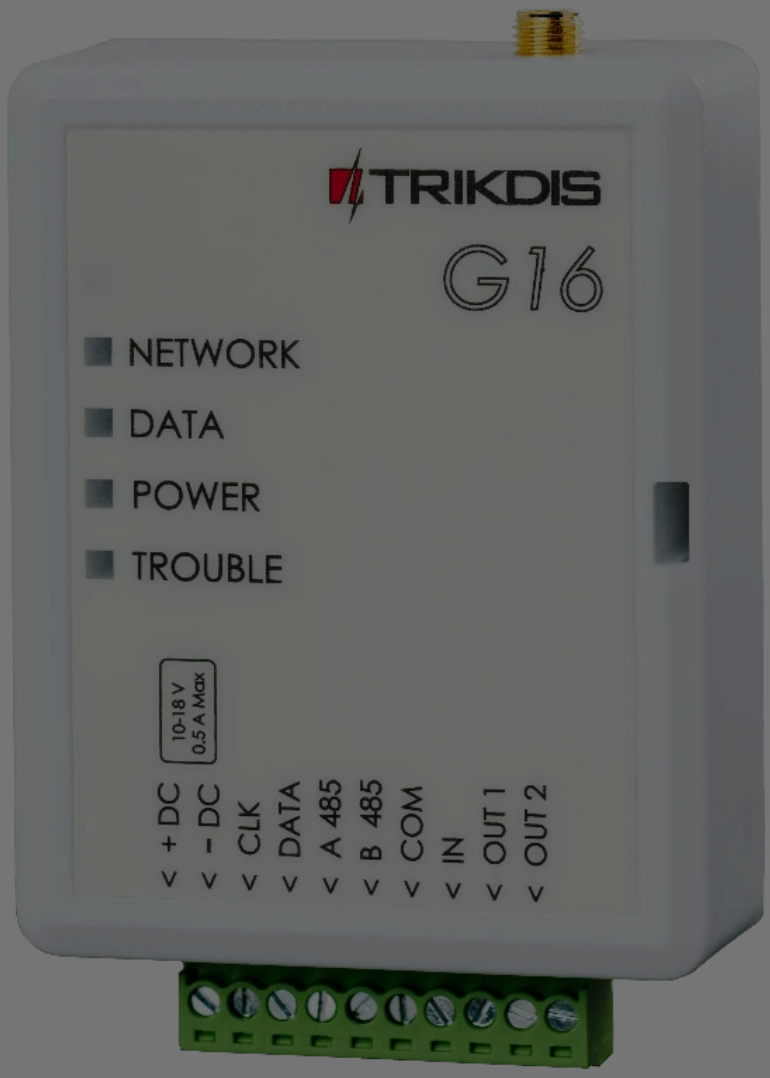
COMMUNICATORS

Cellular communicator G16



1. Description

Cellular communicator G16 directly connects to supported DSC, Paradox, UTC Interlogix

Communicator G16 can connect directly to DSC®, Paradox®, UTC Interlogix® (CADDX), Innerrange®, Texecom®, Honeywell®, Crow® and Pyronix® control panels. For panels from other manufacturers use the G16T communicator.

1.1 Features

Sends events to monitoring station receiver:

- Sends events to TRIKDIS software or hardware receivers that work with any monitoring software.
- Can send event messages to SIA DC-09 receivers.
- Can send event messages to SUR-GARD receivers. The annex has a table for converting Contact ID codes to SIA codes.
- Connection supervision by polling to IP receiver every 30 seconds (or by user defined period).
- Backup channel, that will be used if connection with the primary channel is lost.
- Events can be reported to CMS with SMS messages. SMS will be sent even if data connection stops working in the mobile operator network.
- With parallel communication channels events can be sent to two receivers at same time.
- When Protegus service is enabled, events are first delivered to CMS, and only then are sent to app users.

Works with Protegus app:

- "*Push*" and special sound notifications informing about events.
- Remote system Arm/Disarm.
- Remote control of connected devices (lights, gates, ventilation systems, heating, sprinklers, etc.).
- Remote temperature monitoring (with iO or iO-WL expanders).
- Different user rights for administrator, installer and user.

- SMS message.
- 2 inputs, selectable type: NC; NO; NC/EOL; NO/EOL; NC/DEOL; NO/DEOL.
- Add additional inputs and controllable outputs with wired and wireless iO expanders.

Quick setup:

- Settings can be saved to file and quickly written to other communicators.
- Two access levels for configuring the device for CMS administrator and for installer.
- Remote configuration and firmware updates.

