not been violated, or the exit delay time has not been reduced (see the EXIT DELAY CLEARING option), the partition will not be armed.

Arming control time – if the INFINITE EXIT DELAY option is enabled, instead of PARTITION EXIT DELAY you will program the time before expiry of which the partition should be armed. If the partition is not armed, the "Arming failed" event will be saved into the control panel memory.

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 – delay of automatic arming of a partition by timer. 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 function in user 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 disarm the partition, 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 BLOCKING 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).

7.3 Zones

A zone can only be assigned to one partition. The system can support the following zones:

- hardwired – on the control panel electronics board, in keypads and expanders. The number of available hardwired zones is determined by the control panel during identification procedure.

Note: *If the numbers of LCD keypad and expander zones coincide, and the zone use option is enabled in the keypad, the expander zones will not be supported.*

- wireless – the INTEGRA 128-WRL control panel, as well as the control panels to which the ACU-100 controller is connected. The number of available wireless zones depends on the number of wireless devices registered in the system and is determined during the procedure of adding wireless devices.
- virtual – zones which physically do not exist, but have been programmed as FOLLOW OUTPUT or are controlled by means of a key fob.

7.3.1 Numeration of zones in the system

Hardwired and wireless zones are given their numbers automatically:

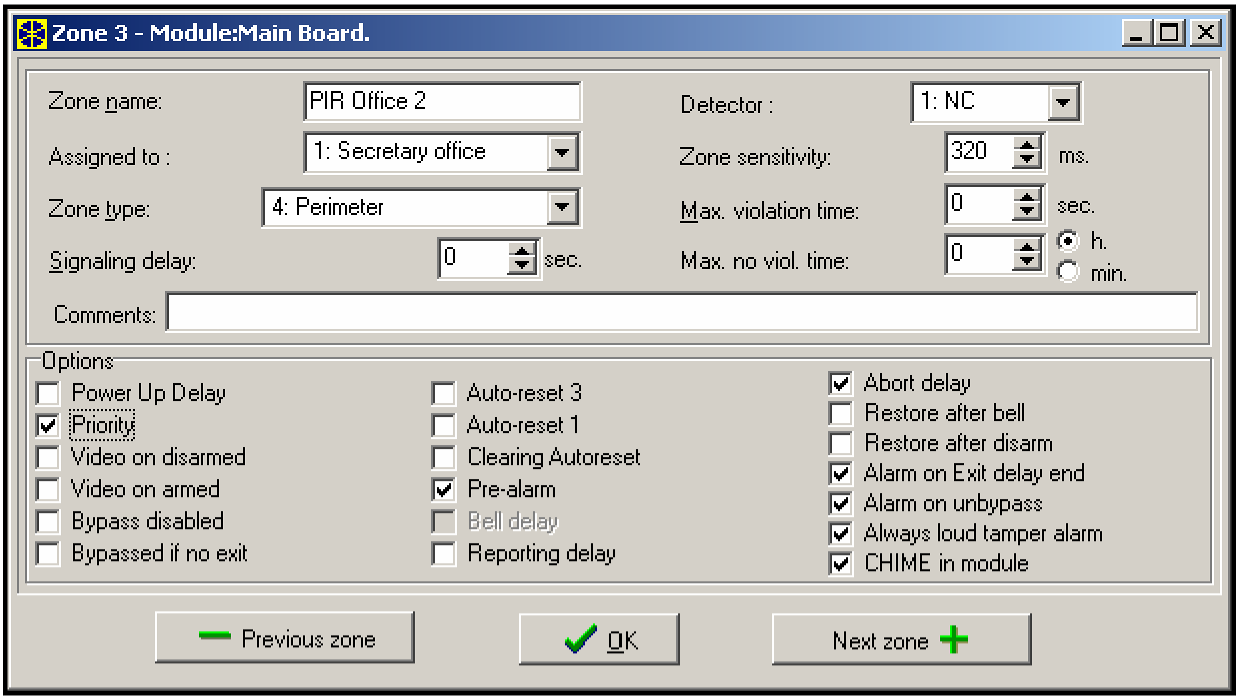
- the numbers of hardwired zones on the control panel electronics board always come first (1-4 for INTEGRA 24 control panel; 1-8 for INTEGRA 32 and INTEGRA 128-WRL control panels; 1-16 for INTEGRA 64 and INTEGRA 128 control panels).
- the numbers of keypad zones are determined during the keypad identification procedure, based on the keypad address and depend on the control panel size (see the installer manual).
- the numbers of zones in expanders and ACU-100 controller are determined during the expander identification procedure. The numeration depends on:
  - control panel size,
  - address set in the expander (the expander zones with a lower address will receive lower numbers than the expander zones with a higher address),
  - number of the bus to which the expander is connected (if the device is connected to the second bus, its address in the system will be determined by adding the number 32 to the address set in it),
  - numbers assigned to the wireless zones supported by the control panel mainboard **only INTEGRA 128-WRL**.

Note: *The control panel reserves 8 zones in the system for each identified expander. Exceptions are the CA-64 ADR expander and the ACU-100 controller, for which up to 48 zones can be reserved. In case of the CA-64 ADR expander, the number of reserved zones depends on the number of detectors with installed CA-64 ADR MOD module which are connected to it. In case of the ACU-100 controller, the number of reserved zones depends on the number of registered wireless devices. In both cases, the number of reserved zones is a multiple of 8.*

- numbers of the wireless zones supported by the mainboard of INTEGRA 128-WRL control panel are set during the procedure of adding wireless devices. Free and available numbers are assigned.

Note: *Numeration of wireless devices supported by the mainboard of INTEGRA 128-WRL control panel need not be continuous. For example, if the system includes 8 wireless zones with numbers 17-24, to which wireless devices are assigned, and the zones 25-32 are already reserved for the expander, then adding a new wireless device will result in reservation of next 8 zones with numbers 33-40 for wireless devices. Numbering of the expander zones will remain unchanged.*

The DLOADX program enables changing the numeration of zones in the system (window STRUCTURE, tab HARDWARE, button ADVANCED for the chosen expander). The changes in numeration will only be valid until the expander identification function is launched again.



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.

7.3.2 Parameters

Zone name – individual name of the zone (up to 16 characters).

Partition – partition to which the zone belongs. The zone can only belong to one partition.

Zone type (see: *Zone types*)

Entry delay – the parameter refers to the delayed zones. The entry delay time makes it possible to disarm the system before triggering alarm.

Signaling delay – the parameter refers to the 4. PERIMETER, 5. INSTANT and 6. EXIT type zones. Loud alarm signaling can be delayed by a programmed time period.

Alarm delay – the parameter refers to the 5. INSTANT and 6. EXIT. The alarm from zone may be delayed by a programmed time period.

Surveillance time – the parameter refers to the 8. EXTERIOR type zones (zone with alarm verification). Violation of the zone will start the surveillance time running. If another violation occurs during the surveillance time, alarm will be triggered. If value 0 is programmed, the alarm will be generated on the first violation.

Bypass time – the parameter refers to the bypassing zones. It indicates for how long the zones will be bypassed. If value 0 is programmed, the zones will remain bypassed until disarming the partitions to which they belong, or until they are unbypassed by the user.

Module number (lock/keypad) – the parameter refers to the 58: TECHNICAL – DOOR BUTTON type zones. It defines which door will be unlocked after zone violation (you can indicate a door controlled by partition keypad, code lock, proximity card reader expander or DALLAS chip reader expander).

Arming mode – the parameter refers to the 80. ARMING and 82. ARM/DISARM type zones. It defines which type of armed mode will be activated by the zone:

0 – full armed mode;

1 – fully armed and, additionally, the zones for which the BYPASSED IF NO EXIT option is enabled, will be bypassed;

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 (beside the partition the zone belongs to). These types of zones can also only control the partition they belong to (select 0 in the DLOADX program).

Wiring type – type of detector and the method of its connection:

no detector – no detector is connected to the zone;

NC – the zone supports a detector of NC (normally closed) type;

NO – the zone supports a detector of NO (normally open) type;

EOL – the zone supports a NO or NC detector in EOL loop;

2EOL/NO – the zone supports a NO detector in 2EOL loop;

2EOL/NC – the zone supports a NC detector in 2EOL loop;

roller – the zone supports a roller shutter detector (available for the zones on the electronics board of INTEGRA 128-WRL control panel, in INT-KSG keypad, in CA-64 E expander with electronics version 2.1 or later and program version 2.0 or later, and in CA-64 EPS expander with electronics version 2.0 or later and program version 2.0 or later),

vibration – the zone supports a vibration detector (available for the zones on the electronics board of INTEGRA 128-WRL control panel, in INT-KSG keypad, in CA-64 E expander with electronics version 2.1 or later and program version 2.0 or later, and in CA-64 EPS expander with electronics version 2.0 or later and program version 2.0 or later),

follow output – the zone status depends exclusively on the status of selected output (activating the selected output is equivalent to zone violation).

roller 2EOL – the zone supports a roller shutter detector in 2EOL loop (the wiring type available for zones in INT-KSG keypad and on mainboard of INTEGRA 128-WRL control panel with electronics version 2.1 or newer),

vibration 2EOL – the zone supports a vibration detector in 2EOL loop (the wiring type available for zones in INT-KSG keypad and on mainboard of INTEGRA 128-WRL control panel with electronics version 2.1 or newer).

Notes:

- *In case of the VIBRATION zone, opening of the circuit for 200 ms – irrespective of the programmed number of pulses and sensitivity (see below) – will be interpreted as violation. This solution enables magnetic detector to be connected in series with vibration detector.*
- *Physical violations and tampers, as well as key fob control, have no effect on status of the zone programmed as FOLLOW OUTPUT.*

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).

Pulses count – the number of pulses after which the zone will be violated. The parameter refers to the ROLLER and VIBRATION zones. For the VIBRATION zone, it is possible to program values from 0 to 7 (pulses with 0 value will not be counted – only the SENSITIVITY [MS] parameter will be included). For the ROLLER zone, it is possible to program values from 1 to 8.

Pulses duration – parameter programmed for the ROLLER zone. It defines within what time after the pulse occurrence next pulses should follow (in the number defined as the PULSES COUNT), so that the zone is violated. You can program the following values: 30 s, 120 s, 240 s and 0. If no further pulses occur within the defined time period, the pulse counter will be reset. The pulse counter is automatically reset during arming / disarming. Programming the 0 value means that the counter will only be reset during arming / disarming.

Sensitivity [ms] – parameter programmed for the VIBRATION zone. Occurrence of a pulse the duration of which is equal to or higher than the time defined will result in violation of the zone. You can program values from the 3 ms to 96 ms range (every 3 ms).

Note: *In the DLOADX program, all the required parameters for zones in ROLLER and VIBRATION zones are programmed in the SENSITIVITY field.*

Output – the number of the output whose activation will result in zone violation. The selected output does not have to be physically connected to the zone. Both the zone and the output can be virtual ones. In case of the physically existing zones, all physical violations and tampers are disregarded. The parameter is available for the FOLLOW OUTPUT zone.

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 failure. 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.

7.3.3 End of line resistors

The value of resistors used in EOL and 2EOL loops is programmable within the range from 500 Ω to 15 kΩ for the zones on the INTEGRA 128-WRL control panel mainboard, in INT-SG keypads and in the zone expanders identified by the control panel as CA-64 Ei and CA-64 EPSi:

- on the INTEGRA 128-WRL control panel mainboard, in INT-KSG keypads and in the zone expanders with firmware version 4.00 – the value of R1 and R2 resistors is programmed individually for the 2EOL zone (see Fig. 11). The resistor value for the EOL wiring is a sum of values programmed as R1 and R2.

Notes:

- *The sum of values programmed for the R1 and R2 resistors may not be lower than 500 Ω or higher than 15 kΩ.*

- *It is possible to program value 0 for the R2 resistor. This means that two resistors should be used in the 2EOL loop, each with resistance equal to half the value defined for the R1 resistor.*

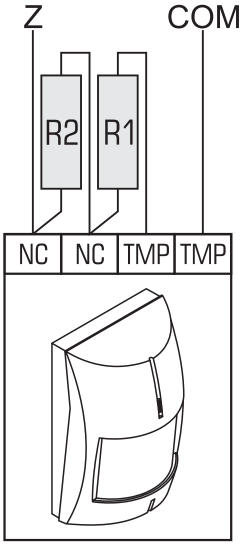


Fig. 11. Double EOL resistors.

