



RT4-5WF object device

User manual

General information

RT4-5WF object device is designed for gathering information from the security panel, it's processing and transmitting to the Central Unit via Ethernet using Wi-Fi network.

Device has two general purpose inputs, AC control input and two outputs, that can function either like PGMs or activated outputs..

Device communication port is designed for connecting different kinds of security panels and gathering full information from them.

RT4-5WF module has 6* switchable working modes:

- 1 — working via Serial BUS protocol
- 2 — working with Esprit control panels
- 3 — working with Magellan control panels
- 4 — working with one- and two-partition DSC panels using Key-BUS protocol
- 5 — working with multi-partitioned DSC panels using Key-BUS protocol
- 6 — working with Digiplex control panels

RT4-5WF also monitors it's power level and transmits alarm message to the Central Unit if power level is lowered.

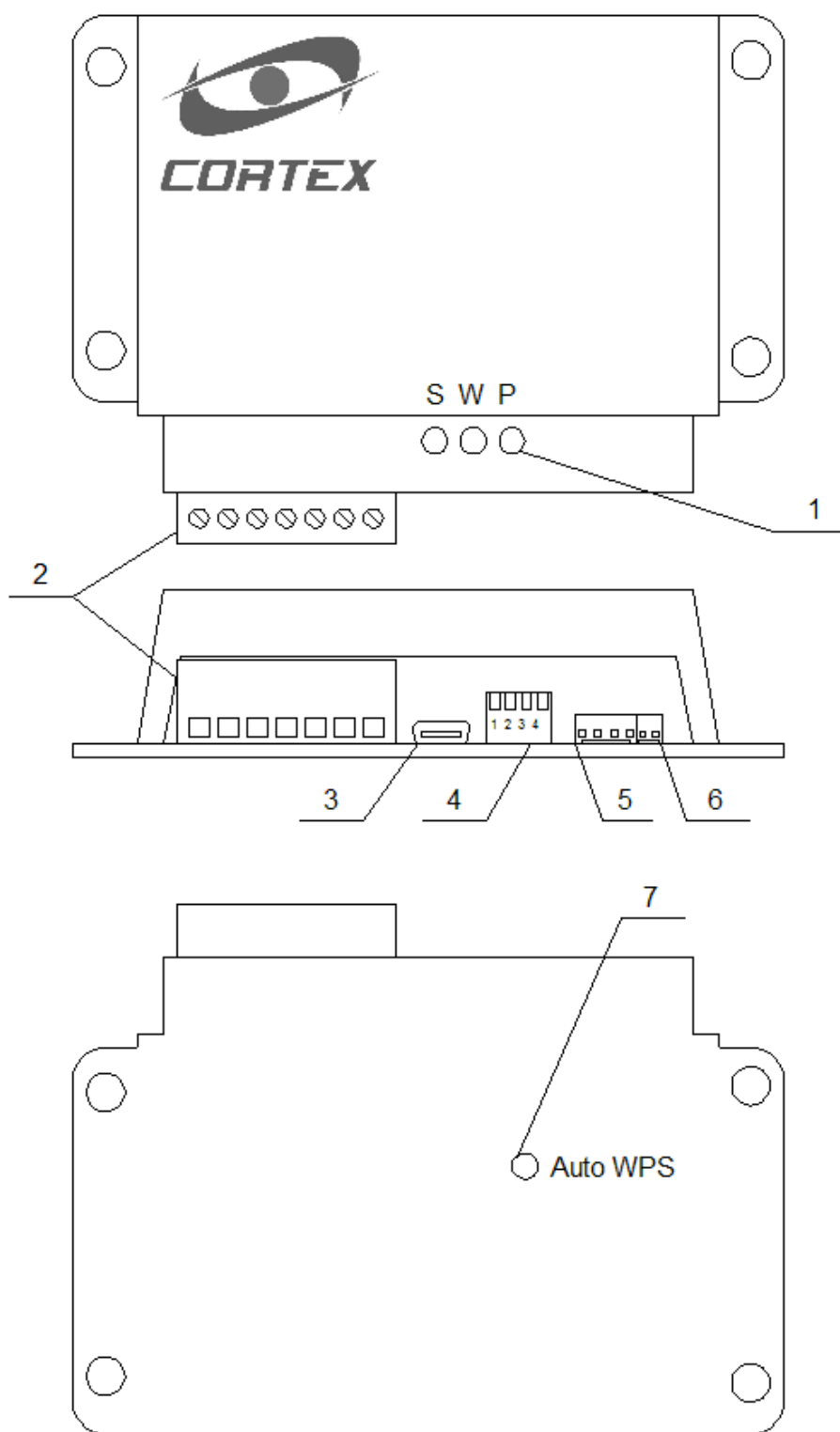
Device features

- Information transmitting via Ethernet using Wi-Fi network;
- Ability to connect to Wi-Fi networks that use different types of encryption and authentication.
- Event log (up to 254 events);
- USB-port for device programming;
- Ability to remotely configure module parameters via Ethernet;
- Working mode and Wi-Fi signal strength indication;
- Power supply status and data transmitting indication;
- 2 general purpose inputs;
- Power supply monitoring input;
- 2 programmable outputs;
- Communication port for Security panels connection;
- Periodic channel test;