1.2 List of compatible control panels

Manufacturer	Model
DSC®	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5015, PC5020
PARADOX®	SPECTRA SP5050+, SP5500+, SP6000+, SP7000+ - while SERIAL out is unlocked
PARADOX®	SPECTRA SP4000, SP5500, SP6000, SP7000, SP65
PARADOX®	MAGELLAN MG5000, MG5050, MG5050E
PARADOX®	DIGIPLEX EVO48, EVO192, EVOHD, NE96, EVO96
PARADOX®	SPECTRA 1727, 1728, 1738
PARADOX®	ESPRIT E55, 728ULT, 738ULT
UTC Interlogix®	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom®	Premier 412, 816, 832, 832+ / Premier 24, 48, 88, 168 / Premier Elite 12, 24, 48, 64, 88, 168
Pyronix®	MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6, MATRIX 816
Innerrange®	Inception, Integriti
Honeywell®	Ademco Vista-15, Ademco Vista-20, Ademco Vista-48
Crow®	Runner 4/8, Runner 8/16

*__Underlined__ - Control panels directly controlled by G16. Firmware PARADOX security panels,

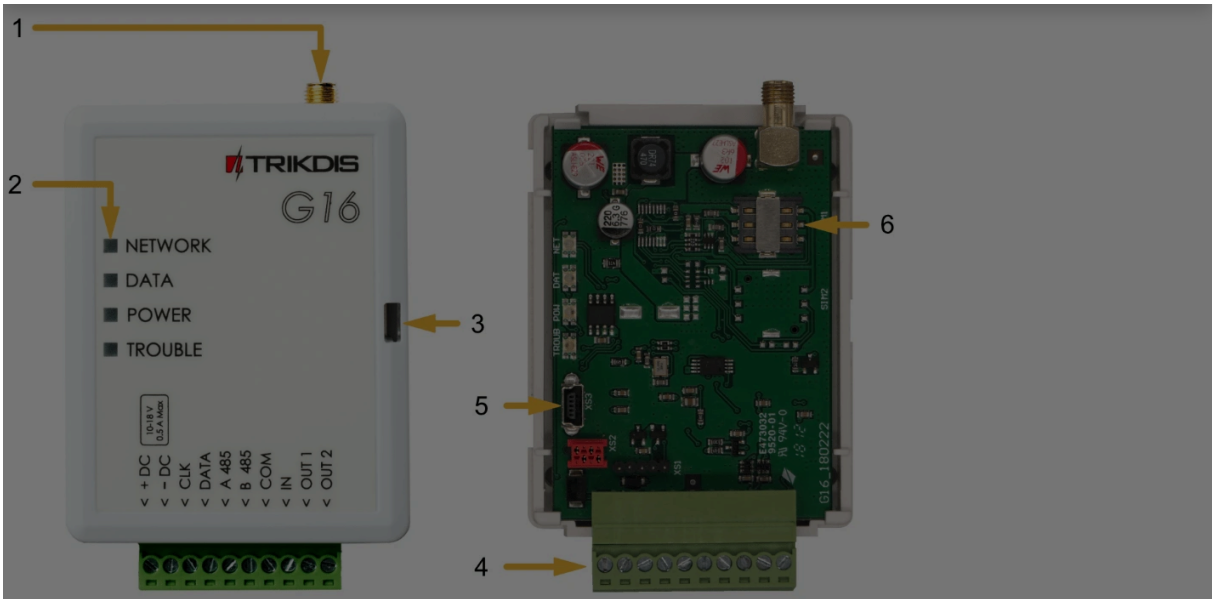
- G16_341x – 3 version, 1 SIM, 4G modem
- G16_3M10 – 3 version, 1 SIM, LTE CatM1 & EGPRS modem.

1.4 Specifications

Parameter	Description
Inputs	1 selectable type input: NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL. / Expandable with iO series expanders.
Output	2, OC type, commutating up to 0,15 A, 30 VDC max. Expandable with iO series expanders.
2G modem frequencies	850 / 900 / 1800 / 1900 MHz
3G modem frequencies	800 / 850 / 900 / 1900 / 2100 MHz
4G modem frequencies	Depends on region
Power supply voltage	10-18 V DC
Current consumption	60-100 mA (on standby) / Up to 250 mA (while sending data)
Transmission protocols	TRK, DC-09_2007, DC-09_2012, TL150
Message encryption	AES 128
Changing settings	With TrikdisConfig computer program remotely or locally via USB Mini-B port / Remotely with SMS messages
Operating environment	Temperature from -10 °C to 50 °C, relative humidity - up to 80% at +20 °C
Communicator dimensions	92 x 65 x 26 mm
Weight	80 g