- in the zone expanders with firmware version 2.00 or 2.01, the resistor value should be programmed for the EOL wiring. For the 2EOL wiring, the value of a single resistor is equal to half the defined value.

In the DLOADX program, you should enter the value of resistors in the "Structure" window, "Hardware" tab, after indicating the mainboard, selected zone expander or INT-KSG keypad in the list.

In the keypad, program the resistor value as follows:

– for the INTEGRA 128-WRL control panel mainboard – use the EOL R1 RESISTOR and EOL R2 RESISTOR functions (SERVICE MODE →STRUCTURE →HARDWARE →EOL R1 RESISTOR / →EOL R2 RESISTOR);

– for zone expanders with firmware version 4.00 – use the EOL R1 RESISTOR and EOL R2 RESISTOR functions (SERVICE MODE →STRUCTURE →HARDWARE →EXPANDERS →SETTINGS →[expander name] →EOL R1 RESISTOR / →EOL R2 RESISTOR);

– for zone expanders with firmware version 2.00 or 2.01 – use the EOL RP RESISTOR function (SERVICE MODE →STRUCTURE →HARDWARE →EXPANDERS →SETTINGS →[expander name] →EOL RP RESISTOR).

Note: *The keypad does not enable programming the resistor values for INT-KSG keypad zones.*

7.3.4 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 violated zones for which the PRIORITY option has not been activated. To do so, select VIOLATED/BYPASSED ZONES PREVIEW WHEN ARMING (→TS →OPTIONS →VARIOUS OPTIONS →ZONES BEF. ARM).*

Violation control – option for 82: ARM/DISARM zone type. If this option is enabled, violation of the zone will arm/disarm the partition (depending on the current status of the partition). If the option is disabled, violation of the zone 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).

No alarm sign. in keypad – option for 13: PANIC-SILENT zone type. If the option is enabled, silent panic alarm from this zone will not be signaled on keypads. Clearing this alarm by means of keypad will not be possible.

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 means of the user functions available in the ZONE BYPASSES submenu.

Bypassed if no exit – the zone will be automatically bypassed, if during the exit delay countdown no exit from the partition has been recorded (the exit zone has not been violated). The zone will also be bypassed if the "full + bypasses" armed mode is active (in such a case, recording an exit from the partition is of no significance). The zone will be unbypassed on partition disarming.

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).

Alarming – option available for the 91. DETECTOR MASK zone type. If enabled, violation of the zone will additionally trigger an alarm.

Auto-reset 3 – the zone can trigger up to 3 alarms. As long as the alarm is not cleared or the partition is not armed/disarmed, violations of the zone will not trigger any alarm.

Auto-reset 1 – the zone can trigger only 1 alarm. As long as the alarm is not cleared or the partition is not armed/disarmed, violations of the zone will not trigger any alarm.

Clearing Autoreset – alarm counters for the zones for which the AUTO-RESET 3 or AUTO-RESET 1 option is enabled can be automatically reset at midnight (violations of these zones will be able to trigger alarms again).

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 restore code will be reported to the central monitoring station only after the alarm signaling is ended.

Restore after disarm – the zone restore code will be reported to the central monitoring station only after disarming the partition to which the zone belongs.

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).

Store to event log – option for the 47: No alarm action and 63: Trouble zone types. Violation of the zone will result in storing an event according to the zone type (in case of the 47: No alarm action zone type, the information to be written depends additionally on the No reporting option).

No reporting – an option for the 47: No alarm action zone type with the Store to event log option enabled:

- enabled – violation of the zone will only write an event informing about zone violation;
- disabled – violation of the zone will result in writing an event informing about keybox opening, the code of which is sent to the monitoring station.

No restore event – an option for the 47: No alarm action zone type with Store to event log and No reporting options enabled. The zone restore is not stored into the event log.

Store event only if armed – option for the 47: No alarm action zone type. It is available, if the Store to event log option is enabled. Violations of the zone will be written into the event log, provided that the partition to which the zone is assigned, is armed.

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 during the exit delay countdown an exit from the partition is recorded).

Abort voice messaging – option for the 81-83 zone types. 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 enabled, tamper alarm is always loud (if option is disabled – tamper alarm is loud only when armed).

Reporting delay – an option for the 4–7 and 64–79 zone types. 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 9. DAY Alarm, 12. Silent alarm and 116. Internal Siren output types). 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 0–2 and 85–86 delayed zone types. Violation of the zone will block verification of alarms in the partition (similarly as violation of the 90. Disabling verification zone type).

Check arm possibility – an option for the arming zones (type 80 and 82). The zone will not arm, 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 delay 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 delay shortening zone (type 89). The end of zone violation will disable verification of alarms in the partition (similarly as violation of the 90. DISABLING VERIFICATION zone type).

Disabled in arm state – an option for the 91. DETECTOR MASK zone type. If the option is enabled and the zone is violated when armed, the information on detector trouble (masking) will not be stored into the event log (the event code will not be sent to the monitoring station).

7.3.5 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 delay may be signaled on keypads;

exit – the zone status is monitored during partition exit delay. Violation of the zone means exit from the partition.

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, or the user has entered the access code / read in the card on the entry keypad (INT-ENT – see the INT-SCR-BL multifunctional keypad manual).

4. PERIMETER – instantly armed zone, allowing no exit delay.

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 5. INSTANT zone.

8. EXTERIOR – a zone with alarm verification: violation of the zone will start counting the surveillance time – 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 – 24 h 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 12. 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 12. SILENT ALARM type outputs. The zone names and the codes of events from those zones are compatible with the Contact ID reporting protocol.

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 reported 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 zones (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.). Additional options (STORE TO EVENT LOG, NO REPORTING and STORE EVENT ONLY IF ARMED) enable the zone to be used for other applications e.g. supervising the keybox.

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

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 – violation of the zone will result in opening the door controlled by means of partition keypad, code lock, expander of proximity card readers or expander of DALLAS chip readers.

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. TROUBLE – violation of the zone results in the control panel signaling trouble.

64–79 BYPASSING – GROUP: 1–16 – violation of this type of zone can bypass a group of zones. The bypass operating mode should be defined for a group of zones:

- BYPASS ONLY – the zones belonging to the group will be bypassed for a defined time (BYPASS TIME). If 0 value is entered, the zones will be one-time bypassed (until disarming the partitions to which they belong or unbypassing by means of the INHIBIT user function).
- BYPASS ON/OFF – the zones belonging to the group will remain bypassed as long as the bypassing zone is violated (they can also be unbypassed by using the INHIBIT user function).

80. ARMING – violation of the zone will arm the partition to which the zone belongs. Additionally, you can select a group of partitions which will also be armed.

81. DISARMING – violation of the zone will disarm the partition to which the zone belongs. Additionally, you can select a group of partitions which will also be disarmed.

82. ARM/DISARM – the zone controls the arming status of the partition it belongs to. The control mode depends on the CONTROL BY PULSE option. 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 – similarly as the 0. ENTRY/EXIT type 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 – similarly as the 0. ENTRY/EXIT type, but after arming and detecting the restoration of this zone, the control panel ends the exit delay countdown and enters the armed mode.

87. EXIT – FINAL – as 6. EXIT type, but after arming and detecting the restoration 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.

91. DETECTOR MASK – the permanently armed zone, dedicated to antimasking control. Violation of the zone will be treated by the control panel as detector trouble (masking).

7.3.6 Zone testing

The LCD keypad makes it possible to test individual zones of the security system (→SERVICE MODE →ZONES →TEST). Information on violation or tamper of the zone is displayed and signaled by beeps in keypad (violation – 5 short beeps; tamper – 1 long beep). Additionally, the function allows selection of a system output which will be used for signaling during the test (violation of the output will activate the output for 0.5 second, tamper – for 2 seconds).

Notes:

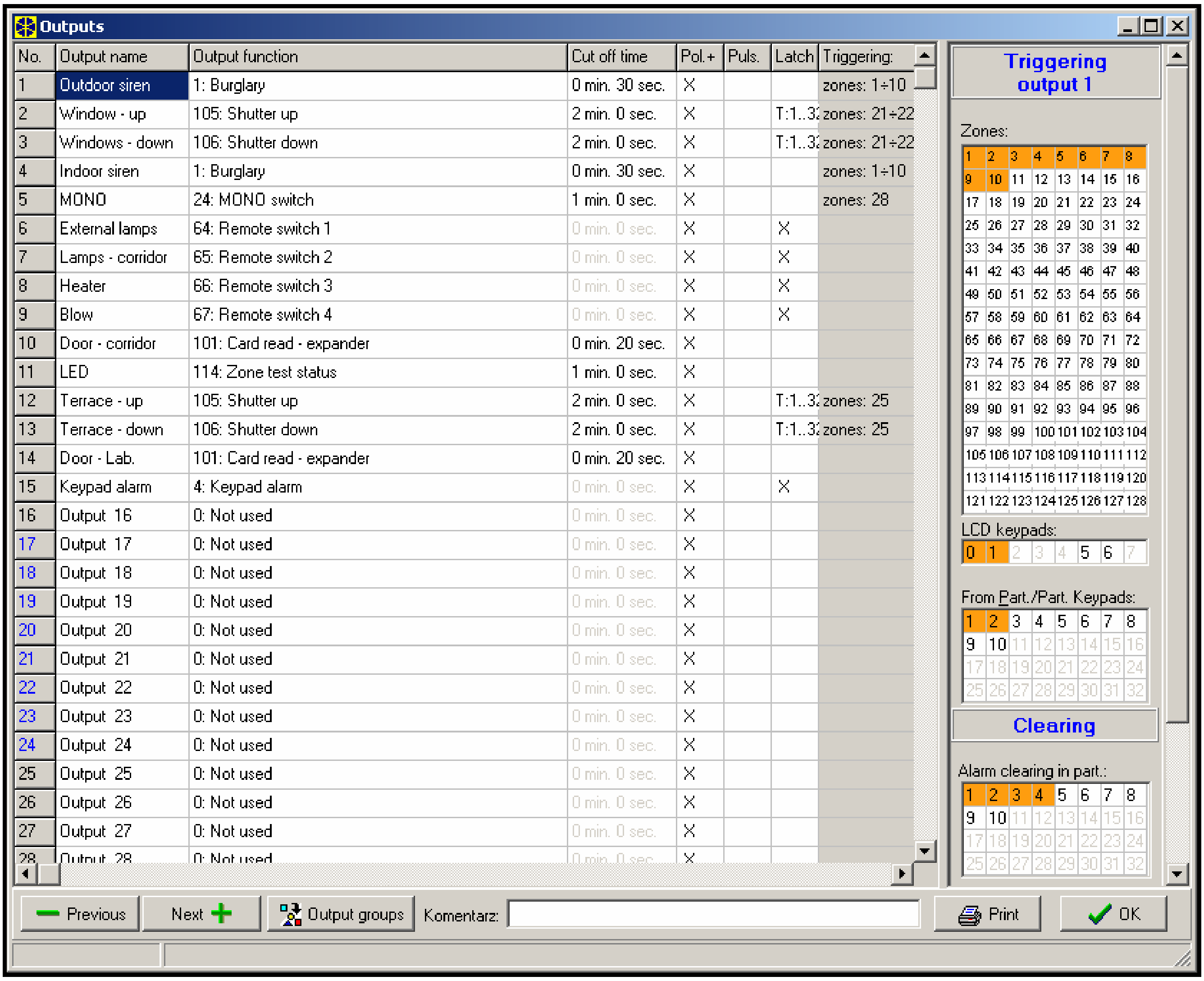
- *Violation/tamper of the zone during the test will not trigger the response programmed for the control panel zone.*
- *The output used for signaling is only remembered until exiting the TEST function. When the TEST function is re-started, the output must be selected again.*
- *Select a zone for testing from the list and press the [#] or ▶ key. The output allocated for signaling will stop doing its present duty (if it was active, it will be disabled) until the zone test is completed (the [*] key pressed).*
- *If wireless sirens are used in the system and any output is selected for signaling, after selecting a zone for testing from the list and pressing the [#] or ▶ key, in the wireless sirens the signaling will be unblock (which is normally blocked for the service mode duration).*
- *If the output selected for signaling controls the wireless siren, it should be borne in mind that the command to block/unblock signaling is sent out during polling. This results in a delay whose duration depends on the programmed response period. Also in case of the ASP-205 siren signaling is only triggered during the polling period.*

7.4 Outputs

The following types of outputs can be used in the system:

- hardwired – on the control panel electronics board and in expanders. The number of available hardwired outputs is determined by the control panel during identification procedure. The hardwired outputs are provided with LEDs indicating their current status.
- wireless – the INTEGRA 128-WRL control panel and the panels to which the ACU-100 controller is connected. The number of available hardwired outputs depends on the number of wireless devices registered in the system and is determined during the procedure of adding wireless devices.
- virtual – the outputs which do not exist physically, but can be used e.g. for execution of logical functions.