Technical information

Supported encoding algorithms	WEP-H, WEP-A, TKIP, AES
Supported authentication types	Shared, WPA2PSK, WPA2PSK
Wireless standard	802.11 b/g/n
Frequency range	2.412GHz-2.484GHz
Output capacity	1A
Max. voltage on closed input	15V
Max. voltage on output	15V
Power supply	11 – 15V
Input current	no more than 50mA
Dimensions	120x80x30 mm

Module appearance



1. Indication LEDs
2. Terminal block for power supply and external device connection
3. USB-port for module programming
4. Dip-Switch for switching working mode
5. Communication port for security panel connection
6. Backup transmitter connector
7. Button for connecting to the router in WPS mode

Device inputs and outputs

Device general inputs are loaded to «+» (react to «0»/«break» signals).

By default both general inputs are programmed as NO.

AC monitoring input is loaded to «+» (reacts on «0»/«break» signals) and programmed as NC.

If you need to change input type (NC/NO), you have to connect all external device, make sure all inputs 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.

Maximum input voltage - **+15V**.

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

Manually activated output is activated and deactivated by the command, sent from the TLF_Server software. You can also activate output for a set number of seconds.

PGM-output can react to the following troubles:

- One of the general purpose inputs is in the alarm state;
- Input voltage is lower than normal;
- Cannot connect to server or cannot establish connection with the router.

Outputs are configured using USB_Reader software. By default both outputs are programmed as manually activated.

Indication

S indicator	
Off	Module not ready to work
Green	Module is ready to work
Blinks green fast	Message is being transmitted
Blinks green once a second	Low voltage
Red	Module in programming mode
W indicator	
Green. Flashing once every 2-3 seconds	Connected to the router and connected to the TLF_Server software. Wi-Fi signal at high level
Yellow. Flashing once every 2-3 seconds	Connected to the router and connected to the TLF_Server software. Wi-Fi signal at medium level
Red. Flashing once every 2-3 seconds	Connected to the router and connected to the TLF_Server software. Wi-Fi signal at low level
Flashing green once every 2-3 seconds	Connected to the router but not connected to the TLF_Server software. Wi-Fi signal at high level
Flashing yellow once every 2-3 seconds	Connected to the router but not connected to the TLF_Server software. Wi-Fi signal at medium level
Flashing red once every 2-3 seconds	Connected to the router but not connected to the TLF_Server software. Wi-Fi signal at low level
Flashing red once per second	Cannot connect to router. Check device settings.
P indicator	
Indication in Serial BUS mode	
Flashes yellow	Transmitting information via communication port
Indication in Esprit, Magellan and Digiplex modes	
Flashes yellow	Transmitting information via communication port
Indication in DSC 1 and DSC 2 modes	
Flashes yellow	Transmitting information via communication port
Blinks yellow fast	No communication with security panel. Check wiring and working mode

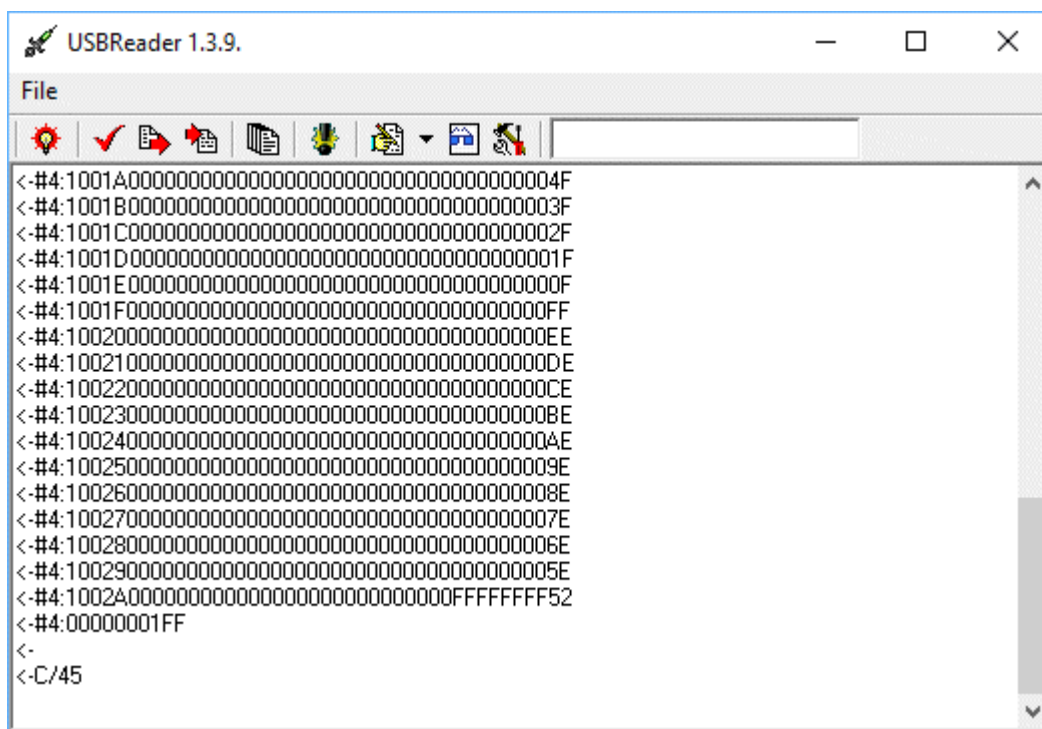
Programming

Programming using USB

In order to program device parameters You will need **USB_Reader** software version **1.3.9** or higher.