1.5 Communicator elements

1. Cellular antenna SMA connector
2. Light indicators
3. Frontal case opening slot
4. Terminal for external connections



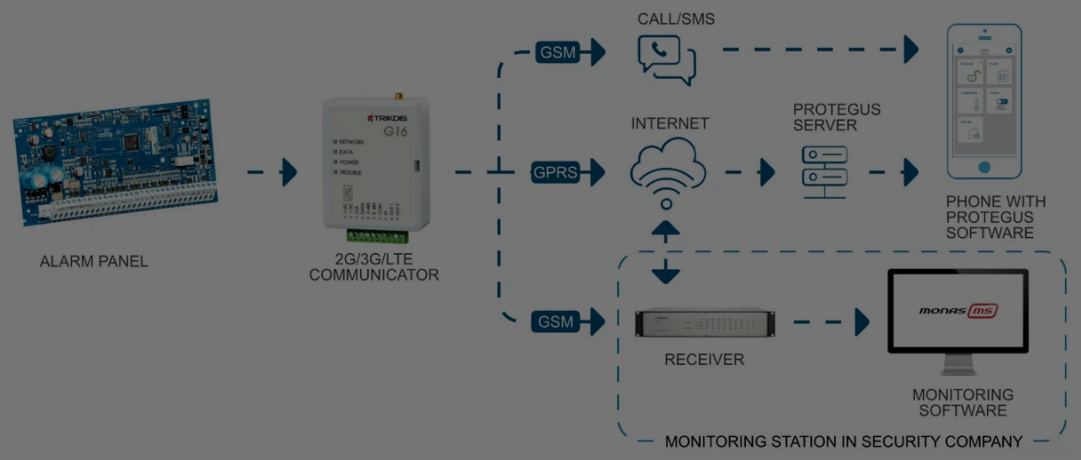
1.6 Purpose of terminals

Terminal	Description
+DC	+10 V/+18 V power supply
-DC	+10 V/+18 V power supply
CLK	Serial bus terminals for direct connection to control panel
A 485	RS485 bus A contact
B 485	RS485 bus B contact
COM	Common (negative) terminal
IN	Input
OUT1	1st open-collector output
OUT2	2nd open-collector output

1.7 LED indication of operation

Indicator	Light status	Description
NETWORK	Off	No connection to cellular network
NETWORK	Yellow blinking	Connecting to cellular network
NETWORK	Green solid with yellow blinking	Communicator is connected to cellular network. / Sufficient cellular signal strength for 2G is level 5 (five yellow flashes) and for 3G level 3 (three yellow flashes)
DATA	Off	No unsent events
DATA	Green solid	Unsent events are stored in buffer
DATA	Green blinking	(Configuration mode) Data is being transferred to/from communicator
POWER	Off	Power supply is off or disconnected
POWER	Green solid	Power supply is on with sufficient voltage
POWER	Yellow solid	Power supply voltage is insufficient (≤11.5V)
POWER	Green solid and yellow blinking	(Configuration mode) Communicator is ready for configuration
POWER	Yellow solid	(Configuration mode) No connection with computer
TROUBLE	OFF	No operation problems
TROUBLE	1 red blink	SIM card not found
TROUBLE	2 red blinks	SIM card PIN code problem (incorrect PIN code)
TROUBLE	3 red blinks	Programming problem (No APN)
TROUBLE	4 red blinks	Registration to Cellular network problem
TROUBLE	5 red blinks	Registration to GPRS/UMTS network problem
TROUBLE	6 red blinks	No connection with the receiver

1.8 Structural schematic with *G16* usage



NOTE

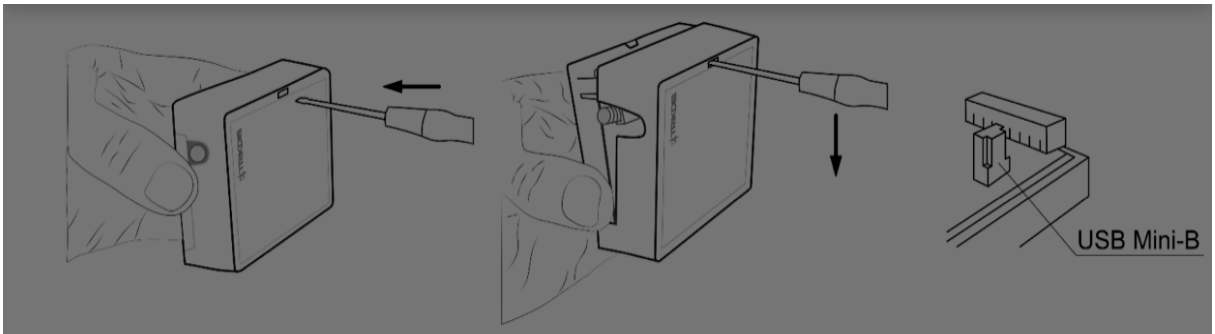
Before you begin, make sure that you have the necessary:

1. USB cable (Mini-B type) for configuration.
2. At least 4-wire cable for connecting communicator to control panel.
3. CRP2 cable for connecting to Paradox panel`s serial port.
4. Flat-head 2,5 mm screwdriver.
5. Sufficient gain cellular antenna if network coverage in the area is poor.
6. Activated SIM card (PIN code request can be turned off).
7. Particular security control panel`s installation manual.

Order the necessary components separately from your local distributor.

2. Quick configuration with *TrikdisConfig* software

1. Download **TrikdisConfig** configuration software from www.trikdis.com (type

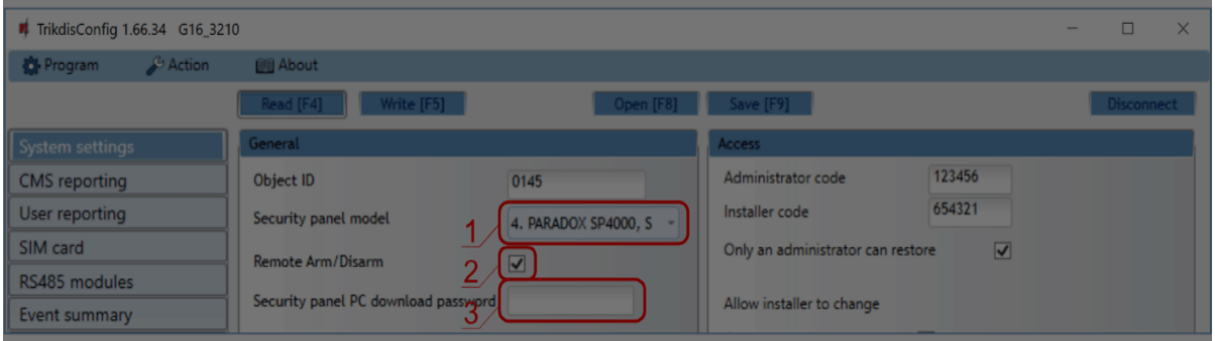


3. Using a USB Mini-B cable connect the G16 to the computer.
4. Run TrikdisConfig. The software will automatically recognize the connected communicator and will open a window for configuration.
5. Click **Read [F4]** to read the communicator's settings. If requested, enter the Administrator or Installer 6-digit code in the pop-up window.