Numeration of the outputs in the system is determined according to the same rules as numeration of the zones.



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			

Fig. 12. Details of output settings.

7.4.1 Parameters

Output name – individual name of the output (up to 16 characters).

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

Cut off time – time during which the output is active. The parameter is irrelevant for the status indicating outputs.

7.4.2 Options

Polarity – defines the output operating mode; selecting the option means (see Table 9):

	high-current output	
	option enabled (normal polarity)	option disabled (reversed polarity)
active status	+12V voltage supply	+12V voltage cut-off
inactive status	+12V voltage cut-off	+12V voltage supply
	low-current output	
	option enabled (normal polarity)	option disabled (reversed polarity)
active status	shorted to ground	isolated from ground
inactive status	isolated from ground	shorted to ground

Table 9. Functioning of outputs, depending on the POLARITY option

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.

Active during violation – the option applies to the 24. MONO SWITCH output types. If enabled, the output is always active when a control zone is violated, and the countdown of output cut-off time will only be running after the violation ends.

7.4.3 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 – the zones, which will activate the output (depending on the type of output, they can be activated by violation / bypassing / tamper / alarm from zone, etc.).

Triggering from LCD keypads – the keypads which in a specific situation will activate the output (depending on the type of output, they can be activated by: triggering alarm from keypad, keypad tamper or reading the card into keypad).

Triggering from partitions/partition keypads – the partitions or partition keypads from which the output can be activated. Depending on the output type, it can be activated by: arming / disarming the partition, triggering alarm in the partition, or tamper in the partition keypad, temporary blocking of the partition, etc. (see description of the output types).

Triggering from control timers – the timers which will activate the output (additional option enables a group of timers to be selected).

Triggering by administrators / users – depending on its type, the output will be activated after:

- entering or using a code by one of the selected administrators / users,
- presenting / holding up the card/Dallas chip by one of the selected administrators / users,
- receiving transmission with information on low battery from a key fob belonging to one of the selected administrators / users.

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

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

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

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

Triggering by voice messages – the messages which will activate the output.

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

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

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

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

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

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

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

Triggering by telephone usage type – the cases of using the control panel telephone line (connections initialized by or with the control panel) which will activate the output.

7.4.4 Clearance availability

Alarm clearing – 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: *The alarm must be signaled in the partition where it is to be cleared. If no alarm is being signaled by the given partition, it will be impossible to clear it.*

7.4.5 Output disabling

Disabling timers – the output will not be activated within the timer preset time (additional option enables selection of a group of timers).

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).

7.4.6 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 loud 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 13. PANIC-SILENT type zones,
- alarms of call for medical help from 14. MEDICAL - BUTTON and 15. MEDICAL - REMOTE CONTROL type zones,
- alarms from 7. DAY/NIGHT type zones, if the partition to which the zone belongs is disarmed,
- alarms from 8. EXTERIOR type zones, 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 4. PERIMETER type zones, if the SIGNALING DELAY has been programmed for them,
- alarm from 5. INSTANT and 6. EXIT type zones, 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 8. EXTERIOR type zones 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** – the output is active when at least one of the selected zones is 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 partition (1 pulse – arming, 2 pulses – disarming, 4 pulses – clearing alarm/disarming with alarm clearing. The pulse duration is approx. 0.3 seconds).
24. **MONO SWITCH** – the output controlled by means of the MONO SWITCH type codes (using the code in partition), zones or timers. The CUTOFF TIME set for output will be running after the MONO SWITCH type code is used in the selected partition or after violating a zone (see also the ACTIVE DURING VIOLATION option). If controlled by the timer, the output will be active as long as the timer is active.
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 the telephone line use in the following cases (you can select the cases which will activate the output):
1 – reporting to station 1, main telephone number
2 – reporting to station 1, backup telephone number
3 – reporting to station 2, main telephone number
4 – reporting to station 2, backup telephone number
5 – messaging
6 – downloading
7 – telephone answering

36. **GROUND START** – the output generates a control pulse necessary for work with some types of telephone exchange.

37. **REPORTING 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 10. 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 control outputs with normal polarity are active and all the control outputs with reversed polarity are inactive (because of the POLARITY option, the output can be used for logical negation).

47. LOGICAL OR – output is activated when any control output with normal polarity is active or any control output with reversed polarity is inactive (because of the POLARITY option, the output can be used for 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 AC LOSS REPORT DELAY (OPTIONS →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 AC LOSS REPORT DELAY 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% 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. TCP/IP REPORTING TROUBLE – the output signals trouble of reporting effected by means of TCP/IP network. You should define which of the troubles below are to be signaled:

- no communication between ETHM-1 module and monitoring station 1
- no communication between ETHM-1 module and monitoring station 2
- no GPRS communication with monitoring station 1
- no GPRS communication with monitoring station 2
- no communication with time server
- GSM module initialization error
- trouble of TCP/IP reporting to monitoring station 1
- trouble of TCP/IP reporting to monitoring station 2

96. TELEPHONE LINE TROUBLE – informs about telephone communication troubles. Determine which of the following troubles are to be signaled:

- no voltage on tel. line
- wrong dial tone
- no dial tone

– Central Station 1 trouble
– Central Station 2 trouble

Note: *In case of the INTEGRA 128-WRL control panel, the name of the output type 96 is GSM TROUBLE. The output can inform of the following troubles:*

- *Central Station 1 trouble,*
- *Central Station 2 trouble,*
- *GSM 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. 17). 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 selected zones.

103. LINK TROUBLE – WIRELESS OUTPUT – the output signals lack of communication with wireless devices assigned to the selected 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 outputs.*
- *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.*
- *Selecting the partition for SHUTTER UP and SHUTTER DOWN type of outputs is necessary to make the roller shutter control function available (see description of the OUTPUT CONTROL*

function in the USER MANUAL) in the keypad serving this partition. If the output is not to be controlled by the partition disarming / arming, the SHUTTER NOT CONTROLLED BY ARMING option should be enabled for the output.

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 – the control panel does not respond to violation of the interior zones (zone type 3. INTERIOR DELAYED). The exterior zones (zone type 8. EXTERIOR) will trigger silent alarm. The other zones work normally.

3 – armed without interior and without entry delay – the control panel will react in the same way as above, but, additionally, the delayed zones (zone type: 0. ENTRY/EXIT, 1. ENTRY, 2. DELAYED WITH DELAY SIGNALING) will work as instant ones.

116. INTERNAL SIREN – the output activates in the same situations as the 1. BURGLARY ALARM or 9. DAY ALARM output types (logic product of the 1. BURGLARY ALARM and 9. DAY ALARM output types).

117. TAMPERING STATUS – the output informs about tamper of selected zones, keypads and expanders. It is active as long as the tamper lasts.

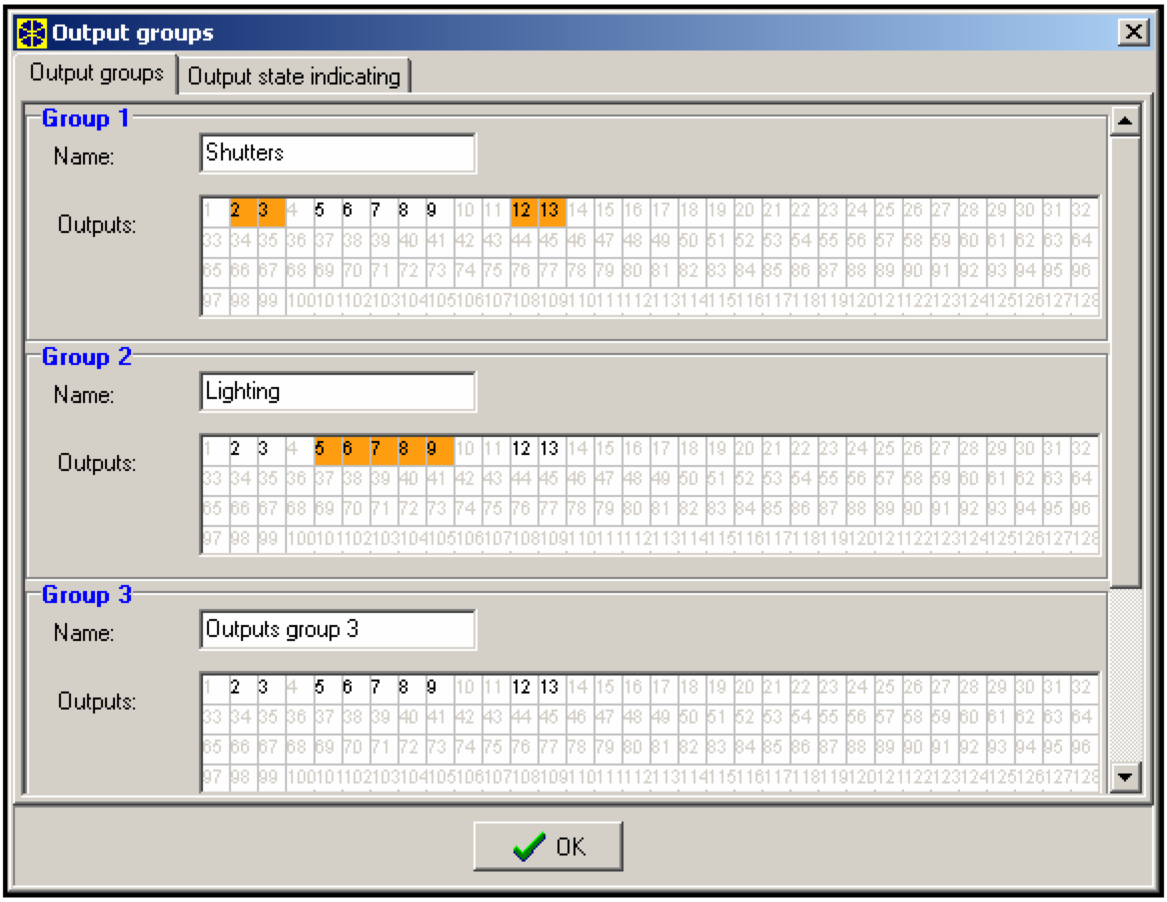
118. KEYFOB BATTERY LOW – the output provides information about low battery in key fobs belonging to selected users. This applies to the key fobs supported by ABAX system or INT-RX module.

119. WIRELESS SYSTEM JAMMING – the output provides information about jamming the selected ACU-100 controllers or the wireless system of INTEGRA 128-WRL control panel mainboard.

7.4.7 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.*



Group 1

Name: Shutters

Outputs:

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

Group 2

Name: Lighting

Outputs:

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

Group 3

Name: Outputs group 3

Outputs:

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

Fig. 13. Window for assignment of outputs to output groups.

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.

