



RT4-5GL object module

V.34-20

User manual

2016

Table of Contents

Device features.....	3
Technical information.....	3
General information.....	4
Module appearance.....	5
Device inputs and outputs.....	6
First start and general programming.....	6
Indication.....	7
Message format.....	8
Working modes.....	9
Working with two SIM cards.....	11
Command activation via call.....	11
Working in SMS mode.....	11
Working with the phone numbers of the defined length.	11
Controlling other GSM devices.....	11
Working in GPRS mode.....	11
Working in Control panel mode.....	14
Device programming.....	14
Module zone configuration.....	15
Dallas mode.....	16
Key-switch mode.....	18
Remote arming and disarming.....	18
Module registration in the WinSC software.....	19
Request status and settings commands.....	20
Connecting external devices.....	21
Enclosure 1. Terminal block pins.....	27
Enclosure 2. Module control commands.....	27
Enclosure 3. Module service commands.....	28
Enclosure 4. Module events.....	30
Enclosure 5. Event codes for Esprit security panels.....	31
Enclosure 6. Event codes for SP/Magellan security panels.....	32
Enclosure 7: Key-BUS event codes.....	35
Enclosure 8. Event codes for Digiplex security panels.....	36
Enclosure 9. Event codes for CADDX NX security panels.....	38

Device features

- Ability to transmit information via both SMS and GPRS channels;
- Working with two SIM cards (main and backup);
- Two IP support for transmitting via GPRS channel (main and backup);
- Ability to connect to server using domain name;
- 254 event log;
- Ability to remotely configure module parameters and update module firmware version via GPRS;
- Ability to control other GSM devices using SMS messages;
- USB port for device programming;
- Indication of the status of both SIM cards, power status, and data transmitting;
- 5 general purpose inputs;
- Power supply control input;
- 2 general purpose outputs/PGMs;
- Two communication ports for connecting to the control panels;
- Ability to work in control panel mode;
- Ability to activate preprogrammed command by calling to the module;
- Ability to send e-mail messages;
- Up to 4 user support;
- Two switchable message modes: "User" and "Modem";
- Periodic channel test;

Technical information

GSM protocol	E-GSM 900/1800/GPRS
GSM modem	Quectel
SIM card type	MicroSIM
SIM interface	3 and 1,8 V
Number of users	4
Output capacity	1A
Maximum voltage on closed output	30V
Maximum voltage on closed inputs	30V
Power supply	10 – 30V
Input current (at 12V power supply)	15mA
Input current in GPRS mode	150mA
Dimensions	68x125x19 mm

General information

RT4-5GL object device is designed for collecting information from control panel, it's processing and transmitting it to the Central Unit. Device can transmit information to 4 users simultaneously. First user can receive information either via GPRS or via SMS, other users – only via SMS.

Module can work with two SIM cards, the first SIM card is considered the main one, the second – backup. In case the first SIM card fails to work for any reason, module starts working with the second one. At the same time module periodically tests the first SIM card, and if it is operational, returns to working with it.

Module also supports work with two IP addresses. The first IP address is considered the main one, the second - backup. When module loses connection with the main IP address, it tries to connect to the second one. While connected to the second IP address, module periodically tries to establish connection with the main IP address. If successful, module returns to working with the first IP address. You can use domain name in the place of the first IP address.

Module has 5 general purpose inputs, power supply control input, 2 outputs that can be used either as PGM or as manually activated outputs, two communication ports that are used for connecting various security panels, and power output for connecting different interface devices and module outputs.

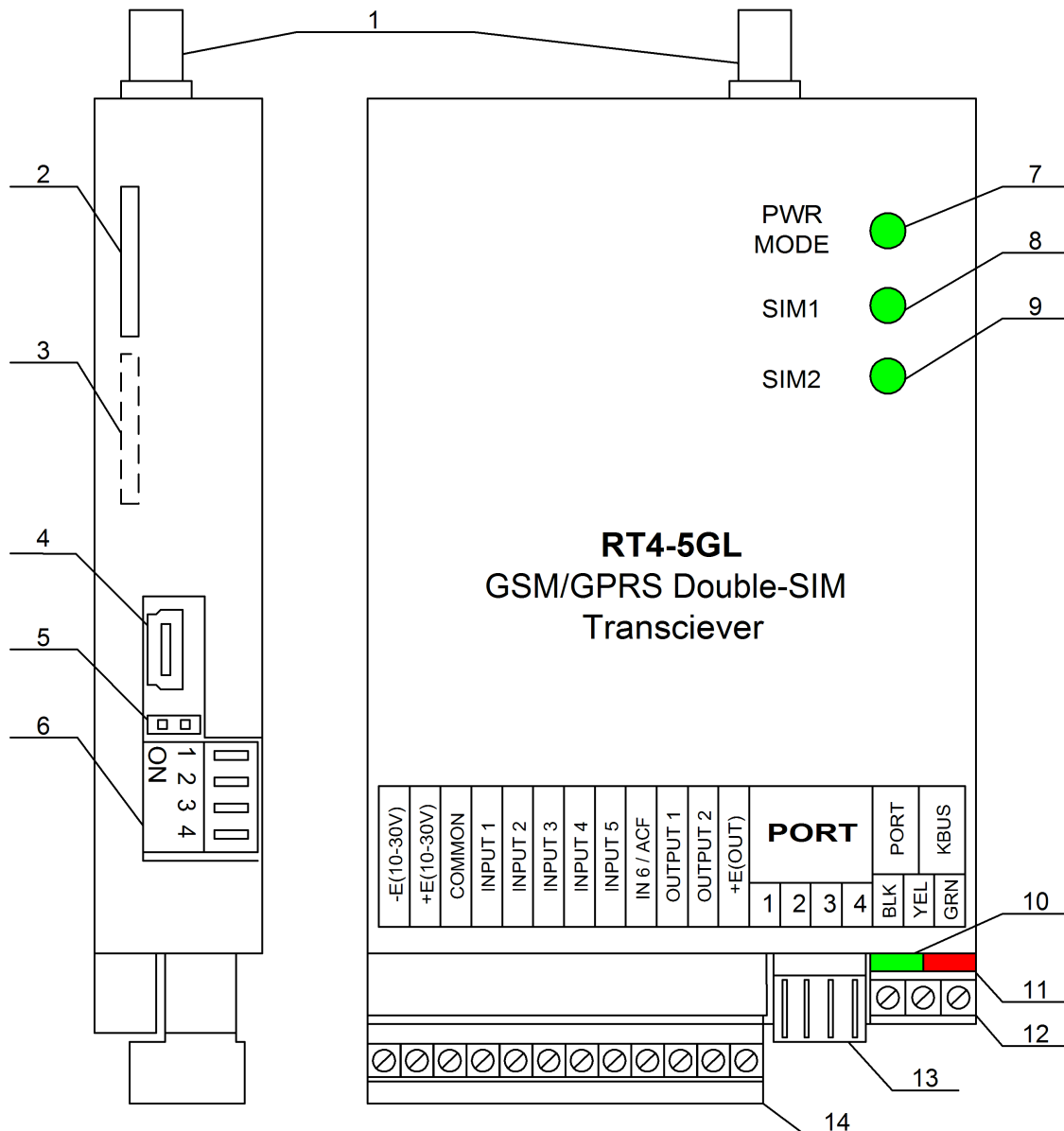
Version 2.0 **RT4-5GL** module has 9* switchable working modes:

- 1 — working via Serial BUS protocol
- 2 — working with Caddx NX control panels
- 3 — working in control panel mode
- 4 — working with Esprit control panels
- 5 — working with Magellan control panels
- 6 — working with one- and two-partition DSC panels using Key-BUS protocol
- 7 — working with multi-partitioned DSC panels using Key-BUS protocol
- 8 — working with Digiplex control panels
- 9 — working with ABAS II address bus.

RT4-5GL also controls it's power level and transmits alarm message in case it is lower than normal.

** Number of working modes may be increased in the future.*

Module appearance



Pic. 1 RT4-5GL module appearance.

1. GSM antenna connector (SMA-F)
2. Main SIM holder (Micro SIM)
3. Backup SIM holder (Micro SIM)
4. Mini USB for module programming
5. Jumper to control input load
6. Dip-Switch for changing working mode
7. Power and mode indicator
8. SIM 1 status and signal strength indicator
9. SIM 2 status and signal strength indicator
10. First communication port indicator (PARADOX panels, interfaces and expanders)
11. Second communication port indicator (DCS and CADDX NX control panels)
12. Communication port for connecting DCS and CADDX NX control panels
13. Communication port for connecting PARADOX panels, interfaces and expanders
14. Terminal block for power supply and external device connection

Device inputs and outputs.

Device inputs can be loaded to «0» or to «+». Choice is made using the jumper. If jumper is removed, inputs are loaded to «+» (reacts to «0»/«break» signals), if set – loaded to «0» (reacts to «+»/«break» signals). Maximum voltage on the input - **+30V**.

By default all general purpose inputs (IN1-5) are programmed as NO and power supply control input (I6) as NC.

Attention! When jumper is set all the inputs change their status to opposite.

If you need to change input type, you have to connect all external devices, make sure they are in the normal state and send the following command to the module: **00.xxxx** where xxxx – module security code. After receiving this command, module will set all input state as normal.

Device outputs can work either as manually activated outputs or PGM outputs.

Manually activated output is activated and deactivated using SMS-message. You can also activate it on time.

PGM-output can react to the following troubles: GSM-signal lost, cannot connect to server or cannot establish GPRS connection.

Outputs are configured using **USB_Reader v.1.3.7** software. By default – manually activated.

First start and general programming.

Insert into the module two activated SIM cards (in case you are using only one SIM card, insert it into the main SIM holder). If the PIN request is activated in the SIM cards, than PIN code must be «0000».

After that you can start module programming. Module is programmed using **USB_Reader v.1.3.7** software. To turn on programming mode, just connect the USB cable. When **POWER/MODE** indicator will turn red you can start programming.

First you must program first user's phone number, module account and, if you are going to use module in GPRS mode, server IP-address, TCP-port, APN and module Online ID. In order for the module to work correctly with TLF_Server and WinSC software, it is recommended to set OnlineID the same as the main SIM card telephone number (without international code).