USB_Reader software: general information

USB_Reader software is designed for programming module parameters, configuring user permissions and message sending addresses, event log downloading, and code table uploading. Main software window is shown below.



Software main window.

Getting ready for programming and software configuration

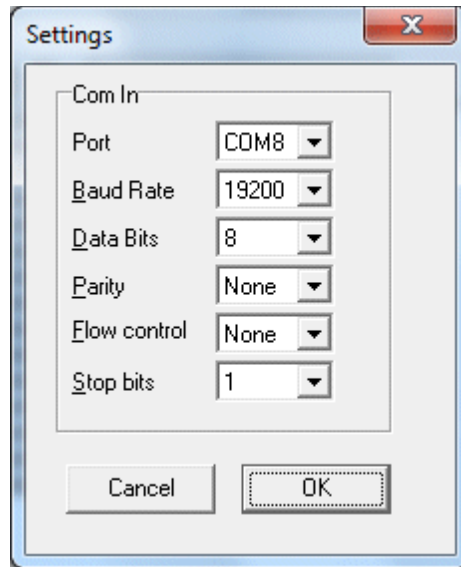
Device programming is made using **USB_Reader** software via PC USB-port.

When You are connecting device to the PC for the first time, You will have to install drivers, so device would be recognised correctly.

When You connected the device to the PC, operating system might ask You to install drivers. In that case, You have to select the option to manually select the drivers and select the path to the **drv** folder. After the drivers are installed, You can start device programming.

To activate device programming mode, simply connect it to the USB-port. After **S** indicator turns red, you can start device programming.

In software settings You will need to specify number of the port that will be used to connect to the module. Settings window can be opened by pressing  icon (Settings).



Port settings window.

In this window You have to choose port number that will be used to connect to the module. It is recommended to leave other options in the default state as shown in the picture.

It is recommended that port number would be lower than 10. If by default port number was set higher than 10, you can change it in the “Device manager”.

If connection to the module was successful, “Ready” icon will look the following way: . Otherwise it will look like this: .

USB_Reader software: Event log download.

Using the software, You can download device event log for further processing.

Log contains up to 254 events. To download log, press  icon. Than specify the path to the folder, where you want to save you .log file, choose a name for it and press **Save**.

To open saved file, press  icon and specify a specify the path to the file.

USB_Reader software: event table upload.

In case You need to update the code tables for security panels information decoding, You have to use  icon. After You pressed it, specify the path to the .hex file that was provided by the developer and press **Open**.

USB_Reader software: module programming

Module programming is initiated from the main menu File/Read or by pressing  icon. When initiated, all the current settings are downloaded from the module and displayed in the programming window. Programming window consists of three tabs:

- General settings – general module parameters
- Advanced settings – additional module parameters
- Security – activation and change of the security code

After you finished configuring module parameters, press OK. In that case, new parameters will be saved into module. To save this configuration into the file, press Save and specify file name and save path. To load previously saved configuration file, press Load and select the file to load parameters from. Load and Save commands are only available when programming window is active (before You press OK).

General settings tab:

In this tab You can configure module account and Online ID, server address and Wi-Fi settings. Parameter description is given in the table below.

Parameter	Default value	Description
Module account	1234	Module account, used for it's identification in WinSC software. Must be unique for every module.
Online ID	11111111	Module account, used for it's identification in TLF_Server software. Must be unique for every module.
TCP port	925	Server TCP pot
TCP port reserved	Not specified	Backup server TCP port
Server IP	0.0.0.0	Server IP address
Server IP reserved	Not specified	Backup server IP address
Domain Name	Not specified	Server domain name
DNS Server IP	Not specified	DNS server IP address
Encryption algorithm	None	Encryption algorithm, used by router
Authentication mode	Open	Authentication mode, used by router.

Parameter	Default value	Description
Checkbox Auto	activated	If active, module automatically detects router encryption algorithm and authentication method. If selected, two previous options become inactive.
Wi-Fi password	Not specified	Password for connecting to Wi-Fi network.
APN	Not specified	Wi-Fi network name. Case sensitive.
Module status	-	Information field. Shows current module connection status.
IP Config method	DHCP	Way of obtaining IP address. If chosen "STATIC", next three options become active.
LOCAL IP	Not specified	Device IP address in local network
SUBNET_MASK	Not specified	Used Subnet mask
GATEWAY	Not specified	Used Gateway

Module status field can show five different statuses:

WfOK(xx)/ServOK – module connected to the router and to the TLF_Server software. xx – Wi-Fi signal level in percentages.