Below we describe what settings need to be set for the communicator to begin sending events to the Alarm Receiving Center and to allow the security system to be controlled with the Protegus app.

2.1 Settings for connection with Protegus app

In "System settings" window:

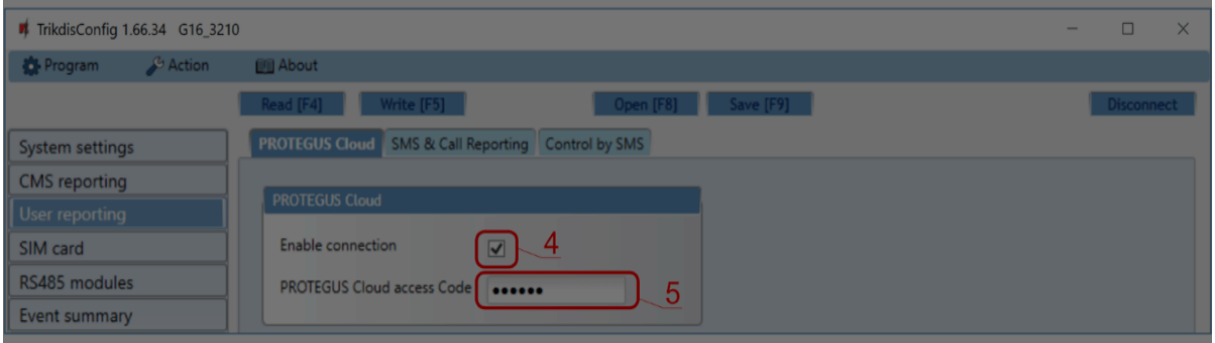


1. Select **Panel type** that will be connected to the communicator.
2. Select **Remote Arm/Disarm** if you want users to be able to control the panel in Protegus

NOTE

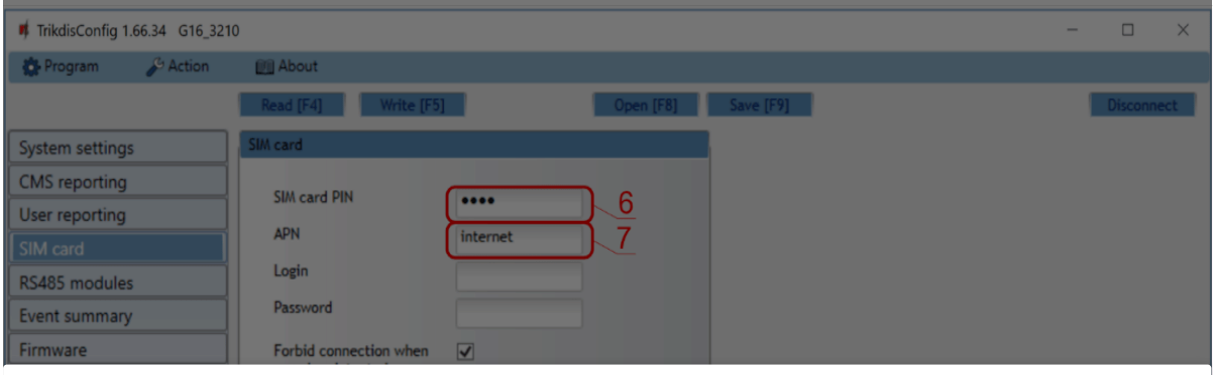
For the direct panel control to work, you will need to change the panel settings. How to do this is described in chapter 4 "Programming the control panel". In this section you will find information on how to change the PC download/UDL password.

In "User reporting" window, "PROTEGUS Cloud" tab:



4. Tick the checkbox **Enable connection** to the Protegus Cloud.
5. Change the **Protegus Cloud access Code** for logging in to Protegus if you want users to be asked to enter it when adding the system to Protegus app (default password – 123456).

In "SIM card" window:

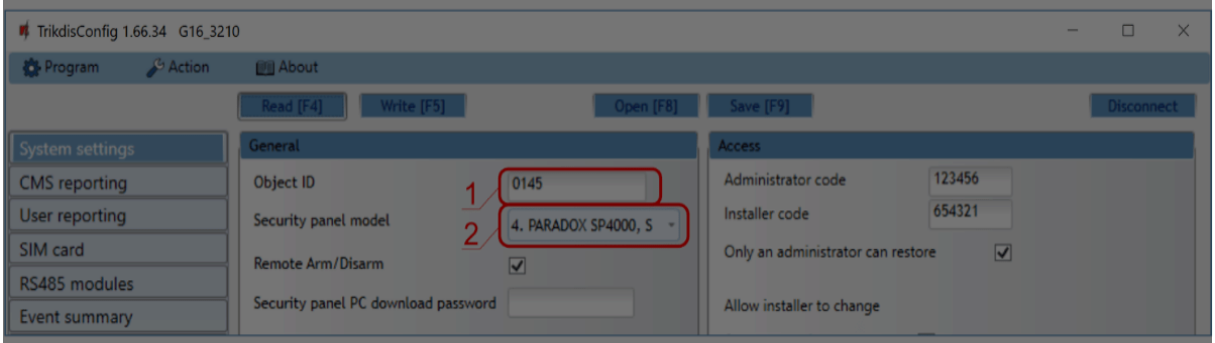


NOTE

For more information about other G16 settings in TrikdisConfig, see chapter **6 "TrikdisConfig window description"**.