In case if it is not possible to use **USB_Reader** software, you can program the module using SMS messages.

To program the first user's phone number, power the module and, after successful initialization (POWER/MODE indicator is green), send to the module the following message: **91.xx...xx**, where **xx...xx** – phone number. This message must be send from the first user's phone only.

Attention! Phone must be programmed with the international code. Before the code must be inserted «+».

If the number is successfully programmed, the first user will receive „OK” message.

Then you have to change device account. To do so, send from installer's phone the following message **95.xxxxyyyy** where xxxx – module security code (default – 1234) and yyyy – new account.

After that you can program the module to connect to the TLF_Server software. Full command list is set in the “Working in GPRS mode” paragraph.

Indication

POWER/MODE indicator	
Off	Module not ready to work
Green	Module is ready to work
Single yellow blink	Message is generated
Blinks green fast	Message is being transmitted
Few red blinks	Failed to transmit a message. Number of blinks indicates user number, to who module failed to transmit the message.
Flashes green once per second	Low voltage
Red	Module in programming mode
Flashes red	Different SIM cards is registered in module
SIM1 indicator	
Off	SIM card is not inserted
Green. Flashing green once every 2-3 seconds	Module in GPRS mode. GSM signal at high level
Yellow. Flashing once every 2-3 seconds	Module in GPRS mode. GSM signal at medium level
Red. Flashing once every 2-3 seconds	Module in GPRS mode. GSM signal at low level
Flashing green once every 2-3 seconds	Module in SMS mode. GSM signal at high level
Flashing yellow once every 2-3 seconds	Module in SMS mode. GSM signal at medium level
Flashing red once every 2-3 seconds	Module in SMS mode. GSM signal at low level
Flashing red once per second	Out of GSM coverage
Flashing red once every 8 seconds	SIM card failure
Flashing green once every 8 seconds	SIM card is operational, but not used at the moment
SIM2 indicator	
Off	SIM card is not inserted
Green. Flashing green once every 2-3 seconds	Module in GPRS mode. GSM signal at high level
Yellow. Flashing once every 2-3 seconds	Module in GPRS mode. GSM signal at medium level
Red. Flashing once every 2-3 seconds	Module in GPRS mode. GSM signal at low level
Flashing green once every 2-3 seconds	Module in SMS mode. GSM signal at high level
Flashing yellow once every 2-3 seconds	Module in SMS mode. GSM signal at medium level
Flashing red once every 2-3 seconds	Module in SMS mode. GSM signal at low level
Flashing red once per second	Out of GSM coverage
Flashing red once every 8 seconds	SIM card failure
Flashing green once every 8 seconds	SIM card is operational, but not used at the moment

Indication

PORT indicators	
Indication in Serial BUS mode (green LED)	
Flashes green	Transmitting information via communication port
Indication in Esprit and Magellan modes (green LED)	
Flashes green	Transmitting information via communication port
Indication in Digiplex mode (green LED)	
Flashes green	Transmitting information via communication port
Indication in DSC 1 and DSC 2 modes (red LED)	
Flashes red	Transmitting information via communication port
Blinks red fast	Wrong mode is set
Indication in Caddx NX mode (red LED)	
Flashes red	Transmitting information via communication port
Control Panel mode: Key reader LED or outer LED in Key-switch mode	
Constantly on	Disarmed. Ready to be armed
Off	Disarmed. Not ready to be armed
Double flashing once every 2 seconds	Armed
Flashes constantly	User key programming mode ON
Triple flashing once every 2 seconds	Guard key programming mode ON

Message format

Module events in "Modem" mode and events from the Paradox, DSC and Caddx NX security panels are always transmitted in ContactID format.

In WinSC software messages are looking the following way:

Partitions=PP EventCode=FEEEZZZ

F – Event type identifier: E — alarm/disarming, R — restore/arming.

EEE – Event code.

PP – Partition. Module own messages are transmitted with partition 99.

ZZZ – Zone/User number.

On the mobile phone information is displayed the following way:

FF, AAAA,EEPPZZZ:<date>-<time>*<CS>

FF – Event type identifier: 06 — alarm/disarming, 07 — restore/arming.

AAAA - Account

EEE – Event code.

PP –Partition. Module own messages are transmitted with partition 99.

ZZZ – Zone/User number.

<CS> - Check sum.

Messages that are transmitted via communication port in the first mode are not automatically converted into ContactID and their format depends on the connected device type.

Working modes

RT4-5GL module has nine different working modes:

▪Serial interface mode (Serial BUS).

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☐ ☐ ☐ ☐ - OFF
☒ - ON

In this mode you can connect interface modules to the communication port, for acquiring information from control panels. In this mode all the messages are transmitted in the same format they are generated by the device, connected to the port (no conversion into ContactID format are made). When connecting security panel to the module in this mode, make sure that their accounts are identical.

▪Control panel mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☒ ☐ ☐ ☐ - OFF
☒ - ON

In this mode device is monitoring it's inputs status, depending on the arming status (armed/disarmed). Arming is made using Dallas touch memory keys, proximity chips or key-switch option. Key or proximity readers are connected to the serial port.

For further information see paragraph «Working with transmitter in control panel mode».

▪ABAS II mode.

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☐ ☐ ☒ ☐ - OFF
☒ - ON

In this mode you can connect devices that communicate using **ABAS** address line and input/output expanders.

Not supported in this version of the module.

▪Esprit mode.

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☐ ☒ ☐ ☐ - OFF
☒ - ON

In this mode you can connect **PARADOX ESPRIT 7x8** (V 3.00 and higher) security panel. Panel is connected via it's specialized serial port. All the panel's messages are converted into ContactID format (see table 6). All messages are transmitted with the **RT4-5GL** account.

▪Magellan mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☒ ☒ ☐ ☐ - OFF
☒ - ON

In this mode you can connect **PARADOX** panels of the **E**, **SP** and **MG** series. Panel is connected via it's specialized serial port. All the panel's messages are converted into ContactID format (see table 6). All messages are transmitted with the **RT4-5GL** account.

▪DCS 1 mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☐ ☒ ☒ ☐ - OFF
☒ - ON

In this mode communication port is connected to the Key-BUS line of the one- and two-partitioned DSC security panels. All messages are transmitted with the **RT4-5GL** account.

▪DSC 2 mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☒ ☐ ☒ ☐ - OFF
☒ - ON

In this mode communication port is connected to the Key-BUS line of the DSC security panels that has more than two partitions. All messages are transmitted with the **RT4-5GL** account.

▪Digiplex mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☐ ☒ ☒ ☒ ☐ - OFF
☒ - ON

In this mode you can connect **PARADOX** panels of the **Digiplex** series. Panel is connected via it's specialized serial port. All the panel's messages are converted into ContactID format (see table 6). All messages are transmitted with the **RT4-5GL** account.

▪Caddx NX mode

To activate this mode you have to set the following combination on the dip-switch:

Switch: ☒ ☐ ☐ ☐ ☐ - OFF
☒ - ON

In this mode communication port is connected to the address line of the **CADDX NX** panels. All messages are transmitted with the **RT4-5GL** account.

Attention!: to register module in the system, you must enter and exit panel programming mode.

Working with two SIM cards.

Module can work with two SIM cards, the first SIM card is considered the main one, the second – backup.

When powered, module analyzes presence of both SIM cards and if any of SIM cards are not inserted, it will no longer be analyzed. This SIM card indicator will not be active.

If both SIM cards are inserted, than module starts working with the main SIM card. Backup SIM indicator will flash green every 8 seconds, indicating that this SIM is operational, but not in use. Main SIM indicator will show current SIM state and signal strength.

If the main SIM fails, module will switch to the backup SIM. In this case main SIM indicator will flash red every 8 seconds and backup SIM indicator will show current SIM state and signal strength.

Simultaneously with the periodic test (default every 24 hours) module checks presence and status of both SIM cards and, if possible, switches to the main SIM card.

Attention!: It is recommended to enable **SIM2 check enable** parameter in module options in order for module to work correctly with two SIM cards (see Programming manual).

Command activation via call.

You can activate preprogrammed command by making a call to the module from one of the registered user phones. For each user you can program only one command.

When module receives a call from registered user, it drops connection and activates preprogrammed command.

You can only program the command using **USB_Reader v.1.3.7** software (see Programming manual).

Working in SMS mode.

In SMS mode each user can receive information in two formats: "modem" and "user". Format selection is made by user and depends on the module usage strategy. Each user can change the format by sending "*" message to the module.

"Modem" format is designed for receiving by CU-GSM central unit and WinSC software.

"User" format is used if information is send to the mobile phone. In this mode module sends information in text format (see enclosures 2 – 4).

You should pay attention to the accuracy of the commands sent to the module. In case of lost or redundant symbol (including spaces) command will be ignored.

Working with the phone numbers of the defined length.

Module identifies users by the phone number. Module can identify phone number by the specified number of digits, instead of the whole number.

Symbol count starts from the end of the number. Maximum number of symbols is 16, "+" is not counted.

Number of symbols is set using **99.Nx** command, where x – number of symbols. If you will send **99.N0** command – module will work only with fully specified phone numbers. By default number length is set as 8.

This option can also be configured using **USB_Reader v.1.3.7** software.

Controlling other GSM devices.

Module can send messages in plain text format, that can be received by other GSM devices made by Cortex company. In this mode time and partition number are removed from the message. To activate this mode you have to set message format as "User" and, using **USB_Reader v.1.3.7** software, add \$ sigh before the message text (see Programming manual).

Working in GPRS mode.

In this mode module establishes direct connection with the TLF_Server software and transmits full information via GPRS channel.

Attention! In GPRS mode module doesn't send SMS messages to the first user.

Working with two IP addresses

You can program two IP addresses in the module. The first IP address will be main, the second – backup. If the domain name is programmed – it will be used instead of the first IP address.

When powered on, module always tries to establish connection with the main IP. If the first IP is not programmed, module will continue working in SMS mode.

If module failed to establish connection with the main IP, or this connection is lost, module establishes connection with the backup IP. When connected to the backup IP, module periodically (default – 1 hour) tries to establish connection with the main IP. If failed, module restores connection with the backup IP and repeats attempt again in an hour.