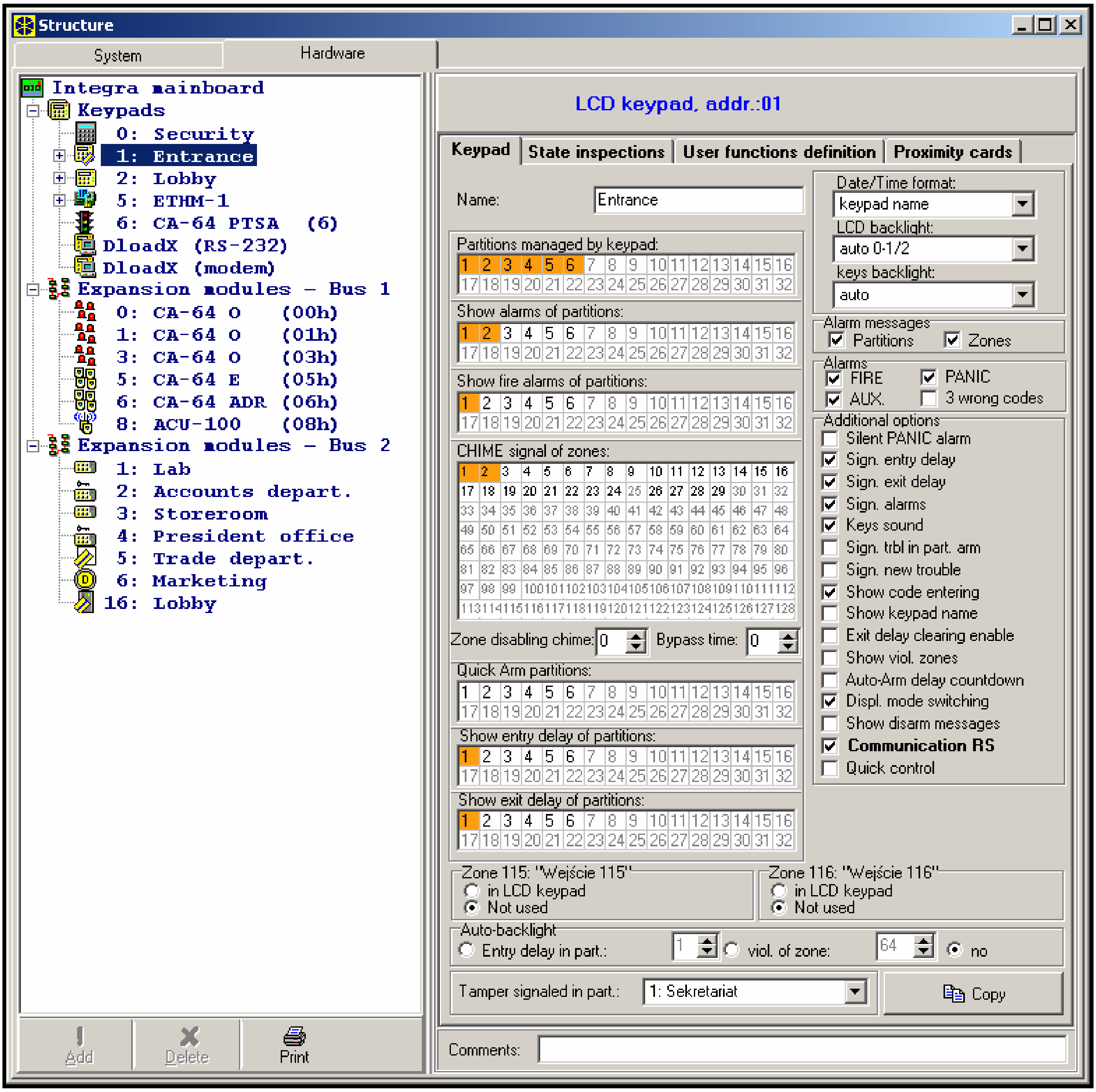
7.4.8 Output testing

The LCD keypad enables testing of individual outputs of the security system (→SERVICE MODE →OUTPUTS →TEST). After starting the function, the list of system outputs will be displayed. Find the output to be tested and press the [#] or ► key. The keypad will display a submenu which enables the output testing. By using the [#] or ► key, you can activate/deactivate the output. You can also deactivate the output by means of the numerical keys. Press [∗] to quit the submenu and return to the list of system outputs.

Notes:

- *The output under test will stop performing its previous function (if it was active, it will be deactivated).*
- *If there are wireless sirens in the system, starting the function of output testing will unblock the signaling in them (the signaling is normally blocked for the service mode duration). It should be remembered that the command to block/unblock the signaling is sent out during polling. This will cause a delay whose duration depends on the programmed response period.*
- *When testing the control output for ASP-205 wireless siren, it should be remembered that the signaling is only triggered during the polling.*

8. LCD keypad



Integra mainboard
Keypads
0: Security
1: Entrance
2: Lobby
5: ETHM-1
6: CA-64 PTSA (6)
DloadX (RS-232)
DloadX (modem)
Expansion modules – Bus 1
0: CA-64 O (00h)
1: CA-64 O (01h)
3: CA-64 O (03h)
5: CA-64 E (05h)
6: CA-64 ADR (06h)
8: ACU-100 (08h)
Expansion modules – Bus 2
1: Lab
2: Accounts depart.
3: Storeroom
4: President office
5: Trade depart.
6: Marketing
16: Lobby

LCD keypad, addr.:01

Keypad | State inspections | User functions definition | Proximity cards

Name: Entrance

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 … 128

Zone disabling chime: 0 Bypass 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: keypad name
LCD backlight: auto 0-1/2
keys backlight: auto

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**
□ Quick control

Zone 115: "Wejście 115" ○ in LCD keypad ● Not used

Zone 116: "Wejście 116" ○ in LCD keypad ● Not used

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

Tamper signaled in part.: 1: Sekretariat

Copy

Comments:

Fig. 14. LCD keypad parameters and options in DLOADX program.

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.

Note: *Using the service code you can operate all partitions, irrespective of which partitions are operated by the keypad.*

Show alarms of partitions – the partitions, the alarm from which will be indicated on the keypad by 🔔 [ALARM] LED, sound, or a text message.

Show fire alarms of partitions – the partitions, the fire alarm from which will be indicated on the keypad by 🔔 [ALARM] LED, sound, or a text message.

CHIME signal – list of zones, violation of which generates audible keypad alarm.

Zone disabling CHIME – number of zone, which, if violated, will disable the CHIME feature for specified time.

Bypass time – time during which the CHIME signal will be disabled after violation of the zone which disables the signaling. If the value 0 is programmed, the signaling will not be disabled.

Quick Arm – partitions which will be armed after pressing [0][#], [1][#], [2][#] or [3][#] on the keypad (see section SYSTEM ARMED MODE in the USER MANUAL).

Show entry delay of partitions – the partitions, for which counting the entry delay will be indicated by text appearing on the LCD display.

Show exit delay of partitions – the partitions for which counting the exit delay will be indicated by text appearing on the LCD display.

Keypad zones – each LCD keypad is provided with two zones which can be used in the security system. 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.

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 – pressing and holding down the key with symbol 🔥 for approx. 3 seconds.
- panic – pressing and holding down the key with symbol 🛡 for approx. 3 seconds.
- auxiliary [medical] – pressing and holding down the key with symbol (!) for approx. 3 seconds.
- 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] – the panic alarm triggered from the keypad can be signaled as the silent alarm (without being signaled on the alarm outputs).

Signaling entry delay [Entry time s.] – the keypad can signal acoustically the entry delay countdown.

Signaling exit delay [Exit time sig.] – the keypad can signal acoustically the exit delay countdown.

Signaling alarms [Alarm signal.] – the keypad can signal acoustically the alarms.

Key sounds [Key sounds] – pressing the keypad keys can be confirmed by beeps.

Signaling troubles in partially arm [Trbl.in p.arm.] – the keypad can signal troubles by means of the ⚠ LED, if some of the operated partitions are armed (the troubles are not signaled if all partitions are armed).

Signal new trouble [New trbl. sign.] – the keypad can audibly signal the 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.] – entering the code can be presented on the keypad display by asterisks.

Show keypad name [Name (2nd row)] – the keypad name can be presented in the lower line of the display.

Exit delay clearing enable [Fin. exit time] – the exit delay time in partitions with the EXIT DELAY CLEARING option enabled can be shortened after pressing in turn the [9][#] keys.

Show violated zones [Zone violation] – violating the CHIME signal triggering zone may additionally result in the zone name being displayed.

Auto-Arm delay countdown signaling [Auto-arm delay] – the auto-arm delay countdown in partition can be signaled acoustically.

Signal on wrong card [Unkn.card sig.] – the option is available for keypad with built-in proximity card reader. If enabled, reading in an unknown card will be signaled by two long beeps.

Event after 3 readings [Ev.3 unk.cards] – the option is available for keypad with built-in proximity card reader. If enabled, reading in an unknown card three times will save the event.

Alarm after 3 readings [Al.3 unk.cards] – the option is available, if the EVENT AFTER 3 READINGS option is enabled. If it is, reading in an unknown card three times will trigger an alarm.

Display mode switching [Dspl.mode chg.] – with the option enabled, you can toggle the display between the standby mode and the partition status display mode by using the [9] key.

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 – the option defines whether the computer with GUARDX program can be connected to the keypad RS-232 port. The option is not available for the INT-KSG keypad.

Quick control [control 8#] – the user can run the CONTROL user function by pressing successively the [8][#] keys (with no need for entering the user code).

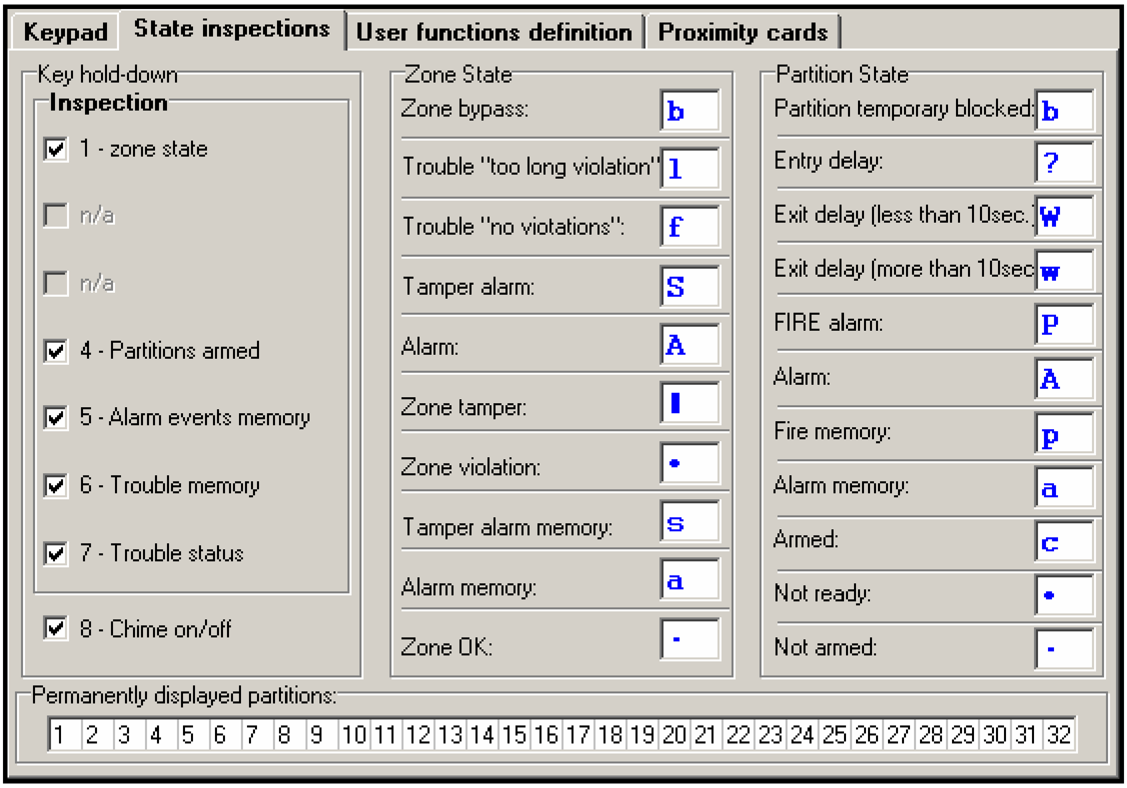
Inspection [Reviews] – you can select which of the functions started by holding the number keys will be available in the keypad.

Permanently displayed partitions [State part.] – you can select the partitions whose state will be permanently presented in the lower line of the display. Up to 16 partitions can be selected. The partitions are displayed successively: for example, if the partitions 3, 6 and 7 are selected, their state will be displayed in the first, second and third position of the display.

Zone state [Zone characters] – you can define the symbols which will illustrate the state of zones.

Partition state [Part. characters] – you can define the symbols which will illustrate the state of partitions.

Code+arrows – you can define which functions will be started on entering the code and pressing the selected arrow key.