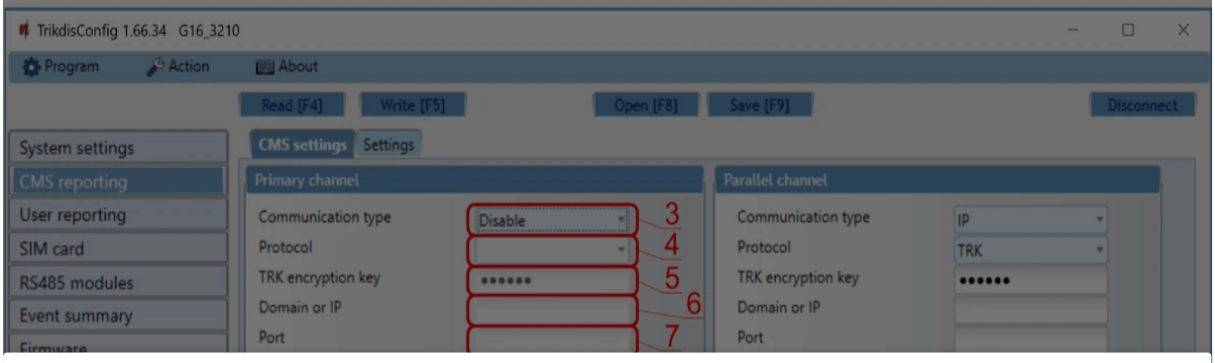
2.2 Settings for connection with Central Monitoring Station

In "System settings" window:



1. Enter **Object ID** (account) number provided by the Central Monitoring Station (4 characters, 0-9, A-F. **Do not use FFFE, FFFF Object ID**).
2. Select **Panel type** that will be connected to the communicator.

In "CMS reporting" window settings for "Primary channel":

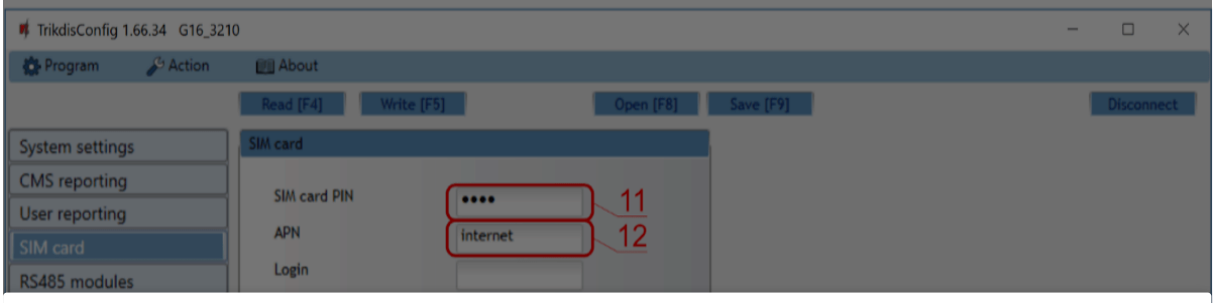


3. **Communication type** - select the **IP** connection method (We do not recommend SMS as the primary channel).
4. **Protocol** - select the protocol type for event messages: **TRK** (to TRIKDIS receivers), **DC-09_2007** or **DC-09_2012** (to universal receivers), **TL150** (to SUR-GARD receivers).
5. **TRK encryption key** - enter the encryption key that is set in the receiver.
6. **Domain or IP** - enter the receiver's Domain or IP address.
7. **Port** - enter receiver's network port number.
8. **TCP or UDP** - choose event transmission protocol (**TCP** or **UDP**) in which events should be sent.

> **NOTE**
>
> If you want to set communication with CMS via **SMS** messages, you only need to set **Encryption key** and **Phone number**. SMS messages can be received only by TRIKDIS receivers: IP/SMS receiver RL14, multichannel receiver RM14 and SMS receiver GM14. / If you selected the **DC-09** protocol, additionally enter object, line and receiver numbers in the **Settings** tab of the **CMS reporting** window.

7. (Recommended) Configure **Primary channel Backup** settings.
8. (Recommended) Enter **Backup SMS reporting number**.