GPRS settings

In order for module to work correctly in GPRS mode you must configure the following parameters: **APN** (Access point name to connect to the GPRS service), Central Unit **IP-address**, Central Unit **TCP PORT**, **Online ID** (module online identifier), Central unit **Domain name** (if used), Central Unit **DNS Server IP** (if used). These parameters can be configured using **USB_Reader** software or by sending a command to the module:

99.I <IP>	Main IP address
99.II <IP>	Backup IP address
99.A <access point>	Main SIM card APN
99.AA <access point>	Backup SIM card APN
99.P <port>	Main server TCP port
99.PP <port>	Backup server TCP port
99.M <мин>	Time between attempts to reconnect to server
99.R <мин>	Time between attempts return to the main IP
99.DI <IP>	IP-address of DNS server (if used)
99.DD <domain name>	Domain name (if used)

If main IP address or DNS server are programmed, module will try to establish GPRS connection directly after powered up. If main IP address is not set or set as 0.0.0.0 and DNS server IP-address is not programmed than module stays in the SMS mode.

Forced exit from GPRS mode

For power saving purposes module can exit GPRS mode if there are troubles with power supply.

You can specify conditions on which module will exit GPRS. Those can be specified either by

USB_Reader software, or by the following SMS commands:

99.F0 – Don't exit GPRS unless command **86.<security code>** is received

99.F1 – Exit GPRS if power low (default).

99.F2 – Exit GPRS if 220V lost.

99.F3 – Exit GPRS if power low or 220V lost.

If this option is enabled and the battery is low and/or power is lost (depends on the settings), the module will send **E804000** (in "modem" mode) or **Check bat or power** (in "User" mode) message when an attempt to turn GPRS mode on is made.

Mobile operator authorization for GPRS activation.

In case you need to authorize with the mobile operator for GPRS activation, you have to specify login and password

Login for the main SIM card is set by the **99.Y1xxxx** command, where xxxx – login.

Password for the main SIM card is set by the **99.Y2xxxx** command, where xxxx – password.

Login for the backup SIM card is set by the **99.YY1xxxx** command, where xxxx – login.

Password for the backup SIM card is set by the **99.YY2xxxx** command, where xxxx – password.

Number of symbols in login and password must not exceed 8.

If you need to delete login and password, you have to send corresponding SMS messages **99.Y1**, **99.Y2**, **99.YY1** and **99.YY2**

Those parameters can also be changed using **USB_Reader v.1.3.7** software.

Online identifier

In order to send a message to the module from the **WinSC** software, you have to assign a unique ID for it. In order for module to work correctly with the **TLF_Server** and **WinSC** software, it is recommended that ID would be the same as module phone number (without international code).

Attention! ID must only contain digits and be maximum 15 symbols long.

You can set online ID either by using **USB_Reader v.1.3.7** software, or by sending **99.Wxxxx** message, where xxxx – identifier.

By default online ID is set as 11111111.

Sending e-mail

Module can send e-mail messages to the specified e-mail address. Messages are sent accordingly to the settings for the third user. Third user phone number are not used in this case and doesn't need to be programmed. To turn this mode on you must activate **Email enable** checkbox in **USB_Reader v.1.3.7** or **TLF_Server** software, or send the following command to the module: **99.E1** To turn this mode off you must deactivate **Email enable** checkbox in **USB_Reader v.1.3.7** or **TLF_Server** software, or send the following command to the module: **99.E0**

In order for the mode to work correctly, you must configure the following parameters:

SMTP address — address of the SMTP server that will be used to send messages.

SMTP port - TCP port of the mail server that will be used to send messages .

User name for authentication – mail server user name (if used)

Password for authentication – mail server password (if used)

With authentication checkbox – if active, module will attempt to register on the mail server. If server doesn't support authentication, this checkbox must be deactivated.

Email enable checkbox – if active, module will send e-mail messages.

Sender's name – Optional field. Determines the name of the e-mail sender that is displayed when e-mail is received.

Sender's mail – Optional field. Determines the e-mail address of the sender that is displayed when e-mail is received.

Mail of recipient – e-mail address, where messages will be send.

It is recommended to use the following SMTP servers with given parameters:

Mobile operator	SMTP server address	SMTP server port	Needs authentication
LMT; Amigo	com.lmt.lv	25	no
Tele 2	smtpserver.swip.net	25	no
	mailgw.swip.net	25	no
Bite	smtp.banga.lt	25	no
	mail.bite.lv	25	no

If you are using different operator, or different SMTP server, than parameter settings may differ. Consult your mobile operator and internet provider.

Attention! Module supports only servers that doesn't use **TSL/SSL** encryption. If **TSL/SSL** encryption is used, message will not be sent.

Possible errors

- If failed to establish GPRS connection:

GPRS error (in „User” mode) or **E854001** (in „Modem” mode).

Possible causes: wrong APN setting or unavailability of this service at the current mobile operator.

- If failed to connect to software or Central unit:

Online error (in „User” mode) or **E854002** (in „Modem” mode).

Possible causes: wrong IP, TCP PORT settings. Firewall restrictions on the Central Unit.

Working in Control panel mode

In this mode device is monitoring it's inputs status, depending on the arming status (armed/disarmed). Arming is made using Dallas touch memory keys or key-switch option. Key reader or key-switch is connected to the serial port.

In „Disarmed” mode any zone violation is monitored, but transmitted only violation of 24H zone and PWR zone. Other zone status is ignored.

In „Armed” mode any zone violation leads to device activation (depending on the input configuration and sequence of zone violation), siren activation and further message transmission to the Central Station. Zone restores are also transmitted to the Central Station

Device programming

Device programming is made using **USB_Reader** software via computer USB-port.

To turn on programming mode, just connect the USB cable and power the module. When **POWER/MODE** indicator will turn red you can start programming.

In order to program control panel parameters you have to open programming window through the main menu **File/Read** or by pressing  icon and than select **Panel mode** tab.

You can configure the following parameters:

EntryDelay – entry delay

EntryDelayForStay – entry delay for the STAY ARM mode

Exit Delay – exit delay

BellCutOff – siren working time when alarm is activated

Z1 Type – type of the first zone. Three options available:

24h. Always activated and causes the alarm regardless of the system status (armed/disarmed)

Interior. After the delayed zone has been activated, interior zone works same as delayed. If delayed zone wasn't activated, it works as instant zone.

Instant. Zone with this parameter has an exit delay, but will immediately activate the alarm when triggered after the exit delay is over.

Z1 StayAway checkbox – first zone parameter that determines if zone will be ignored when system is armed in STAY ARM mode (Stay/Arm) or not (Normal). If zone type is 24h, than this parameter is ignored.

Z3 Type – type of the third zone. Options are the same as for the first zone.

Z3 StayAway checkbox – third zone parameter that determines if zone will be ignored when system is armed in STAY ARM mode (Stay/Arm) or not (Normal). If zone type is 24h, than this parameter is ignored.

Z4 Type – type of the fourth zone. Options are the same as for the first zone.

Z4 StayAway checkbox – fourth zone parameter that determines if zone will be ignored when system is armed in STAY ARM mode (Stay/Arm) or not (Normal). If zone type is 24h, than this parameter is ignored.

Z5 Type - type of the fifth zone. Options are the same as for the first zone.

Z5 StayAway checkbox – fifth zone parameter that determines if zone will be ignored when system is armed in STAY ARM mode (Stay/Arm) or not (Normal). If zone type is 24h, than this parameter is ignored.

KeySwitch checkbox – determines whether arming will be made using electronic keys (deactivated), or key-switch (activated).

PwrZone(Input6)RandomDelay checkbox – not used in current version.

LinesWithSingleEOLResistor checkbox – determines type of the security loops. With EOL resistor (activated) or NC (deactivated).

Settings are saved by pressing “OK” key.

Module zone configuration

Some module zones functions are strictly programmed and cannot be changed.

Zone functions are following (see Pic.2):

1-st input: Programmable zone.

2-nd input: **Entry/Exit**. Delayed zone. Has entry and exit delays and usually is used for the front door. Entry and exit delays can be programmed for the duration you need.

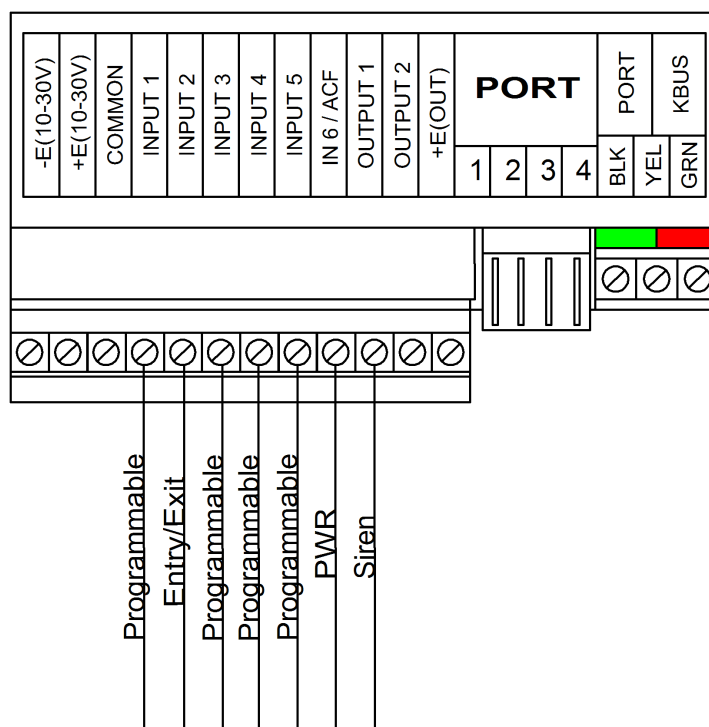
3-rd input: Programmable zone.

4-th input: Programmable zone.

5-th input: Programmable zone.

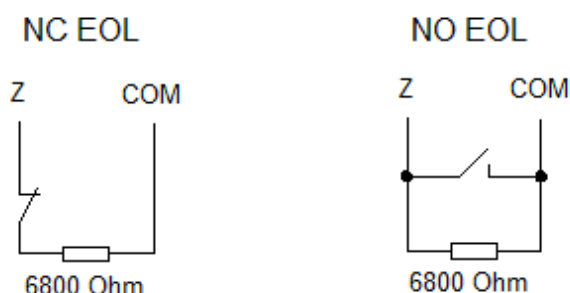
6-th input: **PWR**. Input is designed for power supply monitoring and must be connected to the «ACF» output of the **VSCS-1,5/VSC-3,0-12** devices or to the «OUT» output of the **AC_detector** device.