WfOK(xx)/ServErr – module connected to the router but failed to connect to the TLF_Server software. xx – Wi-Fi signal level in percentages.

ApnOK/WfErr – Failed to connect to Wi-Fi network. Check password, authentication method and encryption algorithm.

ApnNotFound – Wi-Fi network with the specified name not found.

NoInf – no data. Module didn't receive any information about Wi-Fi networks.

Advanced settings tab:

In this tab You can configure output functions and additional module parameters.
Parameter description is given in the table below.

Table 2. Advanced module settings.

Parameter	Default value	Description
Firmware version	-	Firmware version. Information field.
EEPROM ID	-	Internal firmware version. Information field.
Zones response time	500 msec.	Input reaction time for status change.
Test time value	24 h	Time between periodical test messages.
Bat low const.	140 a.u.	Voltage value (in arbitrary units) that determines the low battery state. When lower - "Low battery" message is generated.
Bat norm const.	160 a.u.	Voltage value (in arbitrary units) that determines the normal battery state. When higher - "Battery restored" message is generated.
OUT1 Config	User controlled	First output function configuration.

Parameter	Default value	Description
OUT2 Config	User controlled	Second output function configuration.
Query time in online	15 sec	Channel test period, while connected to TLF_Server
Attempts to send a message	2	Number of attempts to send a message. If failed, message is kept in the memory and will be transmitted together with the next message.

In the **OUT1 config** block are specified function of the first output (**OUT1**). Four options are available:
General output – Output works in the general purpose mode and can be activated/deactivated by the command sent from the TLF_Server software.

Alarm – Output works in PGM mode and is activated when one of the inputs is in the alarm state.

Bat - Output works in PGM mode and is activated when module input voltage becomes lower than normal.

Connection - Output works in PGM mode and is activated when module failed to connect to the TLF_Server or router.

In the **OUT2 config** block are specified function of the second output (**OUT2**). Four options are available:

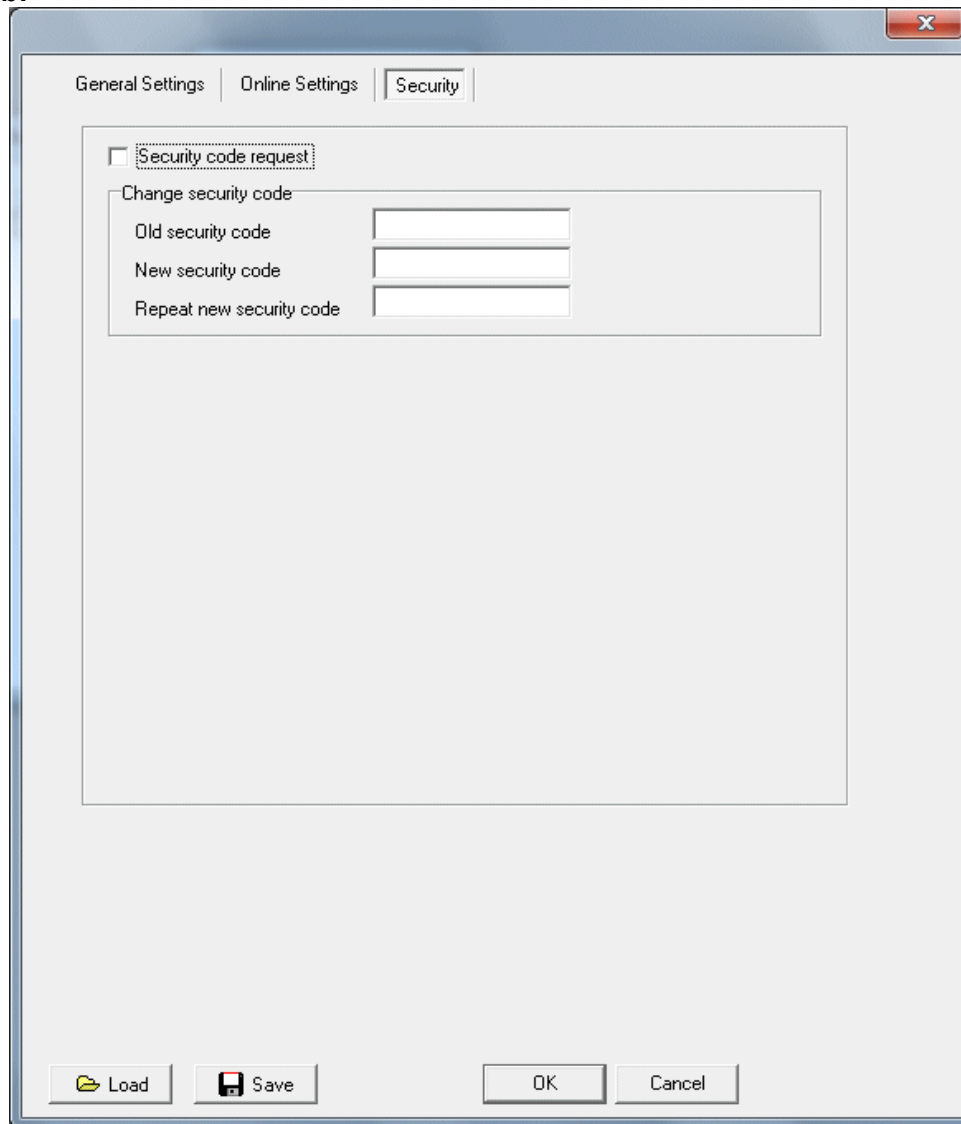
General output – Output works in the general purpose mode and can be activated/deactivated by the command sent from the TLF_Server software.