Key hold-down

Inspection

- ☑ 1 - zone state
- □ n/a
- □ n/a
- ☑ 4 - Partitions armed
- ☑ 5 - Alarm events memory
- ☑ 6 - Trouble memory
- ☑ 7 - Trouble status
- ☑ 8 - Chime on/off

Zone State

Zone bypass:	b
Trouble "too long violation"	l
Trouble "no viotations":	f
Tamper alarm:	S
Alarm:	A
Zone tamper:	▌
Zone violation:	•
Tamper alarm memory:	s
Alarm memory:	a
Zone OK:	·

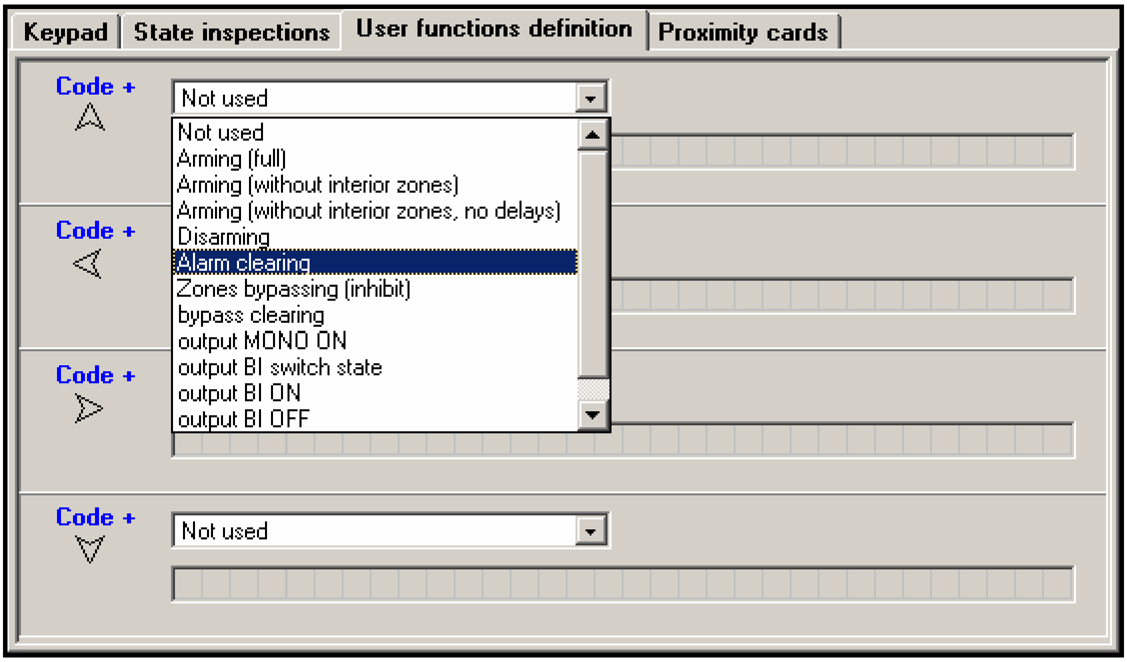
Partition State

Partition temporary blocked:	b
Entry delay:	?
Exit delay (less than 10sec.)	W
Exit delay (more than 10sec	w
FIRE alarm:	P
Alarm:	A
Fire memory:	p
Alarm memory:	a
Armed:	c
Not ready:	•
Not armed:	·

Permanently displayed 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

Fig. 15. Keypad "State inspections" tab in DLOADX program.



Code + ▲: Not used

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

Code + ▼: Not used

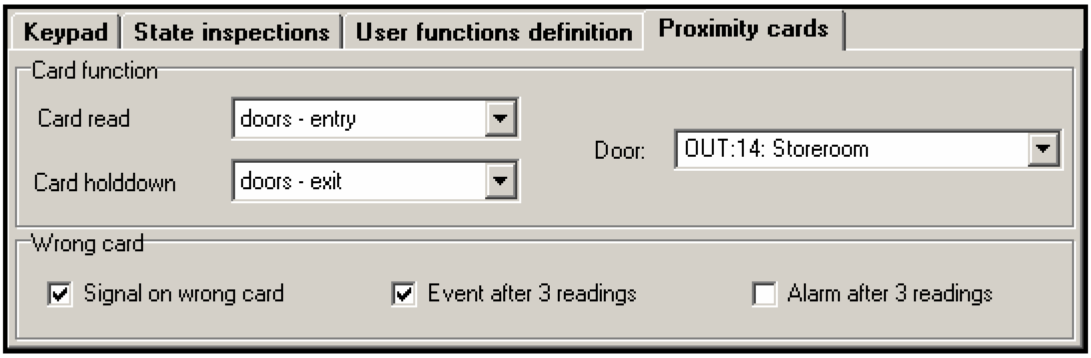
Fig. 16. Programming the functions which are started after you enter the code and press the selected arrow key.

Card function – you can select a function started after presenting or holding the card. If the presenting or holding of the card is to result in opening the door, you can indicate an expander controlled door or the 101: CARD READ - EXPANDER output type of the control panel.

Tamper signaled in partition [Tamper in part.] – selection of the partition in which alarm will be signaled if the keypad tamper contact is opened or the keypad is disconnected from the control panel.

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, INT-KLCDR-BL and INT-KSG. The function is unavailable in the DLOADX program.

Sensitivity – the function makes it possible to control the sensitivity level of built-in proximity card reader in the INT-KLCDR-GR and INT-KLCDR-BL keypads with firmware version 1.06 or newer (1 – the highest sensitivity, 10 – the lowest sensitivity).



Card function

Card read: doors - entry

Card holddown: doors - exit

Door: OUT:14: Storeroom

Wrong card

☑ Signal on wrong card ☑ Event after 3 readings □ Alarm after 3 readings

Fig. 17. Handling proximity cards.

9. 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. The other users' codes are written to the RAM (they will be erased after removal of jumper from the MEMORY pins).

Each user of the system can be assigned 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 or SIA format is enabled). After deletion of the user, the control panel may assign the available number to a new user entered into the system.

9.1 Prefixes

If prefixes preceding the code are to be used in the system, the installer must determine the length of prefixes within the range from 1 to 8 digits, using the PREFIX LENGTH function (SERVICE MODE →OPTIONS →PREFIX LENGTH). It can only be done by using the LCD keypad (the function is not available in the virtual keypads). Setting the prefix length means that from that moment each code in the system must be preceded by a prefix. The installer code need not be preceded by the appropriate prefix: it will be enough when the number of digits preceding the code corresponds to the prefix length.

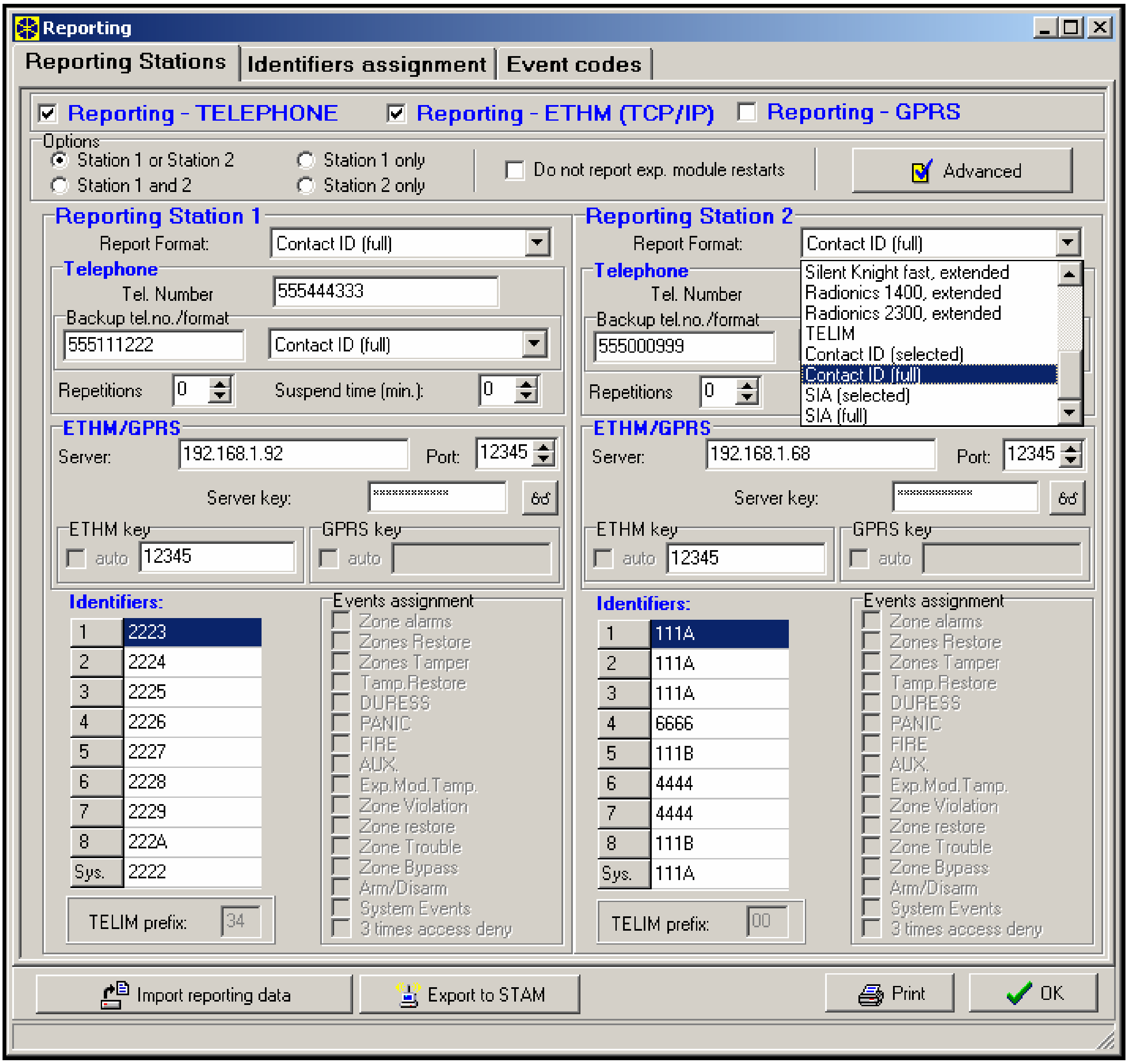
Two kinds of prefixes are used in the system:

– **normal** – for everyday use. By default, it consists of a suitable number of digits 0 (e.g. if the prefix length has been set at 4, the default prefix will be: 0000);

– **DURESS** – used in an emergency situation, when the user is forced to enter the code. If used, a silent alarm will be triggered. By default, the DURESS prefix consists of a suitable number of digits 4 (e.g. if the prefix length has been set at 3, the default prefix will be: 444).

The prefixes and their validity can be programmed by the administrator (master), using the CHANGE PREFIX function.

10. Monitoring



Reporting

Reporting Stations | Identifiers assignment | Event codes

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

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

Reporting Station 1
Report Format: Contact ID (full)
Telephone
Tel. Number: 555444333
Backup tel.no./format: 555111222 Contact ID (full)
Repetitions: 0 Suspend time (min.): 0
ETHM/GPRS
Server: 192.168.1.92 Port: 12345
Server key: *************
ETHM key: □ auto 12345
GPRS key: □ auto
Identifiers:

1	2223
2	2224
3	2225
4	2226
5	2227
6	2228
7	2229
8	222A
Sys.	2222

TELIM prefix: 34

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: Contact ID (full)
Silent Knight fast, extended
Radionics 1400, extended
Radionics 2300, extended
TELIM
Contact ID (selected)
Contact ID (full)
SIA (selected)
SIA (full)
Telephone
Tel. Number
Backup tel.no./format: 555000999
Repetitions: 0
ETHM/GPRS
Server: 192.168.1.68 Port: 12345
Server key: *************
ETHM key: □ auto 12345
GPRS key: □ auto
Identifiers:

1	111A
2	111A
3	111A
4	6666
5	111B
6	4444
7	4444
8	111B
Sys.	111A

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

Import reporting data | Export to STAM | Print | ✓ OK

Fig. 18. Window for format selection and definition of identifiers.

The control panel communicator enables execution of the event monitoring function. The events can be sent to the monitoring station:

- over the Ethernet (TCP/IP) network – if ETHM-1 module is connected,
- using GPRS technology – INTEGRA 128-WRL control panel or if GSM/GPRS module is connected (e.g. GSM-4S or GSM LT-2S),
- as an SMS message – only INTEGRA 128-WRL control panel,
- by telephone (main and reserve telephone number).