1-st output: Siren. In the control panel mode the first output is strictly programmed to work as a **Bell PGM**.



Pic.2.

Zone wiring in EOL mode



Loop resistance in the normal state must be 6,8kΩ

Dallas mode

In this mode arming and disarming is made using Dallas touch memory keys or proximity chips.

Arming

Before arming close all secured doors and windows and stop moving within the sensor range. If at least one zone is triggered (opened) than object is not ready for arming and LED on the key reader won't be lightened. System can be armed only if LED constantly lightened, i.e. all zones are in normal state and system is ready for arming.

To arm the system you have to touch key reader with registered touch memory key. If you will touch the key reader while LED is turned off (not ready to arm), arming operation will be ignored and you will hear long sound signal. Additionally you will be shown the number of the violated zones by the LED blinking (number of blinks – number of the first violated zone). To arm the system, remove all causes that prevent arming and once again touch the key reader with the key.

After the system is armed exit delay will be started. During this you can leave the secured space without triggering the alarm. Delay is indicated by sound signal that will beep once every two seconds and once a second during the last ten seconds of delay. After exit delay expires the system will be armed (LED will double-blink once every two seconds) and a message will be sent to the Central Station.

If during exit delay you will touch the key reader with the registered key, the system will return to the disarm state without sending any message to the Central Station.

Arming in STAY ARM mode

To arm in STAY ARM mode at least one zone must have Stay/Away parameter enabled. If so, during the exit delay Entry/Exit zone (IN2) activation is monitored. If zone didn't activate (door wasn't open) **STAY ARM** mode is activated. In this mode, activation of the zone with enabled **Stay/Away** parameter is ignored. You can also set separate entry delay for this mode.

If during the exit delay Entry/Exit zone was activated (door was opened) than arming is made in the standard mode.

Disarming

When entering secured space, delayed zone triggers. At that moment entry delay is started. Delay is indicated by constant sound signal.

You have to disarm the system (touch the key reader with registered touch memory key) before delay hasn't expired. In that case "Disarmed" message will be sent to the Central Station. Otherwise an alarm message will be sent.

Touch memory/proximity key registration

You can program three key types in the device:

"Master"-key – the first key that was put to the key reader. Using this you can turn on key programming modes.

User keys – keys that are used to arm and disarm the system.

Guard keys – keys that are used to confirm that security crew arrived to the object after alarm receiving. You can't arm or disarm the system or deactivate the siren using these keys. When this key is put to the key reader, transmitter forms and sends a special message to the Central Station.

Registering the "Master"-key is made the following way: Touch the key reader with the "master"-key and wait for the triple beep.

Registering the user keys is made the following way:

Touch the key reader with the "master"-key (for approximately 1 second) – the device will turn on user key registration mode (indication LED blinks fast). Touch the key reader with the user keys, one after another. After touching the key reader with the key, you should either hear triple beep (if registration is successful) or one long beep (if the key is already registered). Maximum number of user keys is 16.

To exit user key programming mode you have to wait 1 minute without touching the key reader (device will return to it's normal mode) or touch the key reader with the "master"-key (device will switch to guard key registration mode).

Registering the guard keys is made the following way:

Touch the key reader with the "master"-key two times (for approximately 1 second each) – the device will turn on guard key registration mode (indication LED blinks three times once every 2 seconds). Touch the key reader with the guard keys, one after another. After touching the key reader with the key, you should either hear triple beep (if registration is successful) or one long beep (if the key is already registered). Maximum number of guard keys is 16.

To exit user key programming mode you have to wait 1 minute without touching the key reader or touch the key reader with the "master"-key.

To delete all registered keys, including the „master“-key you have to connect input 2 and the first contact on the interface port and power up the transmitter.

To delete all registered user keys, you have to connect input 3 and the first contact on the interface port and power up the transmitter.

To delete all registered guard keys you have to connect input 4 and the first contact on the interface port and power up the transmitter.

Attention! When deleting master-key, module status is always changed to "Disarmed".

Key-switch mode

In this mode you can arm and disarm the system by connecting the 1-st and the 2-nd contacts on the interface port.

Arming

Before arming close all secured doors and windows and stop moving within the sensor range. If at least one zone is triggered (opened) than object is not ready for arming and LED on the key reader won't be lightened. System can be armed only if LED constantly lightened, i.e. all zones are in normal state and system is ready for arming.

To arm the system you have connect the 1-st and the 2-nd contacts on the interface port. If you will connect them while LED is turned off (not ready to arm), arming operation will be ignored and you will hear long sound signal. Additionally you will be shown the number of the violated zones by the LED blinking (number of blinks – number of the first violated zone). To arm the system, remove all causes that prevent arming, disconnect the contacts and then connect them again.

After the system is armed exit delay will be started. During this you can leave the secured space without triggering the alarm. Delay is indicated by sound signal that will beep once every two seconds and once a second during the last ten seconds of delay. After exit delay expires the system will be armed (LED will double-blink once every two seconds) and a message will be sent to the Central Station. If during exit delay you will disconnect the contacts, the system will return to the disarm state without sending any message to the Central Station.

Disarming

When entering secured space, delayed zone triggers. At that moment entry delay is started. Delay is indicated by constant sound signal. You have to disarm the system (disconnect the contacts) before delay hasn't expired. In that case "Disarmed" message will be sent to the Central Station. Otherwise an alarm message will be sent.

Attention! To deactivate the siren that has activated during the disarmed state (24H zone) you have to connect and then disconnect the 1-st and the 2-nd contacts on the interface port.

Remote arming and disarming

Module can be armed and disarmed using SMS message.

Attention! Valid remote arming and disarming is possible **only** in Dallas mode.

Remote arming

In order to remote arm the module you have to send it the following message **11.xxxx** where **xxxx** — module security code.

When message is received, module analyses all it's input status and, depending on the result, performs one of the two actions:

1. If all zones are in the normal state than module changes it's status to "armed" and **Remote ARM (R840016** in "modem" mode) message is sent to the users.
2. If one or more zones are in the alarm state, than the module sends back the status message, where all of the alarmed zones are listed. Module stays in "Disarmed" state.

Remote arming in STAY mode

In order to remote arm the module in STAY mode you have to send it the following message **10.xxxx** where **xxxx** — module security code.

When message is received, module analyses all it's input status and, depending on the result, performs one of the two actions:

1. If all zones are in the normal state than module changes it's status to "armed" and **Remote STAY ARM (R841016** in "modem" mode) message is sent to the users.
2. If one or more zones are in the alarm state, than the module sends back the status message, where all of the alarmed zones are listed. Module stays in "Disarmed" state.

Remote disarming

In order to remote arm the module you have to send it the following message **12.xxxx** where **xxxx** — module security code.

When message is received, module changes it's status to "Disarmed" and **Remote DISARM (E840016** in "modem" mode) message is sent to the users.

Module registration in the WinSC software

In order to work correctly module must be registered in the software the following way:

The screenshot shows the 'WSC - Editor' window. The 'Editor' tab is active, displaying fields for 'Object Nr' (1), 'Name', 'Description', 'Radio' (Tx Address: 3991, Slot: 0, Channel: 2, Device type: Tx), 'Phone' (Account: 1234, Line: GSM, Channel: 1, Phone: 26632248), 'Transm. test time' (25:00), 'Object test time' (25:00), 'Reminder timeout' (01:00), and 'Mainten. period MM:DD' (00:00). Below these fields are tabs for 'Objects', 'Details', 'Zone', 'Events', 'TLF Events', 'Work Schedule', 'Hardware', and 'Notes'. The 'Events' tab is selected, showing a table of events. The table has columns: NR, Partition Nr, Event code, M, T, Message, rEv, and R. The events listed are: 1, ??, R3840??, R, Wireless zone [E] battery OK; 1, ??, R4000??, A, Armed by RCU [E]; 1, ??, R4010??, A, Armed by user [E]; 1, ??, R4030??, A, AutoArm by timer [E]; 1, ??, R5700??, E, Zone [E] unbypass; 1, ??, R5710??, E, Fire zone [E] unbypass; 1, ??, R5720??, E, 24Hr zone [E] unbypass; 1, ??, R5730??, E, Burglary zone [E] unbypass; 1, ??, R6040??, E, End of fire test. User [E]; and 1, ??, R6070??, E, End of walk test. User [E]. At the bottom, there is a status bar with various icons and a legend: P-Panic, F-Fire, B-Bur, T-Trbl, W-PWR, A-Arm, D-DArm, R-Restore, E-Event, S-Tst.

NR	Partition Nr	Event code	M	T	Message	rEv	R
1	??	R3840??		R	Wireless zone [E] battery OK		N
1	??	R4000??		A	Armed by RCU [E]		N
1	??	R4010??		A	Armed by user [E]		N
1	??	R4030??		A	AutoArm by timer [E]		N
1	??	R5700??		E	Zone [E] unbypass		N
1	??	R5710??		E	Fire zone [E] unbypass		N
1	??	R5720??		E	24Hr zone [E] unbypass		N
1	??	R5730??		E	Burglary zone [E] unbypass		N
1	??	R6040??		E	End of fire test. User [E]		N
1	??	R6070??		E	End of walk test. User [E]		N

Radio block is not used and may be left unfilled.

In the **Phone** block you must enter the following RT4-5GL parameters.

Account – Device account. Every device must have its own unique account.

Channel – number of the receiving (IP Client).

Line – must be set as GSM

Phone – Phone number of the RT4-5GL. Without international code.

Transm.test time – must be set as 00:00.

Object test time – RT4-5GL/security panel test period

Reminder timeout – with this time period not restored alarm events from the “Alarm list” window will be repeated.

Into the **TLF Events** tab you have to load RT4-5GL code card and, depending on the panel connected, add corresponding card.

Request status and settings commands

For the status and settings request there are 5 commands:

99.C1 — GPRS connection settings request. Reply has the following appearance:

V:3420, IP1:0.0.0.0, PORT1:923, IP2:0.0.0.0, PORT2:924, ForceOff:1

V: - Module firmware version.