Alarm – Output works in PGM mode and is activated when one of the inputs is in the alarm state.

Bat - Output works in PGM mode and is activated when module input voltage becomes lower than normal.

Connection - Output works in PGM mode and is activated when module failed to connect to the TLF_Server or router.

Security tab:



The screenshot shows a software settings window with three tabs: "General Settings", "Online Settings", and "Security". The "Security" tab is selected. Inside the "Security" tab, there is a checkbox labeled "Security code request". Below this checkbox is a section titled "Change security code" which contains three input fields: "Old security code", "New security code", and "Repeat new security code". At the bottom of the window, there are four buttons: "Load" (with a floppy disk icon), "Save" (with a floppy disk icon), "OK", and "Cancel".

In this tab You can activate security code request and change security code.

Security code request checkbox, when active, will activate security code request when trying to configure module parameters with the **USB_Reader** or **TLF_Server** software.

Change security code area is used to change security code:

Old security code – current security code (default - 1234)

New security code – new security code

Repeat new security code – repeat new security code

USB_Reader software: configuration template creation

Software allows creating configuration file without directly connecting the module to the PC. To do so, press  icon and choose **WF (Wi-Fi)** option.

After that, software will open window that is identical to the window that is described in the **“USB_Reader software: module programming”** paragraph. The only difference is that all the parameters will have zero value.

After configuring all parameters as you need, save module configuration into the file by pressing **Save** and specifying file name and path.

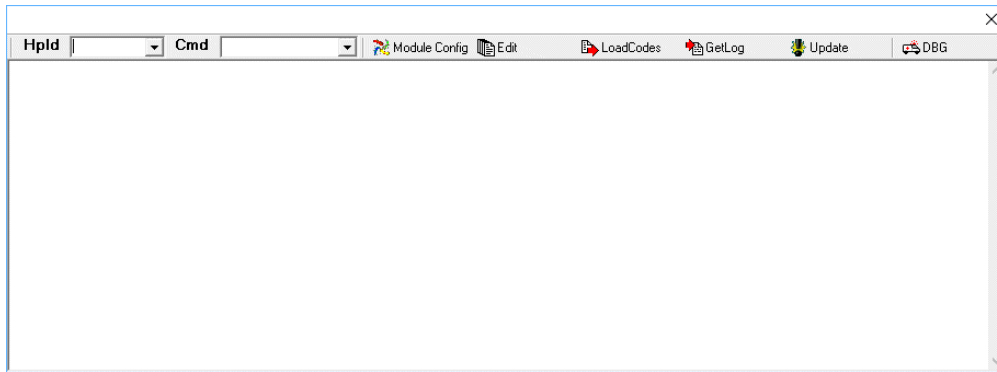
To load previously saved configuration file, press **Load** and select the file to load parameters from.

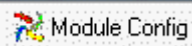
Remote programming

For remote programming you must use TLF_Server software.

TLF_Server software: module programming.

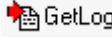
To start module programming, in the main program window You must press  icon. Device control window will open:



In this window, press  icon, and in RPT_ID drop-down menu select Online ID of the module You wish to configure and press OK. After that a configuration window will open, that is fully identical to the window described in the “**USB_Reader software: module programming**” paragraph.

After all the changes is made press Ok. New configuration will be uploaded into the module and it will reload with the new parameters.

TLF_Server software: Event log download.

Using the software, You can download device event log for further processing. Log contains up to 254 events. To download log, press  icon. Than specify the path to the folder, where you want to save you .log file, choose folder, where you want to save you .log file, choose a name for it and press **Save**.

TLF_Server software: event table upload.

In case You need to update the code tables for security panels information decoding, You have to use  icon. After You pressed it, specify the path to the .hex file that was provided by the developer and press **Open**.

Working with module

Connecting to router.

In order to connect to router, you have to configure the following parameters:

Encryption algorithm – The following variants are available: NONE (no encryption), WEP-H, WEP-A, TKIP, AES.

Authentication method – The following variants are available: OPEN, SHARED, WPAPSK, WPA2PSK

If the Auto checkbox is activated, these two parameters are determined automatically.

Wi-Fi password – password for connecting to Wi-Fi network.

APN – Wi-Fi network name. Attention!: Name is case sensitive.