In "SIM card" window:



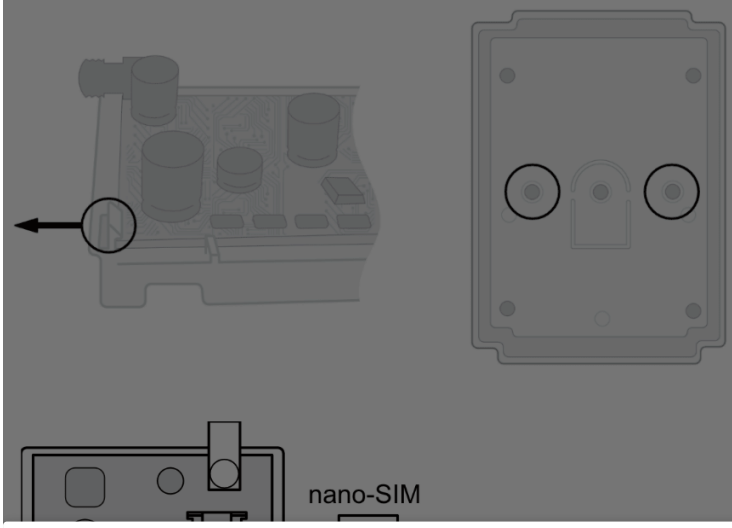
NOTE

For more information about other G16 settings in TrikdisConfig, see chapter 6 "TrikdisConfig window description".

3. Installation and wiring

3.1 Installation process

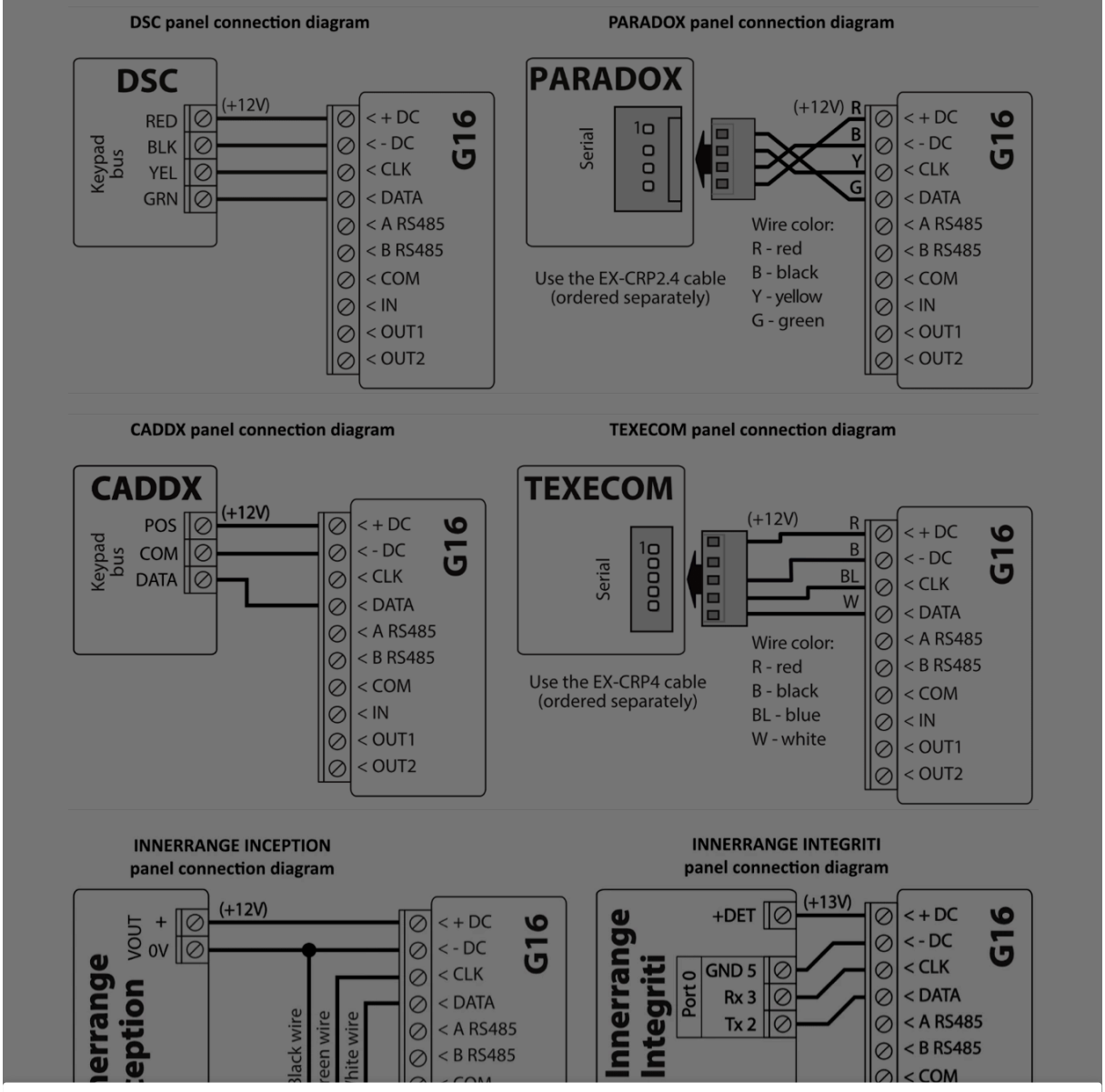
1. Remove the top cover and pull out the contact terminal.
2. Insert SIM card into the holder
3. Remove the PCB board from the bottom part of the case.
4. Fix the bottom part to a suitable place with screws.
5. Place the PCB board back into case, insert contact terminal.
6. Screw cellular antenna on.
7. Close the top cover