IP1: - Main IP address.

PORT1: - Main TCP port.

IP2: - Backup IP address.

PORT2: - Backup TCP port.

ForceOff: - Force offline mode. 0 — don't go offline, 1 — go offline if battery low, 2 — go offline if AC lost, 3 - go offline if battery low or AC lost.

99.C2 — general settings request. Reply has the following appearance:

V:3420, TestTime:144, QTime: 15s, RTime: 2m, IpRTime: 60m, GprsAtt: 2, SIA IP: OFF, LNr:8, OUT1: General, OUT2: General

V: - Module firmware version.

TestTime: - Test message period*10 minutes.

QTime: - Connection test period in GPRS.

RTime: - Time between attempts to connect to server.

IpRTime — Time between attempts to return to main IP.

GprsAtt – Number of attempts to establish GPRS connection.

SIA IP: - SIA IP mode status. Not available in current version.

LNr: - Number of digits to determine phone number.

OUT1: - First output working mode.

OUT2: - Second output working mode.

99.C3 — GSM network status and settings request. Reply has the following appearance:

MV:3420; CSQ: 30,0; COPS: 0,0,"LMT GSM"; CGREG: 1,1; SIM1:(L:, P:, APN:internet.lmt.lv), SIM2:(L:, P:, APN:internet.lmt.lv)

V: - Module firmware version.

CSQ: - GSM signal strength. Acceptable level 15-20, good – 20–30.

COPS: - Mobile operator.

CGREG: - GPRS service availability. Must be 1,1 when available.

SIM1: - GSM settings for the main SIM card (Login, Password, APN).

SIM2: - GSM settings for the backup SIM card (Login, Password, APN).

99.C4 — Module status request. Reply has the following appearance:

V:3420, Mode: panel, SIM1: ACTIVE, SIM2: BACKUP, IN: , OUT: , PanStat: D(1), Users: U1(code) U4 (txt), Security: OFF, SimLock: OFF, Online: ON

V: - Module firmware version.

Mode: - current working mode.

SIM1: - Main SIM status.

SIM2: - Backup SIM status.

IN: - List of inputs that are in alarm state.

OUT: - List of activated outputs.

PanStat: - Status (only in control panel mode). D - disarmed, A — armed, StayA — armed in STAY mode. In brackets is shown number of user that changed the status last.

Users: - List of registered users. In brackets shown message format: text or codes.

Security: - Security mode. Turned on/turned off.

SimLock: - SIM card lock in module. Turned on/turned off.

Online: - Current online status.

99.C5 – E-mail sender status. Reply has the following appearance:

MMOn, **SA:** com.lmt.lv, **SP:** 25, **L:** , **A**Off, **SN:**RT4-5GL, **SM:**GC@cortex.lv, **M:**info@cortex.lv

MM – E-mail sender status: On/Off.

SA: - SMTP server address.

SP: - SMTP server TCP port.

L: - Mail server login.

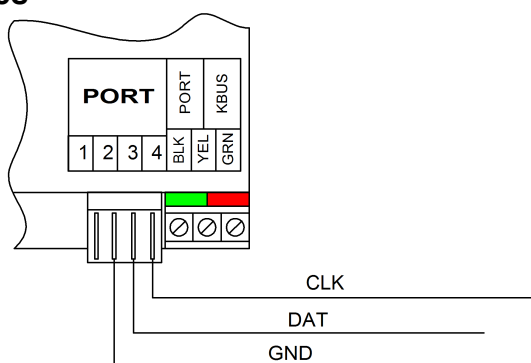
A – Authentication status: On/Off.

SN: - Sender name.

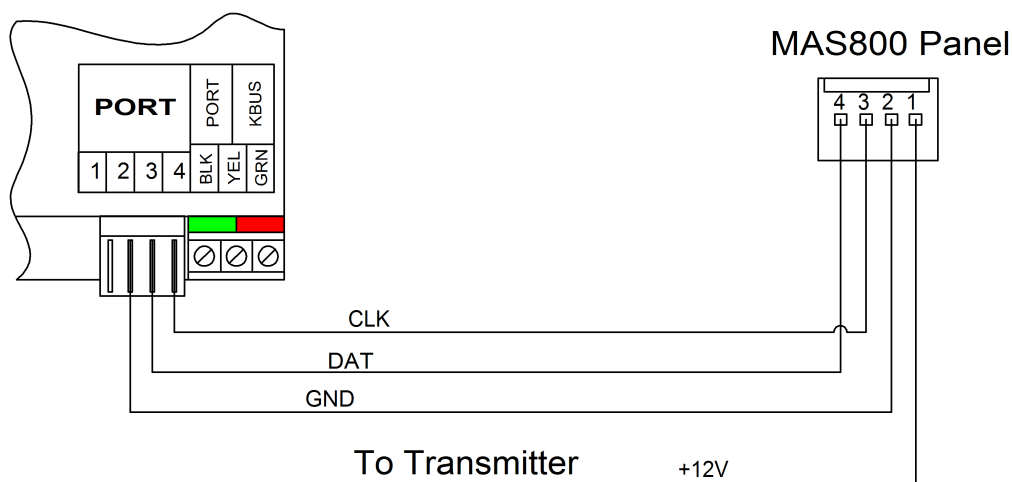
SM: - Sender's e-mail.

M: - Target e-mail address

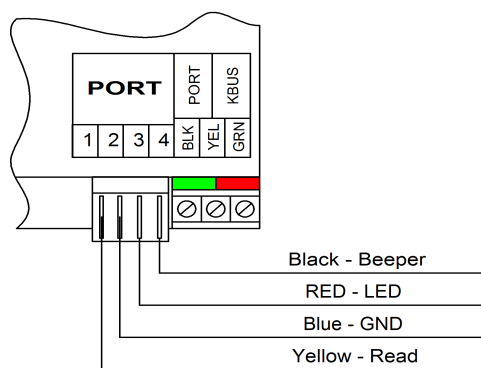
Connecting external devices



Connecting interface modules with Serial BUS support (1-st mode)

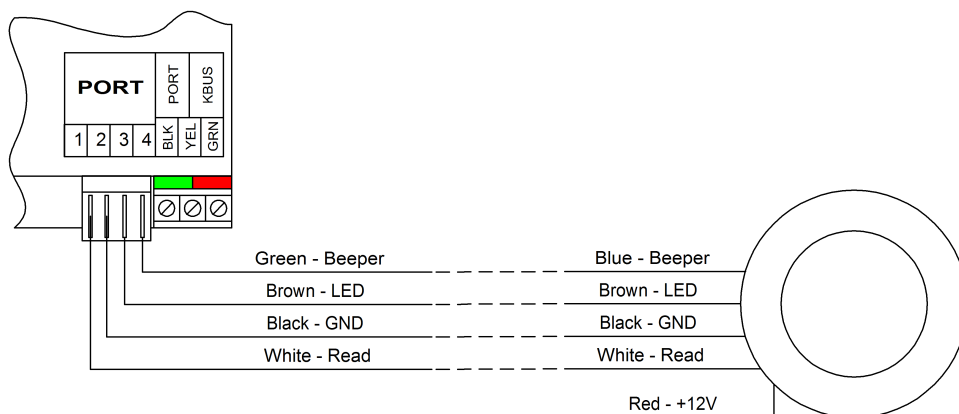


Connecting security panel of the MAS800 system(1-st mode)

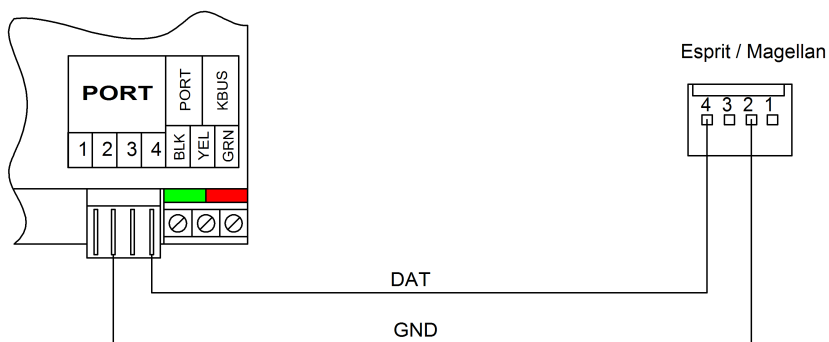


Connecting the key reader in control panel mode (2-nd mode)

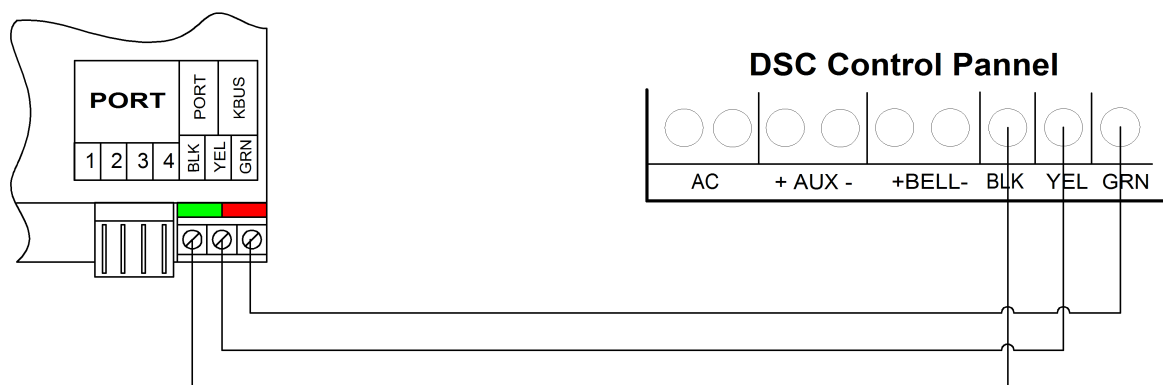
Attention! Depending on reader model, wire colors may vary