IP config method – Method of acquiring local IP address. Two options are available: DHCP – IP address assigned by router automatically and STATIC – IP address assigned manually. If STATIC option is chosen, than you have to additionally fill the LOCAL IP, SUBNET_MASK and GATEWAY fields.

Connecting to router in WPS mode

Module can connect to router in WPS mode. To do so, you first have to activate WPS mode on the router (in majority of routers, activated with the special button) and than, in 5 seconds time, press Auto WPS button on the back of the module. If everything is done correctly, module must receive all settings from the router.

Attention! In order for this option to work correctly, APN field must be left empty.

Programming Online-identifier

In order to send a message to the module from the WinSC software, you have to assign a unique ID for it.

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

Online ID is programmed using **USB_Reader** software in the “Online ID” field.

By default Online ID is set as 11111111.

Backup IP address

If the connection with the TLF_Server software is lost, module can connect to the backup server using another IP address and/or TCP port. Backup server parameters are configured in the **TCP port reserved** and **Server IP reserved** fields.

Attention!: after connection with the backup server is established, module cannot automatically return to the main server. To force module to return to the main server, you have to manually break connection with the backup server.

Status and settings request commands

To request module status and it's settings, there are four specialized commands:

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

V:3311, L:WPAPSK, P:TKIP, IP:213.21.196.68, PORT:923, APN:KORTEKS, QTime:15s, Id=11111111

V: - Module firmware version.
L: - Authentication method.
P: - Encryption algorithm.
IP: - IP-address.
PORT: - TCP port.
APN: - Wi-Fi network name.
Qtime: - Frequency of the connection test.
ID= - module Online ID.

Attention!: Due to the technical limitations, this reply will not appear in the WinSC software. You can see in in the TLF_Server Cmd window or in the event log.

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

V:3311, TestTime: 144h, OUT1: General Output, OUT2: General Output, Id=11111111

V: - Module firmware version.
TestTime: - Test message period *10 minutes.
OUT1: - First output working mode.
OUT2: - Second output working mode.
ID= - Module Online ID.

Attention!: Due to the technical limitations, this reply will not appear in the WinSC software. You can see in in the TLF_Server Cmd window or in the event log.

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

V:3311, Mode: DSC1, IN: , OUT: , Security: OFF

V: - Module firmware version.
Mode: - current working mode.
IN: - List of the inputs in alarm state.
OUT: - List of activated outputs.
Security: - Security mode ON/OFF.

Attention!: Due to the technical limitations, this reply will not appear in the WinSC software. You can see in in the TLF_Server Cmd window or in the event log.

99.C6 — Signal strength request. Reply has the following appearance:

E805xxx where xxx — signal level in percentages.

Working modes

RT4-5WF module has six 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 is made). When connecting security panel to the module in this mode, make sure that their accounts are identical.

- **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 **RT4-5WF** 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 **RT4-5WF** 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 **RT4-5WF** 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 **RT4-5WF** 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 **RT4-5WF** account.

Message format

Module events in "Modem" mode, from Paradox and DSC 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.

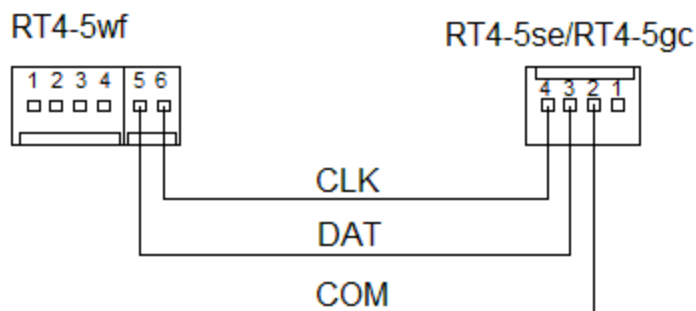
Messages that are transmitted via communication port in the first mode are not automatically converted into ContactID and their format depends on the connected device type.

Connecting RT4-5SE radio transmitter and RT4-5GL, RT4-5GP GSM transmitters

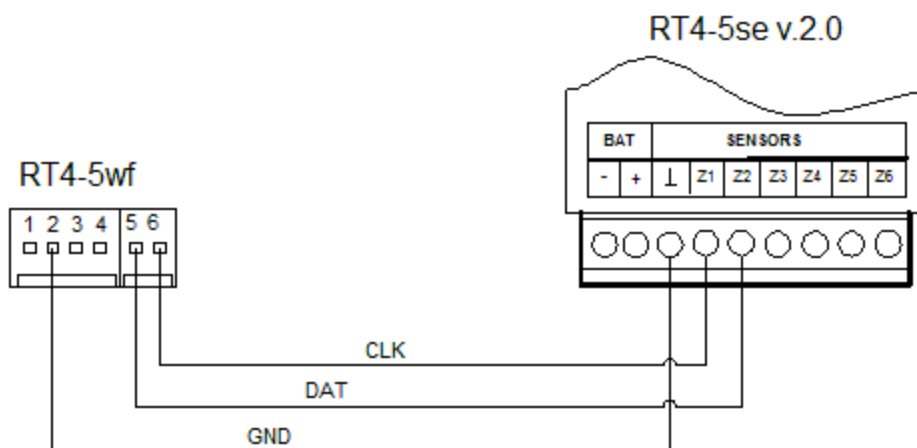
You can connect RT4-5WF to the radio RT4-5SE transmitter or to the GSM transmitters RT4-5GL and RT4-5GP.