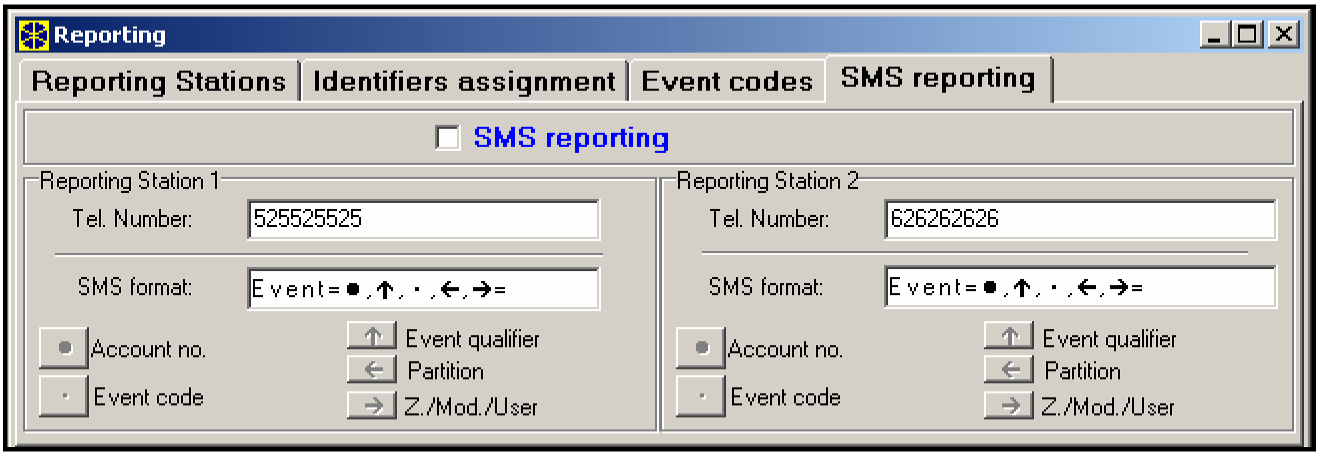
The control panel will make an attempt to send the event, in turn: over the Ethernet (TCP/IP) network, using the GPRS technology, as an SMS message and, finally, by telephone (to main and reserve telephone number). The procedure will be terminated when the event is successfully sent to the monitoring 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.



☐ SMS reporting

Reporting Station 1

Tel. Number: 525525525

SMS format: Event=●,↑,·,←,→=

Reporting Station 2

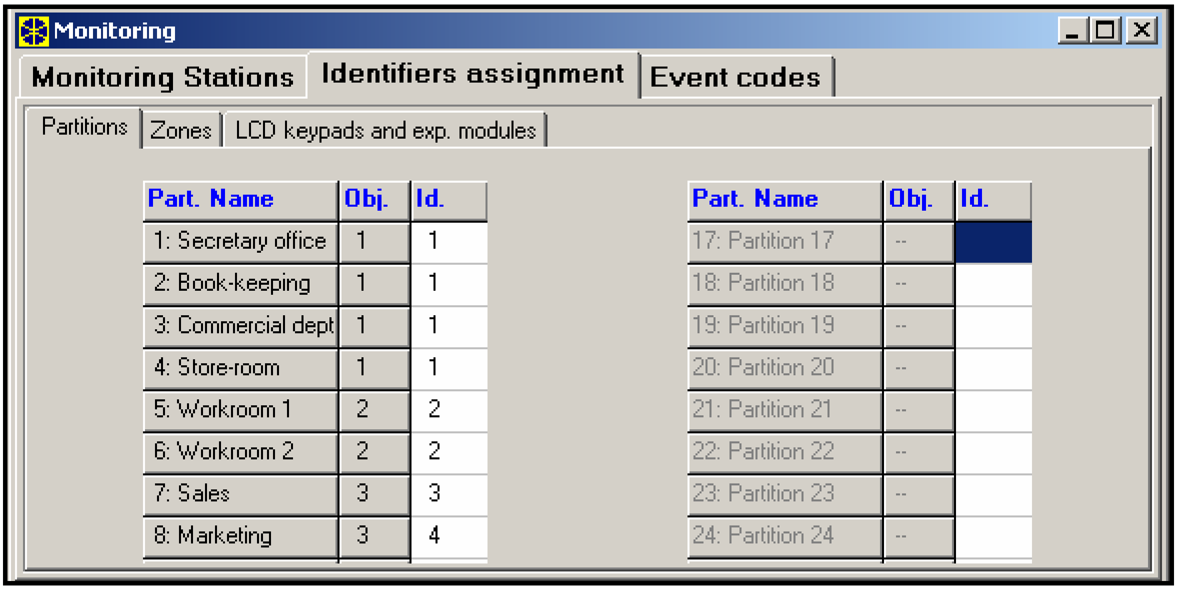
Tel. Number: 626262626

SMS format: Event=●,↑,·,←,→=

Fig. 19. Tab for SMS monitoring settings in the "Reporting" window.

- 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)" or „SIA (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) or „SIA (selected)" 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.
- 6-character identifier can be programmed for the SIA format. For this purpose, enable the 6-CHARACTER IDENTIFIER option (which is available in the monitoring advanced options). The 6-character identifier is composed of 2 parts: 2-character prefix and 4-character identifier.
- The SIA format makes it possible to send to the monitoring station, apart from the event code, also the event source name (zone, user, etc.) and the partition name (this requires programming of suitable settings in the advanced monitoring options).



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. 20. Window for assigning partition events to identifiers.

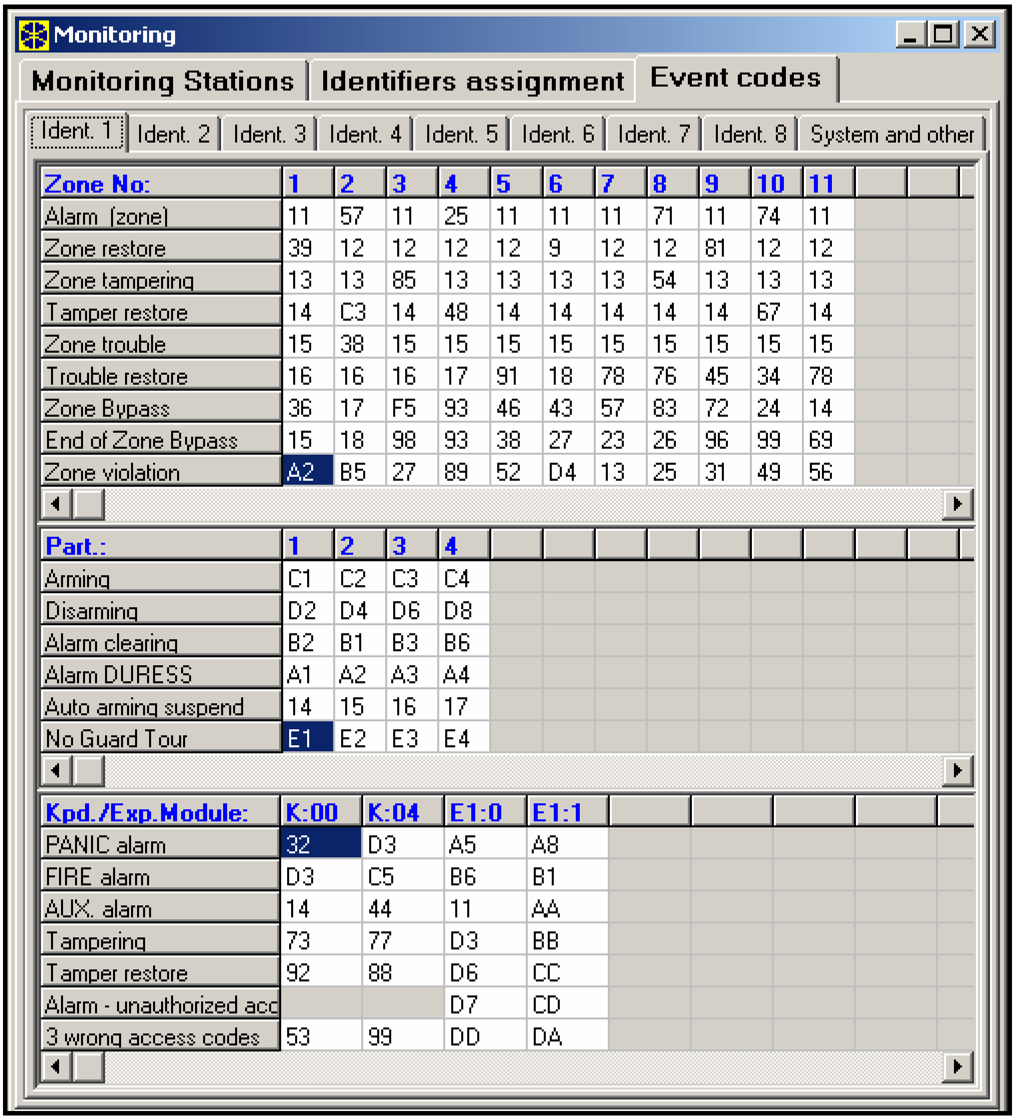
Notes:

- *It is advisable to correctly indicate to how many stations the events are to be reported.*
- *GPRS monitoring can be performed by the INTEGRA 128-WRL control panel and by any other INTEGRA series control panel to which the GSM-4S module (firmware version 4.11 or later) or the GSM LT-2S module (firmware version 2.11 or later) is connected. In that case, the GSM module must be connected to the control panel RS-232 port (used as an external modem). If the module is only connected to the telephone line terminals in control panel (TIP and RING), the GPRS monitoring settings programmed in the control panel will be ignored.*
- *The SMS message format for SMS monitoring (INTEGRA 128-WRL control panel) must be defined as required by the monitoring station. The SMS message format programmed by default in the INTEGRA 128-WRL control panel corresponds to the default settings of the STAM-2 monitoring station (firmware version 1.2.0 or later). The symbols used when programming the SMS format have the following meaning:*

  ● - *account number;*
  ↑ - *event qualifier;*
  · - *event code;*
  ← - *partition;*
  → - *zone/module/user.*

For formats other than Contact ID, only account number and event code are sent. Question marks will be sent instead of the other information.

- *When the „Contact ID (selected)" or „SIA (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 or SIA 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)" or „SIA (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* S*TATION* 1 *OR* S*TATION* 2 *operating mode (as well as for the* S*TATION* N *ONLY, with both numbers entered), do not select the „Contact ID (full)" or „SIA (full)" format for one number, and different formats for the other numbers.*



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

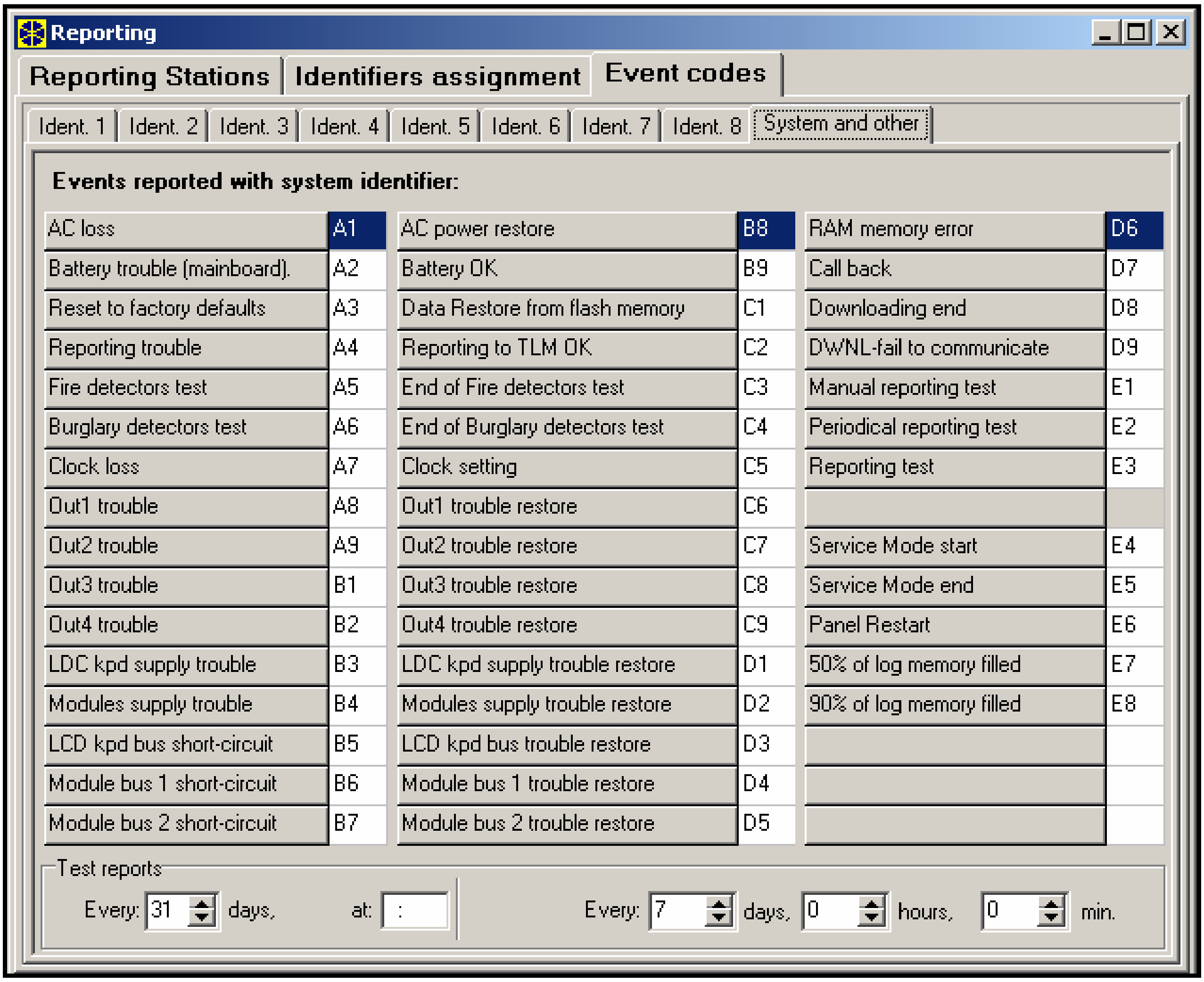
Kpd./Exp.Module:	K:00	K:04	E1:0	E1:1
PANIC alarm	32	D3	A5	A8
FIRE alarm	D3	C5	B6	B1
AUX. alarm	14	44	11	AA
Tampering	73	77	D3	BB
Tamper restore	92	88	D6	CC
Alarm - unauthorized acc			D7	CD
3 wrong access codes	53	99	DD	DA