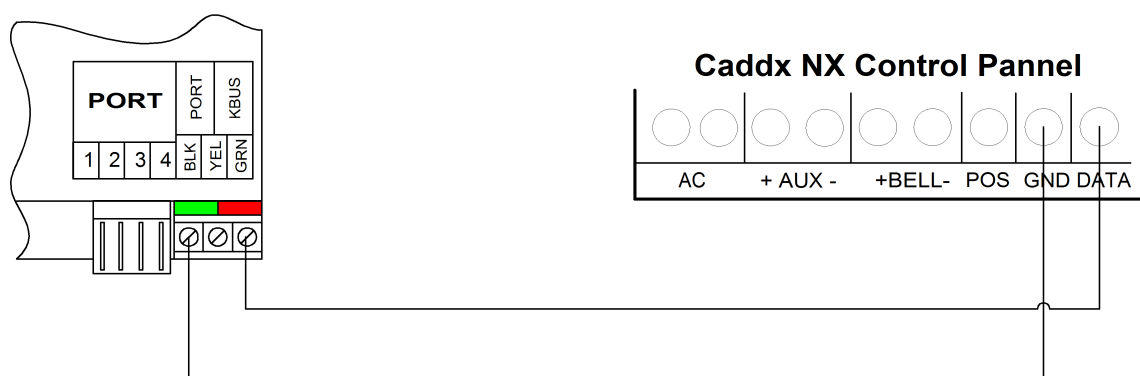
Connecting proximity reader in control panel mode (2-nd mode)



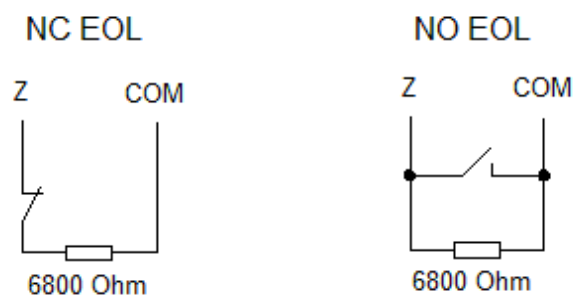
Connecting Esprit, Magellan and Digiplex control panels (4-th, 5-th and 8-th modes)



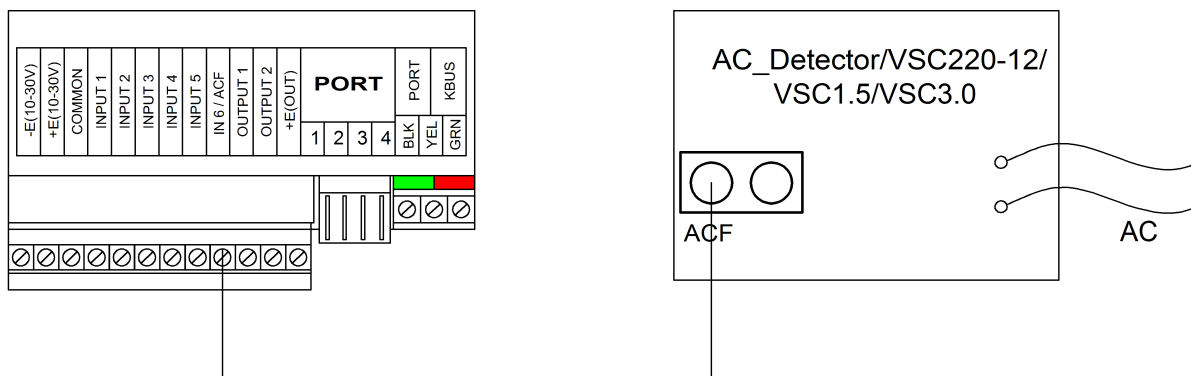
Connecting to the Key-BUS of the DSC control panel (6-th and 7-th modes)



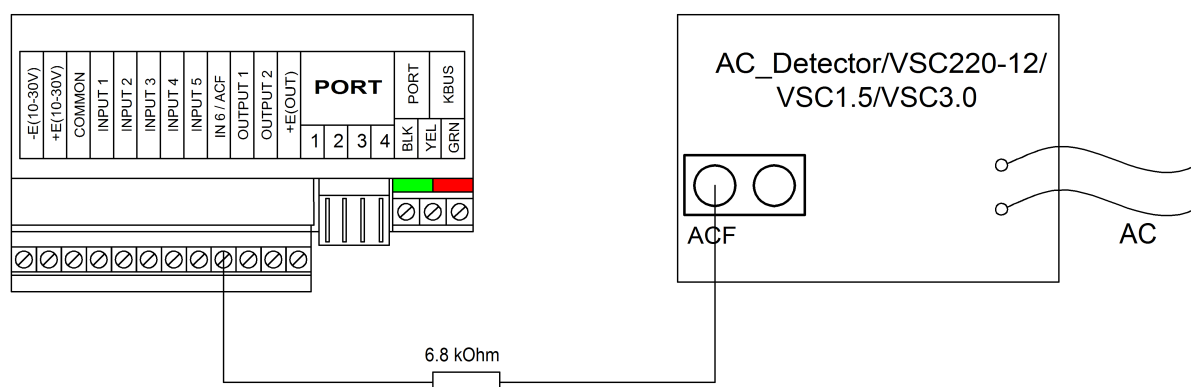
Connecting CADDX NX control panels (9-th mode)



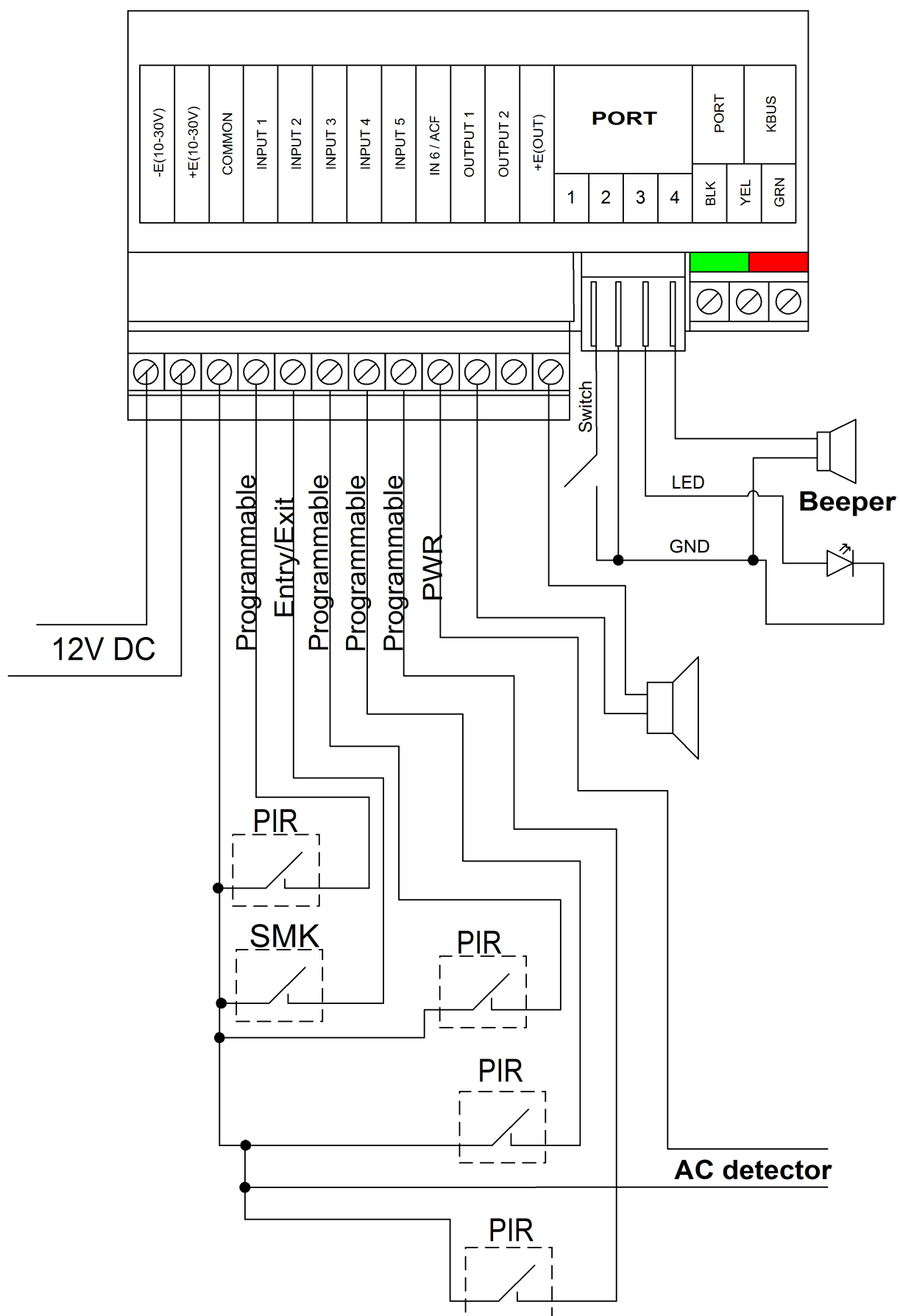
Zone wiring in EOL loop mode



ACF input connection in NC mode



ACF input connection in NC/EOL mode



Connecting external devices in control panel mode (2-nd mode)
Attention! Passive piezoelectric beeper must be connected to the reader.

Enclosure 1. Terminal block pins.

Pin	Name	I/O	Description
1	-E(10-30V)	I	Power supply 10-30V
2	+E(10-30V)	I	
3	COMMON		Common
4	INPUT1	I	Alarm input 1
5	INPUT2	I	Alarm input 2
6	INPUT3	I	Alarm input 3
7	INPUT4	I	Alarm input 4
8	INPUT5	I	Alarm input 5
9	IN6/ACF	I	Power supply control input
10	OUTPUT1	O	General output 1
11	OUTPUT2	O	General output 2
12	+E(OUT)		Power output for connecting interface devices

Enclosure 2. Module control commands.

Command	Description	Reply	By default allowed to:
*	Change message format	/Status/ ¹	Everybody
0	Request status	/Status/	Everybody
1	Activate Out 1	E802001	U1, U2 ²
2	Deactivate Out 1	R802001	U1, U2
1.xxx	Activate Out 1 on time (xxx – minutes)	E802001	U1, U2
3	Activate Out 2	E802002	U1, U2
4	Deactivate Out 2	R802002	U1, U2
3.xxx	Activate Out 2 on time (xxx – minutes)	E802002	U1, U2
081.xxxx	Restart module (xxxx – security code)	R308000	U1
85	Restart GPRS mode to apply new settings (only in GPRS mode)	---	Server
10.xxxx	Remote arming in STAY mode (in control panel mode)	Depending on the result ³	U1
11.xxxx	Remote arming (in control panel mode)	Depending on the result ³	U1
12.xxxx	Remote disarming (in control panel mode)	E840016	U1

Notes:

1. Status is a list of all active modes and alarms.
2. U1, U2, U3, U4 – User numbers; U1 – Master
3. See paragraph «Remote arming and disarming».