Transmitter is used as a backup channel, when RT4-5WF fails to connect to both registered IP addresses.

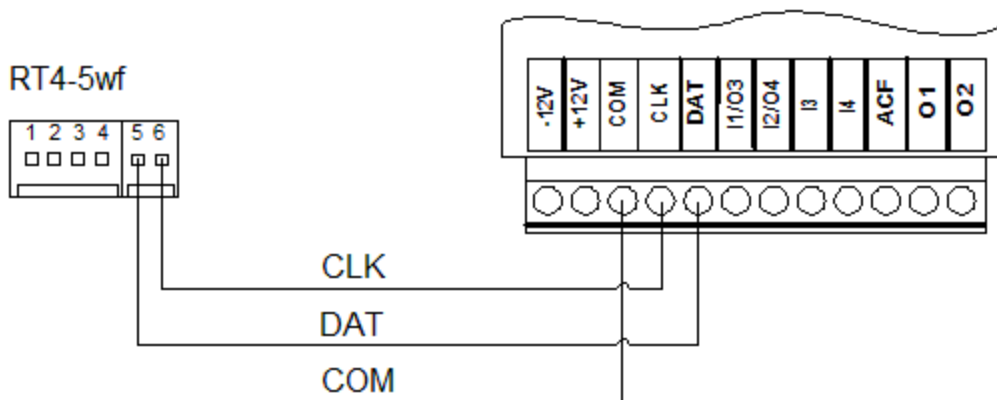
In the RT4-5SE v.2.0 radio transmitter, jumper must connect two upper contacts. In the RT4-5SE v.3.x, RT4-5GL, RT4-5GP transmitters, the first working mode (Serial BUS) must be activated.