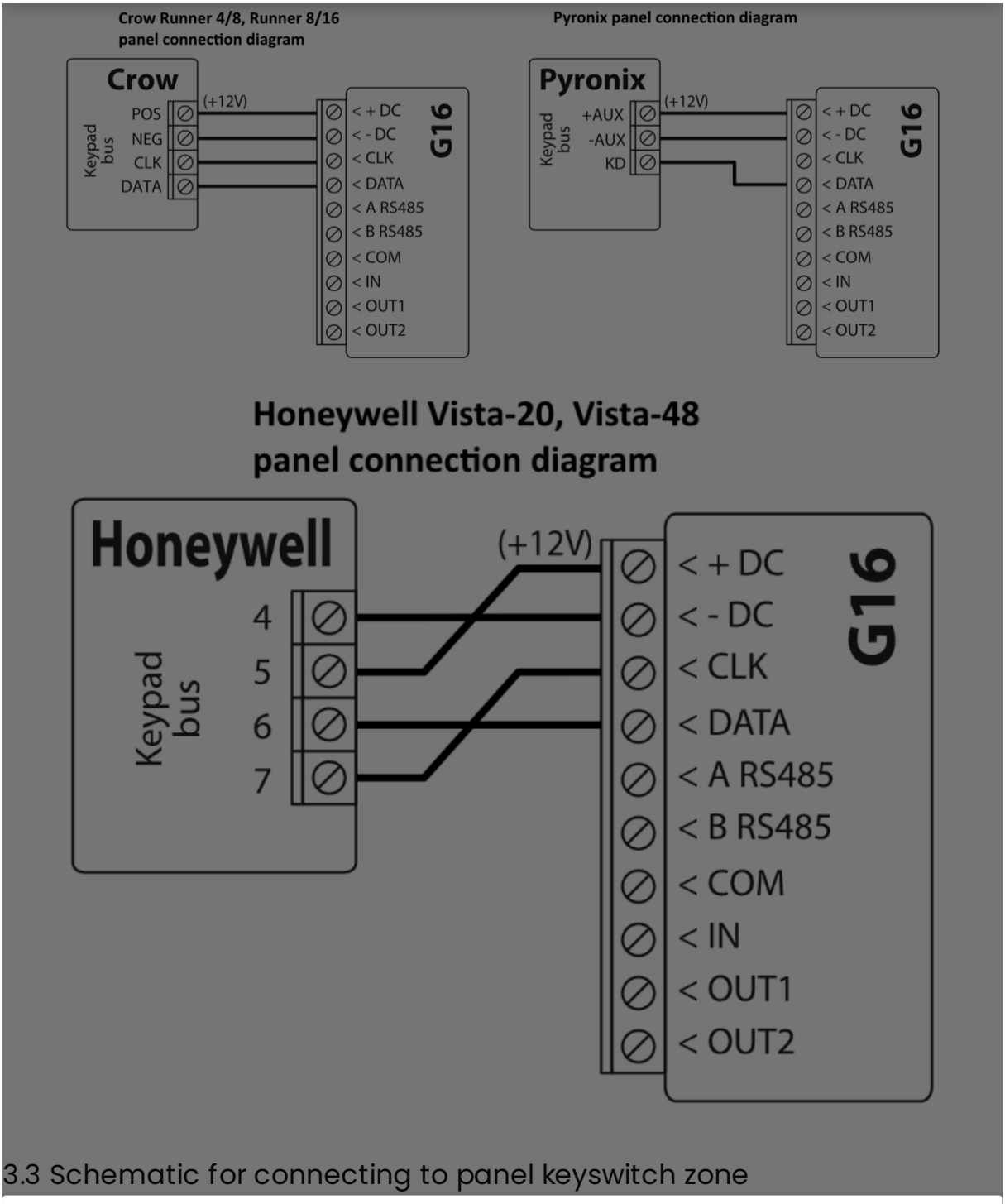


3.2 Schematics for wiring the communicator to a security control panel

Following one of the schematics provided below, connect communicator to the control panel.