Enclosure 3. Module service commands.

Command	Description	Reply	By default allowed to:
00.xxxx	Set current state as normal (xxxx – module security code)	/Status/	U1
81	Request master phone number	/TLF number/	U1
82	Request 2-nd user phone number	/TLF number/	U1
83	Request 3-rd user phone number	/TLF number/	
84	Request 4-th user phone number	/TLF number/	
92	Delete 2-nd user phone number	E801000	U1
93	Delete 3-rd user phone number	E801000	U1
94	Delete 4-th user phone number	E801000	U1
91.xx...xx¹	Change master phone number	E801000	U1
92.xx...xx	Change 2-nd user phone number	E801000	U1; U2
93.xx...xx	Change 3-rd phone number	E801000	U1; U3
94.xx...xx	Change 4-th user phone number	E801000	U1; U4
95.xxxxyyyy	Change module account xxxx – security code, yyyy – new account	E803000	U1
96.xxxxyyyy	Change security code xxxx – old code, yyyy – new code	E803000	U1
87.xxxx	Turn on GPRS-mode (xxxx - module security code)	Depending on the result ³	U1
99.CddMMyyhhmmss²	Set time and date (dd – day, MM – month, yy – year, hh – hours, mm – minutes, ss - seconds)	E801000	U1
99.Wxxxx	Set module online ID. xxxx – identifier (15 digits max.)	E801000	U1
99.Txxx	Set test period (xxx – time *10 minutes. Max. - 255)	E801000	U1
99.I<IP>	Set main server IP-address	E801000	U1
99.II<IP>	Set backup server IP-address	E801000	U1
99.DI<IP>	Set DNS-server IP-address (if used) ⁴	E801000	U1
99.DD<domain name>	Set domain name (if used)	E801000	U1
99.A<access point>	Set APN for main SIM card	E801000	U1
99.AA<access point>	Set APN for backup SIM card	E801000	U1
99.P<port>	Set main server TCP port	E801000	U1
99.PP<port>	Set backup server TCP port	E801000	U1
99.R<min>	Time between attempts to return to main IP	E801000	U1
99.O<sec>	GPRS channel test period Min - 15. Max - 255	E801000	U1
99.M<min>	Time between attempts to reconnect to server Max - 255	E801000	U1
99.Y1<login>	Set login for main SIM GPRS service Max – 8 symbols	E801000	U1
99.Y2<password>	Set password for main SIM GPRS service Max – 8 symbols	E801000	U1
99.YY1<login>	Set login for backup SIM GPRS service Max – 8 symbols	E801000	U1

Command	Description	Reply	By default allowed to:
99.YY2<password>	Set password for backup SIM GPRS service Max – 8 symbols	E801000	U1
99.E1	Turn on E-mail sender	E801000	U1
99.E0	Turn off E-mail sender	E801000	U1
99.Nx	Set number of symbols for number recognition. Max - 16	E801000	U1
99.C1	Show module online configuration	/Configuration/	U1
99.C2	Show module general configuration	/Configuration/	U1
99.C3	Show operator and GSM-signal strength ⁵	/Configuration/	U1
99.C4	Show user configuration, current working mode, input and output status and configuration	/Configuration/	U1
99.C5	Show E-mail sender configuration	/Configuration/	U1

Notes:

1. It is recommended to register phone numbers with the international code. If international code is used than it must contain «+» before it (for example, Latvia: +371xxxxxxx, Estonia: +372xxxxxxx, Russia: +7xxxxxxxxxxx). Maximum phone length – 15 digits.
2. Date and time are added to every message. To receive the correct time you either have to activate GPRS mode or send this SMS-message.

Attention! After restarting module time and date will be lost and you will have to set them again.

3. See paragraph «Working in GPRS mode».
4. If you need to stop using domain name and start using IP-address again, just delete DNS-server IP-address. You can do so by sending 99.DI message.
5. Acceptable level 15-20, good – 20–30

Enclosure 4. Module events.

Event code in WinSC software	SMS-message on mobile phone (by default)	Description	By default sent to:
E802001	OUT 1 activated	Out 1 activated	Command sender
E802002	OUT 2 activated	Out 2 activated	Command sender
R802001	OUT 1 deactivated	Out 1 deactivated	Command sender
R802002	OUT 2 deactivated	Out 2 deactivated	Command sender
E803000	Code changed	Account/Security code changed	Command sender
E830001	Alarm zone 1	Alarm zone 1	U1, U2
E830002	Alarm zone 2	Alarm zone 2	U1, U2
E830003	Alarm zone 3	Alarm zone 3	U1, U2
E830004	Alarm zone 4	Alarm zone 4	U1, U2
E830005	Alarm zone 5	Alarm zone 5	U1, U2
E830006	AC lost	AC lost	U1
E822000	Battery low	Battery low	U1
E804000	Check bat or power	Forced exit from GPRS mode	U1
E801000	Configuration changed	Module configuration changed	Command sender
E854001	GPRS 1 error	Main SIM failed to establish GPRS connection	U1
E854002	Online 1 error	Failed to connect to main IP address	U1
E854003	GPRS 2 error	Backup SIM failed to establish GPRS connection	U1
E854004	Online 2 error	Failed to connect to backup IP address	U1
E855001	SIM 1 error	Main SIM failure	
E855002	SIM 2 error	Backup SIM failure	
R830001	Restore zone 1	Restore zone 1	U1, U2
R830002	Restore zone 2	Restore zone 2	U1, U2
R830003	Restore zone 3	Restore zone 3	U1, U2
R830004	Restore zone 4	Restore zone 4	U1, U2
R830005	Restore zone 5	Restore zone 5	U1, U2
R830006	AC restored	AC restored	U1
R822000	Battery restored	Battery restored	U1
E823000	Test	Test message	U1
R855001	SIM 1 OK	Main SIM operational	
R855002	SIM 2 OK	Backup SIM operational	
R808000	Ready	Module is ready to work	U1
E829000	Key program mode ON	Key registration mode entry	U1
R829000	Key program mode OFF	Key registration mode exit	U1
R8400xx	Armed by user xx	Armed by user xx	U1
E8400xx	Disarmed by user xx	Disarmed by user xx	U1
R840016	Remote ARM	Module is remotely armed	U1
E840016	Remote DISARM	Module is remotely disarmed	U1
R8410xx	Stay Armed. User xx	User xx armed module in Stay Arm mode	U1
R841016	Remote STAY armed	Module remotely armed in STAY mode	U1

E8410xx	Stay Disarmed. User xx	User xx disarmed module in Stay Arm mode	U1
E8580xx	Guard key xx	Guard xx touched the reader with his key	U1
E821000	Not registered key	Key not registered in the system	
E833020	Port failure	Communication port failure	U1
R833020	Port OK	Communication port restored	U1

Note! Module events are transmitted with partition 99.

Enclosure 5. Event codes for Esprit security panels

Event code	Description
E100000	Auxiliary alarm
E115000	Fire alarm
E120000	Panic
E121000	Duress alarm
E1300xx	Alarm! Zone xx, where xx - zone number
R1300xx	Zone xx restored, where xx - zone number
E1370xx	Tamper alarm! Zone xx, where xx - zone number
R1370xx	Tamper restore. Zone xx, where xx - zone number
E301000	AC fail
R301000	AC restore
E302000	Battery low
R302000	Battery restore
E312000	Power supply over current limit
R312000	Power supply restore
E321000	Bell trouble
R321000	Bell OK
E351000	Telephone line fail
R351000	Telephone line restore
R354000	Communication restore
E373000	Fire zone trouble
R373000	Fire zone restore
E401000	Special disarming
R401000	Special arming
E4010xx	Disarmed by user xx, where xx - user number
R4010xx	Armed by user xx, where xx - user number
E405000	Auto-arm canceled
E406000	Alarm canceled
E421000	Keypad lockout
E452000	Late open/close
E459000	Recent closing

E456000	Partial arming
E5700xx	Zone bypass, where xx - zone number
E602000	Periodic test
E626000	Date/time loss
E625000	Date/time restore
E627000	Programming mode entry

Enclosure 6. Event codes for SP/Magellan security panels

Event code	Description
E100000	Auxiliary alarm
E1000xx	Medical alarm, where xx - user number
E1100xx	Fire zone alarm, where xx - zone number
R1100xx	Fire zone restore, where xx - zone number
E115000	Fire alarm
E120000	Panic
E121000	Duress alarm
E1300xx	Alarm! Zone xx, where xx - zone number
R1300xx	Zone xx restore, where xx - zone number
E1370xx	Tamper alarm. Zone xx, where xx - zone number
R1370xx	Tamper restore. Zone xx, where xx - zone number
E1430xx	Module trouble, where xx - module address
R1430xx	Module restore, where xx - module address
E1450xx	Wireless module tamper alarm, where xx - module address
R1450xx	Wireless module tamper restore, where xx - module address
E301000	AC fail
R301000	AC restore
E302000	Battery low
R302000	Battery restore
E305000	System reset
E308000	System shutdown
E312000	Power supply over current limit
R312000	Power supply restore
E321000	Bell trouble
R321000	Bell restore
E333000	Expansion module trouble
R333000	Expansion module restore
E338000	Expansion module low battery
R338000	Expansion module battery restore
E341000	Expansion module tamper alarm