Fig. 21. 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 Fig. 21).

System events and troubles are transmitted with their own identifier. Fig. 22 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. 22. 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 3.6 h battery. If the settings are stored in the FLASH memory, detection of this error forces "Module restart" that will be followed by "Settings restore".*
- *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 initialized with the user function, provided the "Manual transmission test" code is programmed.*

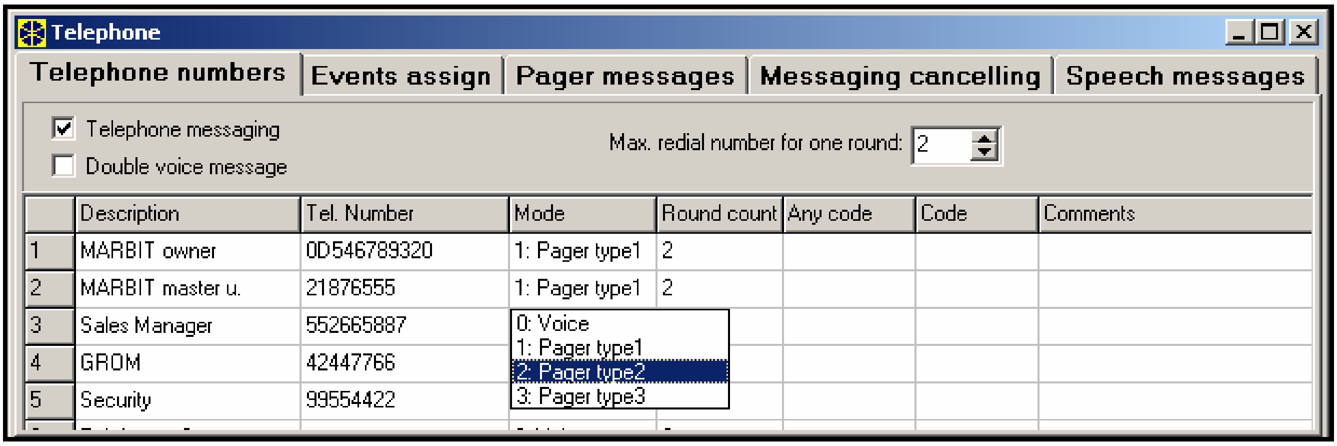
- *"Module Restart" appears at each power supply connection.*
- *Checking communication with the station is facilitated by the "Station XX test" function (in the TESTS menu of the user functions), accessible after programming the station phone numbers, system event identifier and "Monitoring test" code. Calling of this function initializes monitoring, when the control panel displays on the keypad information on the current transmission phase and the test result.*
- *The event codes shown in Fig. 21 and 22 are taken at random to illustrate an example of programming. They should be programmed as recommended by the monitoring station operating personnel.*

11. Messaging

All the INTEGRA series control panels can inform of events in the system by means of voice messages (connection of voice synthesizer is required) and PAGER type text messages. The INTEGRA 128-WRL control panel can additionally notify by means of SMS messages. The SATEL made GSM modules offer optional conversion of PAGER messages into SMS messages, thus enabling this form of messaging to be used also in case of the other INTEGRA control panels.

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.

The number of telephones to which the messaging is performed as well as the number of available voice messages or text messages depend on the size of control panel.



☑ 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					

Fig. 23. Programming phone numbers for messaging.

11.1 Activation of the messaging

1. Enable the TELEPHONE MESSAGING option.
2. Define the number of attempts to get connected in one round (function MAX. REDIAL NUMBER FOR ONE ROUND [REPETITION COUNT]). Values from 1 to 7 can be programmed.
3. Determine whether the voice message is to be played back once or twice (option DOUBLE VOICE MESSAGE).
4. Program the data for at least one telephone to which the messages are to be sent:
   – name (up to 16 characters),
   – telephone number,
   – type of messaging (voice message, PAGER or SMS messages),
   – number of rounds – the number of attempts taken by the control panel to notify the indicated telephone number of the event, unless reception of the message has

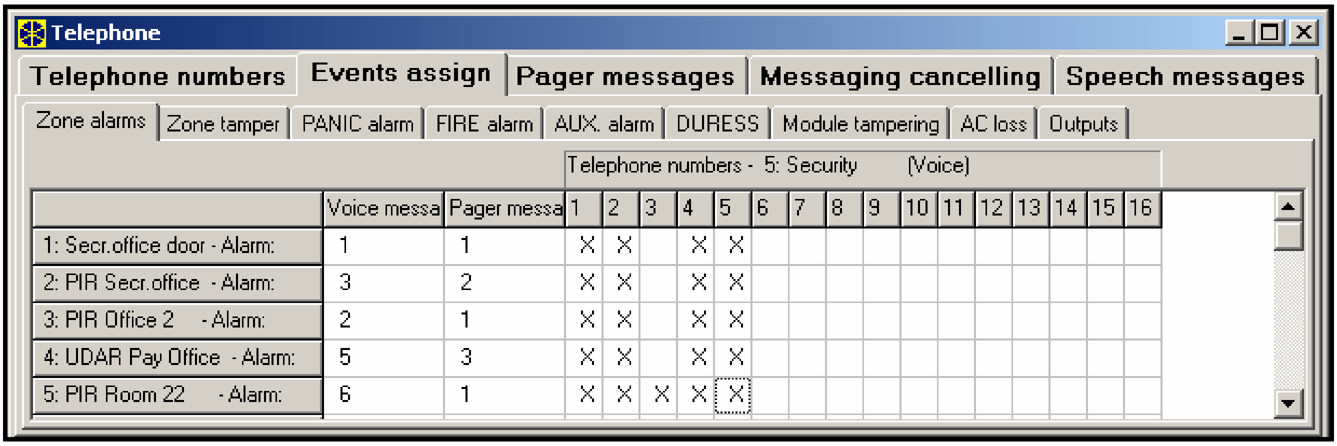
been acknowledged. Values from 0 to 15 can be programmed. Entering 0 means that notification for the indicated telephone number will be disabled.

– how the voice message is to be acknowledged (if the person receiving the message is to confirm the fact that he/she familiarized himself/herself with it, enable the ANY CODE option or enter a 4-digit code).

Notes:

- *The control panel acknowledges receiving the code by a special signal. In case of notifying of several events, the acknowledgement signal for receipt of the code sounds different, thus informing that further messages are to be expected.*
- *If no code has been programmed to acknowledge receipt of the voice message, nor the ANY CODE option has been enabled, the control panel will recognize receipt of the message as acknowledged when the receiver is picked up after two rings and any sound occurs.*

5. Record in the voice synthesizer the messages which are to be used for messaging (see the CA-64 SM voice synthesizer manual).
6. Define the contents of PAGER/SMS messages which are to be used for messaging.
7. Program any additional parameters for notifying by means of PAGER messages (PAGER TYPES) or SMS messages (SMS CENTER NUMBER).



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. 24. Defining the way of communicating alarms from zones.

8. Assign the numbers of corresponding voice messages and PAGER/SMS messages (EVENT ASSIGNMENT) to the events which are to start the messaging function.
9. Define the events of which each of the programmed telephone numbers will be notified (EVENT ASSIGNMENT).
10. In order to limit unnecessary messaging, define the cases in which notification can be cancelled (the functions CANCEL MESSAGING IN PARTITIONS and CANCEL MESSAGING AFTER ACKNOWLEDGEMENT as well as the option CANCEL TEL. AND ALARM SIMULTANEOUSLY).

12. Answering phone calls and remote control

The call answering function allows the control panel users to receive information on the partition status (arm mode, alarms). Owing to the telephone control function, the users can control the REMOTE SWITCH type of outputs by means of a telephone. For detailed information on how to use these functions please refer to the USER MANUAL.

12.1 Activation of the phone calls answering

1. Enable the ANSWERING option.

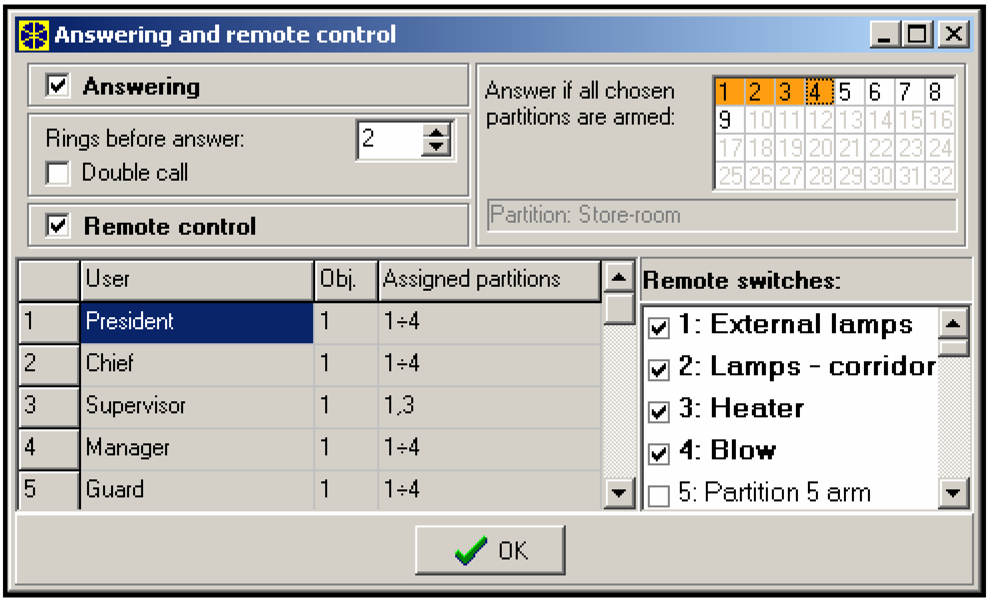
2. Define the rules of call answering by the control panel (RINGS BEFORE ANSWER parameter and DOUBLE CALL option).
3. Define whether the function is to be available at all times, or only when selected partitions are armed (function ANSWER IF PARTITIONS ARE ARMED: [ON ARMED PART.]).

Note: *If the ANSWERING - MODEM option is enabled, the control panel will be answering the calls whether the partitions are armed or not.*

4. Program the telephone codes for the users who are to use the function (see description of the USERS functions in the USER MANUAL).

12.2 Activation of the remote control

1. Activate the call answering function. The users with the telephone code assigned will have access both to the call answering function and the telephone control function.
2. Enable the REMOTE CONTROL option.
3. Program the selected outputs as the REMOTE SWITCH (type 64-79 or 98).
4. Define for each user the relays which he/she will be allowed to control. The relays can also be assigned to the users who do not have any telephone code, however only by using the telephone code one can get access to the telephone control functions.