RT4-5SE v.3.x, RT4-5GL and RT4-5GP transmitters wiring

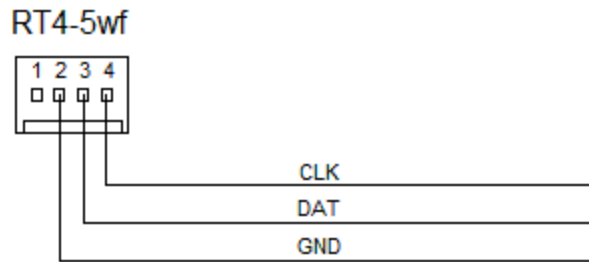


RT4-5SE v.2.0 transmitter wiring

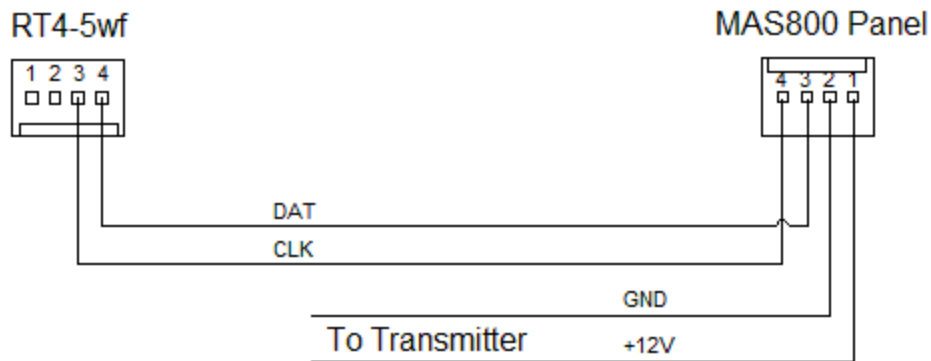


RT4-5GC v.2.x transmitter wiring

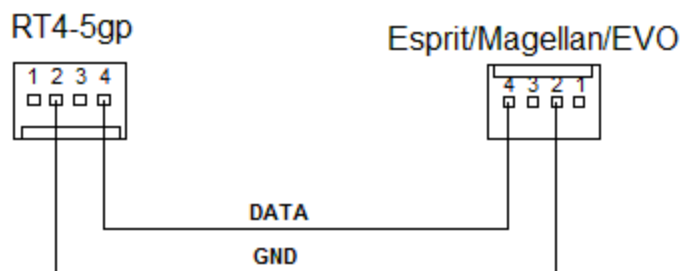
External device wiring



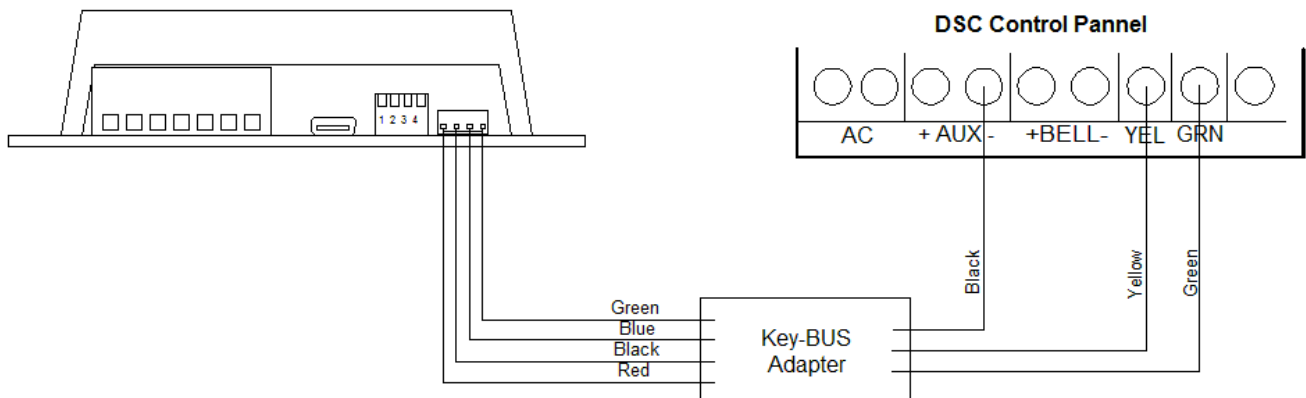
Serial BUS interface modules wiring (1-st mode)



MAS800 security panel wiring (1-st mode)



Esprit, Magellan and Digiplex panels wiring (2-nd, 3-rd and 6-th modes)



DSC panel Key-BUS wiring (4-th and 5-th modes)

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), and 'Phone' (Account: 1234, Line: GSM, Channel: 1, Phone: 26632248). On the right, there are time settings: 'Transm. test time' (25:00), 'Object test time' (25:00), 'Reminder timeout' (01:00), and 'Mainten. period MM:DD' (00:00). Below these are 'Mail' and 'Settings' buttons. A tabbed interface at the bottom shows 'Objects', 'Details', 'Zone', 'Events', 'TLF Events', 'Work Schedule', 'Hardware', and 'Notes'. The 'Events' tab is selected, showing a table of events.

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] unbyypass		N
1	??	R5710??		E	Fire zone [E] unbyypass		N
1	??	R5720??		E	24Hr zone [E] unbyypass		N
1	??	R5730??		E	Burglary zone [E] unbyypass		N
1	??	R6040??		E	End of fire test. User [E]		N
1	??	R6070??		E	End of walk test. User [E]		N

At the bottom of the window, 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.

In the **Radio** block you must enter parameters of the radio transmitter that is connected to the RT4-5WF. If transmitter is not connected, this block can be ignored.

TxAddress – transmitter number.

Channel – number of the receiving channel (Central Unit).

Slot – slot that the receiver is connected to.

Device type – must be set as Tx.

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

Account – Device account. Every device must have it's own unique account.

Channel – number of the receiving (IP Client).

Line – must be set as GSM

Phone – RT4-5WF Online ID

Transm.test time – radio transmitter test period. If transmitter is not connected must be set as 00:00.

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

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

Into the **Events** and **TLF Events** tabs you have to load RT4-5WF code cards.

If the radio transmitter is not connected to the RT4-5WF than Events tab may be left blank.

Enclosure 1. Terminal block pins.

Pin	Name	I/O	Description
1	12V-	I	Module power supply
2	12V+	I	
3	I1	I	First alarm input
4	I2	I	Second alarm input
5	ACF	I	Power supply control input
6	O1	O	Output 1
7	O2	O	Output 2

Enclosure 2. Module control commands.

Command	Description	Reply
0	Request status	/Status/: ¹
1	Activate Out 1	E802001
2	Deactivate Out 1	R802001
1.xxx	Activate Out 1 on time (xxx – seconds)	E802001
3	Activate Out 2	E802002
4	Deactivate Out 2	R802002
3.xxx	Activate Out 2 on time (xxx – seconds)	E802002
00.xxxx	Set current input state as normal (xxxx – security code)	/Status/: ¹
081.xxxx	Restart module (xxxx – security code)	R308000
99.C1	Connection settings request	---
99.C2	General settings request	---
99.C4	Current module status request	---
99.C6	Signal strength request (xxx – Signal level in percentages)	E805xxx

Notes:

- 1) Status is a list of all active modes and alarms.

Enclosure 3. Module events.

Event code	Description
E802001	Out 1 activated
E802002	Out 2 activated
R802001	Out 1 deactivated
R802002	Out 2 deactivated
E803000	Account/Security code changed
E830001	Alarm zone 1
E830002	Alarm zone 2
E850000	AC lost
E822000	Battery low
E801000	Module configuration changed
R830001	Restore zone 1
R830002	Restore zone 2
R850000	AC restored
R822000	Battery restored
E823000	Test message
R808000	Module is ready to work
E833020	Communication port failure
R833020	Communication port restored
E805xxx	Signal strength. xxx – signal level in percentages

Enclosure 4. 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 cancelled
E406000	Alarm cancelled
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 5. 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 6: 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 7. 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