R341000	Expansion module tamper restore
E342000	Expansion module AC lost
R342000	Expansion module AC restore
E344001	RF jamming
E344002	GSM jamming
R344001	RF restored
R344002	GSM restored
E350000	GSM – no service
E350001	IP – no service
R350000	GSM - service restored
R350001	IP - service restored
E351000	Telephone line 1 fail
R351000	Telephone line 1 restore
E352000	Telephone line 2 fail
R352000	Telephone line 2 restore
E354001	Communication fault (voice report)
E354002	Communication fault IP1 (GPRS)
E354003	Communication fault IP2 (GPRS)
E354004	Communication fault IP1
E354005	Communication fault IP2
R354000	Communication restored
R354001	Communication restored (voice report)
R354002	Communication restored IP1 (GPRS)
R354003	Communication restored IP2 (GPRS)
R354004	Communication restored IP1
R354005	Communication restored IP2
E373000	Fire zone trouble
R373000	Fire zone restore
E3800xx	Sensor trouble, where xx - sensor number
R3800xx	Sensor restore, where xx - sensor number
E381000	Loss of supervision — RF
E381001	Loss of supervision — GSM
E381002	Loss of supervision — IP
R381000	Supervision restore — RF
R381001	Supervision restore - GSM
R381002	Supervision restore – IP
E3840xx	Wireless sensor battery low, where xx - sensor number
R3840xx	Wireless sensor battery restore, where xx - sensor number
E400000	Open after alarm (Winload/keyswitch)

E4000xx	Open after alarm, where xx - user number
R400000	Special closing
E401000	Disarmed (Winload/keyswitch)
E4010xx	Disarmed, where xx - user number
R4010xx	Armed, where xx - user number
R403000	Auto-arming
E405000	Auto-arm canceled
R408000	Quick arm
R409000	Arming using Keyswitch
E406000	Alarm canceled (Winload/keyswitch)
R4060xx	Alarm canceled by user, where xx - user number
E421000	Keypad lockout
E452000	Late open/close
E456000	Partial arming
E4580xx	Disarmed using StayD, where xx - zone number
E459000	Recent closing
E531000	Module added
E532000	Module deleted
E5700xx	Zone bypass, where xx - zone number
E602000	Periodic test
E625000	Date/time restore
E626000	Date/time lost
E627000	Programming mode entry
E628000	Programming mode exit
E654000	System inactivity

Enclosure 7: Key-BUS event codes

Event code	Description
E1300xx	Alarm! Zone xx, where xx - zone number
R1300xx	Zone xx restored, where xx - zone number
E100000	Auxiliary alarm
R100000	Auxiliary alarm restored
E115000	Fire alarm
R115000	Fire alarm restored
E120000	Panic
R120000	Panic restored
E111000	2-wire smoke detector alarm
R111000	2-wire smoke detector restore
E121000	Duress alarm
E139000	Intrusion verify
E143000	Expansion module trouble
R143000	Expansion module restore
E1450xx	Expansion module tamper alarm, where xx — module address
R1450xx	Expansion module tamper restore, where xx — module address
E301000	AC lost
R301000	AC restore
E302000	Battery low
R302000	Battery restore
R305000	System reset (Cold start)
E321000	Bell trouble
R321000	Bell restore
E3330xx	Module fail, where xx - module address
R3330xx	Module restore, where xx - module address
E351000	Telephone line fail
R351000	Telephone line restore
R354000	Communication restore
E373000	Fire zone trouble
R373000	Fire zone restore
E3830xx	Zone xx tamper alarm, where xx - zone number
R3830xx	Zone xx tamper restore, where xx - zone number
E384000	Wireless key battery low
R384000	Wireless key battery restore
E3840xx	Wireless sensor battery low, where xx - sensor number
R3840xx	Wireless sensor battery restore, where xx - sensor number
E400000	Special opening

R400000	Special closing
E4010xx	Disarmed by user xx, where xx - user number
R4010xx	Armed by user xx, where xx - user number
E402040	Disarmed with master code
R402040	Armed with master code
E405000	Auto-arm canceled
E406000	Open after alarm
E421000	Keypad lockout
E459000	Recent closing
E470000	Partial arming
E601000	System test
E602000	Periodic test
E627000	Programming mode entry
E628000	Programming mode exit

Enclosure 8. Event codes for Digiplex security panels

Event code	Description
E100000	Auxiliary alarm
E110xxx	Fire zone alarm, where xxx - zone number
R110xxx	Fire zone restore, where xxx - zone number
E115000	Fire alarm
E120000	Panic
E121xxx	Duress code, where xxx — user number
E130xxx	Alarm, zone xx, where xx - zone number
R130xxx	Restore, zone xx, where xx - zone number
E139000	Police code
E144xxx	Zone tamper alarm xx, where xx - zone number
R144xxx	Zone tamper restore xx, where xx - zone number
E145000	Expansion module tamper alarm
R145000	Expansion module tamper restore
E300000	System failure
E301000	AC lost
R301000	AC restore
E304000	RAM/ROM failure
R304000	RAM/ROM restore
E305000	System reset
E308000	System shutdown
E309000	Battery low

R309000	Battery restore
E321000	Bell trouble
R321000	Bell restore
E333000	Expansion module trouble
R333000	Expansion module restore
E336000	Printer failure
R336000	Printer restore
E338000	Expansion module battery low
R338000	Expansion module battery restore
E342000	Expansion module AC lost
R342000	Expansion module AC restore
R351000	Telephone line 1 fault
E352000	Telephone line 2 fault
R352000	Telephone line 2 restore
E354000	Failed to communicate
R354000	Communication restore
E373000	Fire zone trouble
R373000	Fire zone trouble restore
E381xxx	Sensor trouble, where xx - sensor number
R381xxx	Sensor restore, where xx - sensor number
E384xxx	Wireless sensor low battery, where xx - sensor number
R384xxx	Wireless sensor battery restore, where xx - sensor number
E400000	Open after alarm (Winload/keyswitch)
E400xxx	Open after alarm, where xx - user number
E401xxx	Disarmed by user xx, where xx - user number
R401xxx	Armed by user xx, where xx - user number
R403000	Auto-arming
E406000	Cancel alarm (Winload/keyswitch)
E406xxx	Cancel alarm, user xx, where xx - user number
R407000	Remote arming
E407000	Remote disarm
R408000	Quick arm
R409000	Armed using Keyswitch
E409000	Disarmed using Keyswitch
E421000	Kepad locked
E429000	Programming mode entry using Winload
E430000	Programming mode exit using Winload
E451xxx	Early open, user xx, where xx - user number
R451xxx	Early close, user xx, where xx - user number

R452000	Late close
E452xxx	Late close, user xx, where xx - user number
R452xxx	Late open, user xx, where xx - user number
E456000	Partial arming
R459000	Recent close
E464000	Auto-arming canceled
E531xxx	Module xx added, where xx - module number
E532xxx	Module xx removed, where xx - module number
E570000	Zone forced
E570xxx	Zone xx bypass, where xx - zone number
E602000	Test message
R625000	Date/time restored
E626000	Date/time fail
E627000	Programming mode entry
E628000	Programming mode exit
E654000	System inactivity

Enclosure 9. Event codes for CADDX NX security panels

E301xxx	AC lost where xx - module number
R301xxx	AC restore where xx - module number
E601xxx	Manual test where xx - module number
E602001	Autotest
E312xxx	Power supply over current limit where xx - module number
R312xxx	Power supply restored where xx - module/zone number
E137xxx	Tamper alarm, where xx - module/zone number
R137xxx	Tamper restore, where xx - module number
E570xxx	Zone bypass, where xx - zone number
R570xxx	Zone restored where xx - zone number
E406xxx	Cancel alarm where xx - user number
E401xxx	Disarmed by user xx where xx - user number
R401xxx	Armed by user xx where xx - user number
E412001	Download successful
E393001	CleanMe alarm
R393001	CleanMe restore
E121001	Duress code entered
E451001	Early open/close
E627001	Programming mode entry
E628001	Programming mode exit
E605000	Event log overflow

E457xxx	Exit error, user xx where xx - user number
E333xxx	Module trouble where xx - module number
R333xxx	Module restore where xx - module number
E454001	Failed to arm
E354001	Fail to communicate
E423001	Forced door
R423001	Forced door restore
E310001	Ground failure
R310001	Ground restore
E100001	Auxillary alarm (Keypad)
E110001	Fire alarm (Keypad)
E120001	Panic (Keypad)
E121001	Silent panic
E309001	Battery low
R309001	Battery restore
E381xxx	RF sensor xx lost where xx - zone number
R381xxx	RF sensor xx restore where xx - zone number
E384xxx	Sensor xx battery low where xx - zone number
R384xxx	Sensor xx battery restore where xx - zone number
E321xxx	Bell trouble where xx - module number
R321xxx	Bell restore where xx - module number
E351001	Telephone fault
R351001	Telephone restore
E391xxx	Zone xx activity fault where xx - zone number
R391xxx	Zone xx activity restore where xx - zone number
E380xxx	Zone xx trouble where xx - zone number
R380xxx	Zone xx restore where xx - zone number
E122001	Silent panic
R122001	Silent panic restore
E130xxx	Burglary! Zone xx, where xx - zone number
R130xxx	Burglary restore zone xx, where xx - zone number
E131xxx	Perimeter alarm zone xx, where xx - zone number
R131xxx	Perimeter restore zone xx, where xx - zone number
E132xxx	Interior alarm zone xx, where xx - zone number
R132xxx	Interior restore zone xx, where xx - zone number
E133xxx	24H alarm zone xx, where xx - zone number
R133xxx	24H restore zone xx, where xx - zone number
E134xxx	Entry alarm zone xx, where xx - zone number
R134xxx	Entry restore zone xx, where xx - zone number

E135xxx	Day/night alarm zone xx, where xx - zone number
R135xxx	Day/night restore zone xx, where xx - zone number
E150xxx	24H non-burglary alarm zone xx, where xx - zone number
R150xxx	24H non-burglary restore zone xx, where xx - zone number
E123xxx	Audible panic alarm zone xx, where xx - zone number
R123xxx	Audible panic restore zone xx, where xx - zone number
E151xxx	Gas detected! Zone xx, where xx - zone number
R151xxx	Gas restore zone xx, where xx - zone number
E154xxx	Water leakage zone xx, where xx - zone number
R154xxx	Water restore zone xx, where xx - zone number
E140xxx	General alarm zone xx, where xx - zone number
R140xxx	General restore zone xx, where xx - zone number
E158xxx	High temperature alarm zone xx, where xx - zone number
R158xxx	High temperature restore zone xx, where xx - zone number
E159xxx	Low temperature alarm zone xx, where xx - zone number
R159xxx	Low temperature restore zone xx, where xx - zone number
E115001	Manual fire alarm
R115001	Manual fire restore