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. 25. Defining which remote switches may be controlled by users.

13. SMS control only INTEGRA 128-WRL

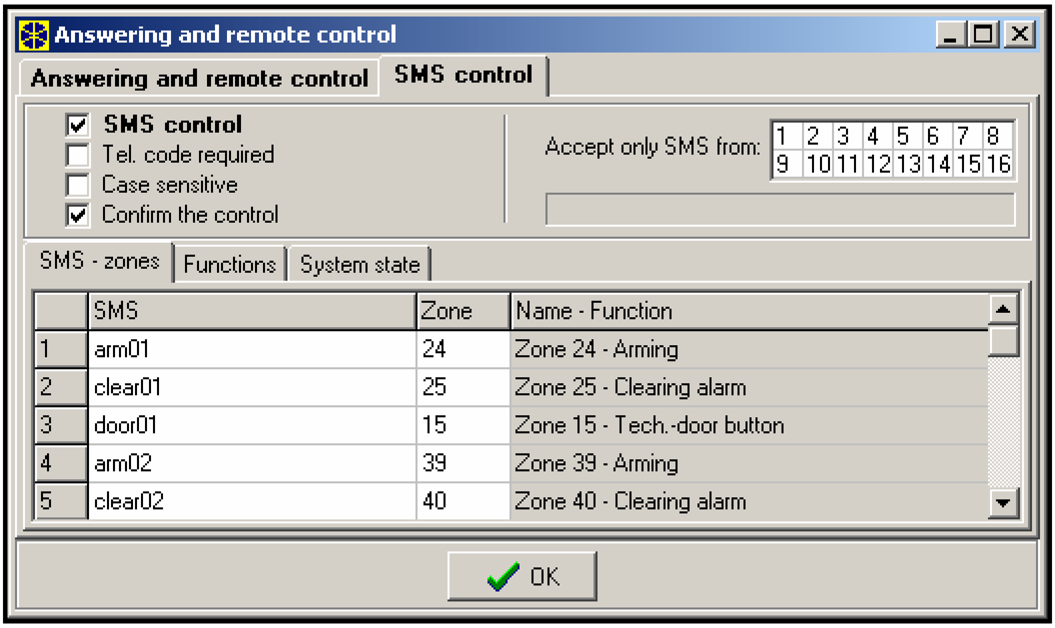
The INTEGRA 128-WRL control panel makes the SMS message control function available to the users. Receiving by the control panel of a message containing the suitable command may result in zone violation, starting the selected function, or sending the return message with information on system status. Several control commands may be included in one SMS message.

13.1 Activation of the SMS control

1. Enable the SMS CONTROL option.
2. Define whether all users will be allowed to use the SMS control function, or only those who have the telephone code (option TELEPHONE CODE REQUIRED). In the latter case, program the telephone codes for the users who are to use the function (see description of the USERS functions in the USER MANUAL). Apart from the control

command, the body of SMS message to be sent to the control panel will have to include the telephone code.

3. Define whether the control panel is to analyze the received command for case sensitivity (option CASE SENSITIVE).
4. Define whether the control panel is to confirm execution of the control by SMS message (option CONFIRM THE CONTROL). If the control panel is to send SMS messages, it is necessary to program the SMS center number (see section GSM PHONE).



☑ SMS control
□ Tel. code required
□ Case sensitive
☑ Confirm the control

Accept only SMS from: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

	SMS	Zone	Name - Function
1	arm01	24	Zone 24 - Arming
2	clear01	25	Zone 25 - Clearing alarm
3	door01	15	Zone 15 - Tech.-door button
4	arm02	39	Zone 39 - Arming
5	clear02	40	Zone 40 - Clearing alarm

Fig. 26. SMS control configuration.

5. If the control panel is to only accept the commands sent from specified telephone numbers, you should select these numbers (function ACCEPT SMS ONLY FROM SELECTED NUMBERS [AUTHORIZED TEL.]). The selection is to be made from among the telephone numbers preprogrammed for telephone messaging (see section MESSAGING). If no telephone number is selected, it will be possible to send the control messages from any telephone.
6. Program the contents of control commands and assign zones, functions, etc. to these commands. You can define 32 commands to control zones, 8 commands to start functions, and the command after receipt of which the control panel will inform about the status of selected partitions. The zones need not exist physically, but the wiring type programmed for them must be different from "Not used" or "Follow output". You can program any zone type.

Note: *When programming the control commands, remember that:*

- *the command may include up to 16 characters,*
- *the command may not contain diacritic characters and/or spaces,*
- *the commands must be different (the same command must not be used for controlling two zones, two functions, etc.),*
- *the command must not be based on contents defined for another command. In case of such commands as "zone1" and "zone11" or "arm" and "armed" the control panel will not be able to execute the second command.*

14. Control of outputs from LCD keypad

Using the LCD keypad, you can control the outputs of MONO SWITCH, BI SWITCH, REMOTE SWITCH, SHUTTER UP and SHUTTER DOWN TYPE. The way of using the control function by means of LCD keypad is described in the USER MANUAL.

To start the control function you should:

1. Program the parameters of control outputs (type, cut-off time, polarity).
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 (the zones which are to indicate the output status can be programmed as the FOLLOW OUTPUT type, which eliminates the need for making an electrical connection and enables virtual zones to be used).
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.
6. If the control is to be available without the need to enter a code, enable the QUICK CONTROL option for selected keypads.

15. 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.

16. History of the manual updates

Given below is a description of changes as compared with the manual for the control panel with firmware in version v1.04.

DATE	FIRMWARE VERSION	INTRODUCED CHANGES
2007-08	1.05	• Service mode menu has been supplemented (p. 7-21). • Information has been added regarding the armed mode to be activated by timer (p. 50, 50). • Information has been added regarding the option of resistor value programming for EOL and 2EOL loops in case of zones in CA-64 E and CA-64 EPS expanders (modules in version manufactured from 2007). • Information on new wiring types supported by the control panel has been added (p. 54). • Description of PULSES COUNT parameter has been added (p. 55). • Description of PULSES DURATION parameter has been added (p. 55). • Description of SENSITIVITY [MS] parameter has been added (p. 55). • Description of OUTPUT parameter has been added (p. 55). • Description of INTERIOR DELAYED type of zone has been supplemented with information about delay activation from INT-SCR-BL keypad, identified in the system as INT-ENT (p. 59). • Description of output triggering from partitions and partition keypads has been modified (p. 64). • Description of output triggering by control timers has been supplemented (p. 64). • Description of output triggering by type of telephone usage has been added (p. 65). • Description of output blocking by timers has been supplemented (p. 65). • Information on optional control of MONO SWITCH output by means of timer has been added (p. 66). • Description of output type 35. TELEPHONE USAGE STATUS has been modified (p. 67). • Information on new option SHUTTER NOT CONTROLLED BY ARMING has been added for outputs type 105: SHUTTER UP and 106: SHUTTER DOWN (p. 70). • Section MONITORING has been supplemented with information about SIA transmission format (p. 78-83).
2007-10	1.05	• QUICK ARM LCD keypad parameter has been supplemented (p. 74).
2008-06	1.06	• Information on INTEGRA 128-WRL control panel has been included in the manual. • Because of substituting RJ type of socket for PIN-5 socket on the control panel electronics board, the drawing illustrating computer connection to control panel has been replaced (p. 4). • Section ENTERING SERVICE MODE "FROM PINS" has been modified (p. 6). • Service mode menu has been supplemented (p. 7-21). • Section DLOADX-INSTALLER PROGRAM has been modified and supplemented (p. 24). • Section GUARDX– USER PROGRAM has been modified and supplemented (p. 32). • Section about programming GSM telephone in INTEGRA 128-WRL control panel has been added (p. 33). • New section about wireless system of the INTEGRA 128-WRL control panel mainboard has been added (p. 34). • Information on new method of arming by means of timer has been added (p. 50, 50). • Description of PARTITION EXIT DELAY parameter has been supplemented (p. 51). • Description of INFINITE EXIT DELAY option has been added (p. 51). • Description of ARMING CONTROL TIME parameter has been added (p. 51). • Section ZONES has been modified and supplemented (p. 52). • Description of NO ALARM SIGN. IN KEYPAD option has been added (p. 57). • Description of STORE EVENT ONLY IF ARMED option has been added (p. 58). • Section about new function enabling single zone testing has been added (p. 62). • Section OUTPUTS has been modified and supplemented (p. 62). • Description of new TAMPERING STATUS output function has been added (p. 71). • Section about new function enabling single output testing has been added (p. 72). • Description of QUICK CONTROL new keypad option has been added (p. 75). • Section REPORTING has been modified and supplemented (p. 78).

		• Section MESSAGING has been modified and supplemented (p. 83). • Section ANSWERING PHONE CALLS AND REMOTE CONTROL has been modified and supplemented (p. 84). • Section about controlling operation of INTEGRA 128-WRL control panel by means of SMS messages has been added (p. 85). • Section CONTROL OF OUTPUTS FROM LCD KEYPAD has been modified (p. 87).
2009-08	1.06 1.07	• Service mode menu has been supplemented (p. 7-21). • Section describing hardwired zone/output expanders in ABAX system has been modified (p. 36). • Information on ABAX system wireless detectors in passive and active mode has been modified (p. 36). • Information on configuration of AMD-102 wireless magnetic detector with input for roller shutter detector has been added (p. 38). • Information on configuration of ARD-100 wireless reorientation detector has been added (p. 39). • Subsection describing rules of using resistors in EOL and 2EOL zones and programming values of such resistors has been added (p. 55). • Description of STORE TO EVENT LOG option has been modified (p. 58). • Description of new NO REPORTING option has been added (p. 58). • Description of new NO RESTORE EVENT option has been added (p. 58). • Description of new DISABLED IN ARM STATE option has been added (p. 59). • Description of zone type 47. NO ALARM ACTION has been modified (p. 60). • Description of zone type 63. TROUBLE has been added (p. 61). • Description of zone type 80. ARMING has been modified (p. 61). • Description of zone type 81. DISARMING has been modified (p. 61). • Description of zone type 91. DETECTOR MASK has been added (p. 62). • Information on triggering outputs after receiving transmission with low-battery information from key fob has been added (p. 64). • Information on troubles signaled by output function 95. TCP/IP REPORTING TROUBLE has been added (p. 69). • Description of new output function 118. KEYFOB BATTERY LOW has been added (p. 71). • Description of SENSITIVITY function available for INT-KLCDR-GR and INT-KLCDR-BL keypads with firmware version 1.06 has been added (p. 77).
2009-09	1.07	• Declaration of conformity information (inside front cover) has been updated.
2010-08	1.07 1.08	• Declaration of conformity information (inside front cover) has been updated. • Information on INT-KSG keypad and INT-CR proximity card arm/disarm device has been added. • Service mode menu has been restructured and supplemented (p. 7-21). • Section ENTERING DATA BY MEANS OF THE KEYPAD has been added (p. 21). • Note about the new PERMANENT DLOADX ACCESS option available to the master user has been added (p. 24). • Section about remote programming through modem has been altered (s. 25). • Description of new GSM BAND parameter programmed for INTEGRA 128-WRL control panels with electronics version 2.01 has been added (p. 34). • Section SYSTEM OPTIONS has been added (p. 42). • Description of new VALID WITHIN 60 SEC option for partitions has been added (p. 50). • Section about zone parameters has been altered and supplemented (p. 53). • Description of new wiring types available for zones on mainboard of INTEGRA 128-WRL control panels with electronics version 2.01 has been added (p. 54). • Description of new ALARMING zone option has been added (p. 57). • Description of new ACTIVE DURING VIOLATION output option has been added (p. 64). • Some descriptions in section SOURCE OF OUTPUT TRIGGERING have been modified (p. 64). • Description of 23. ARM/DISARM ACKNOWLEDGE output type has been modified (p. 66). • Description of 24. MONO SWITCH output type has been modified (p. 66). • Description of 46. LOGICAL AND output type has been modified (p. 68). • Description of 47. LOGICAL OR output type has been modified (p. 68). • Description of new 119. WIRELESS SYSTEM JAMMING output type has been added (p. 71).

		• Section describing LCD keypad parameters and options has been altered and supplemented (p. 73). • Section PREFIXES has been altered (p. 77).

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