1. **Schemes for connecting to the security control panels:**

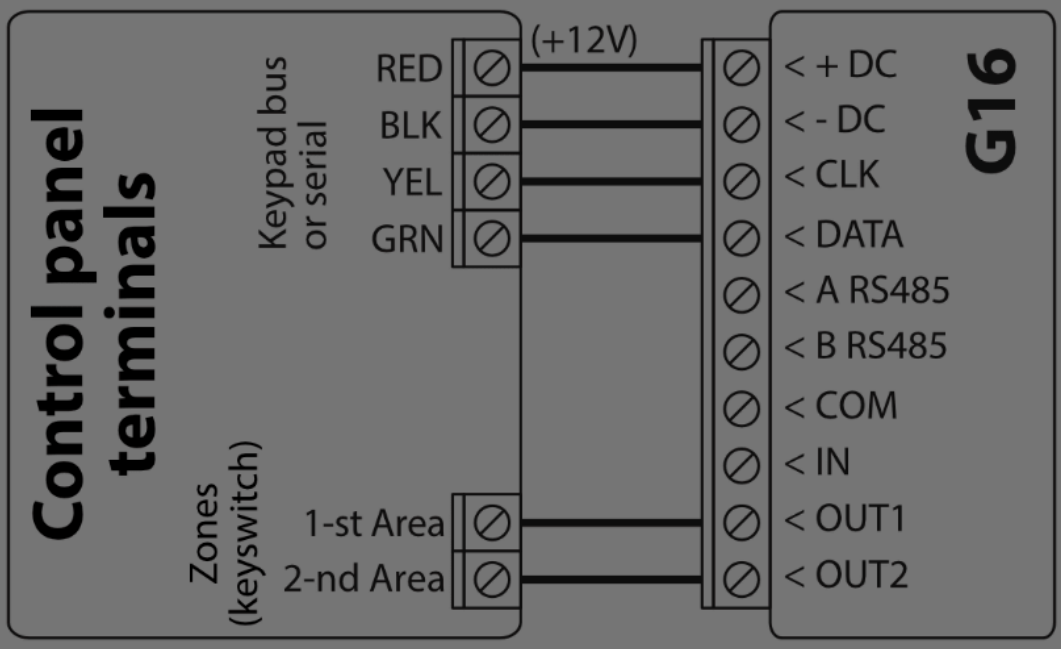




3.3 Schematic for connecting to panel keyswitch zone

NOTE

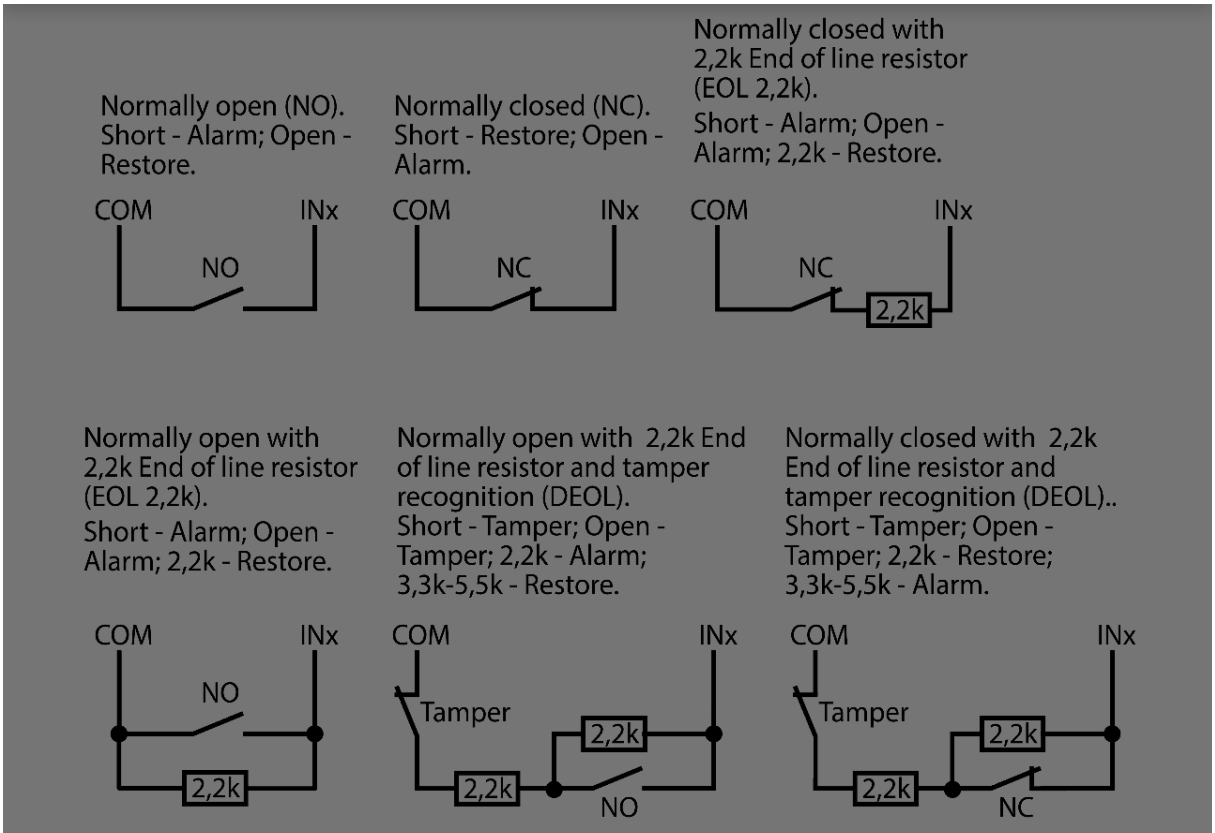
G16 communicator has two programmable outputs OUT (PGM) that can control two areas of the security system. If you want to control the system in this way, **Output OUT1 & OUT2 mode** needs to be set to **Remote control** (default setting) in the TrikdisConfig window **"System settings"**. Also, do not select the **Remote Arm/Disarm** box.



3.4 Schematics for input connection

The communicator has one input terminal (IN1) for connecting NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL type circuits. Default input setting - NO. The input type can be changed in the TrikdisConfig window **System settings -> Input IN1 type**.

Connect the input according to the selected input type (NO, NC, NC/EOL, NO/EOL, NO/DEOL, NC/DEOL), as shown in the schemes below:



NOTE

If more inputs or outputs need to be connected to the communicator, connect the TRIKDIS iO series wired or wireless output expander. Connection method is described in the iO manual and chapter **3.6 "Schematics for connecting iO series expansion modules"**.

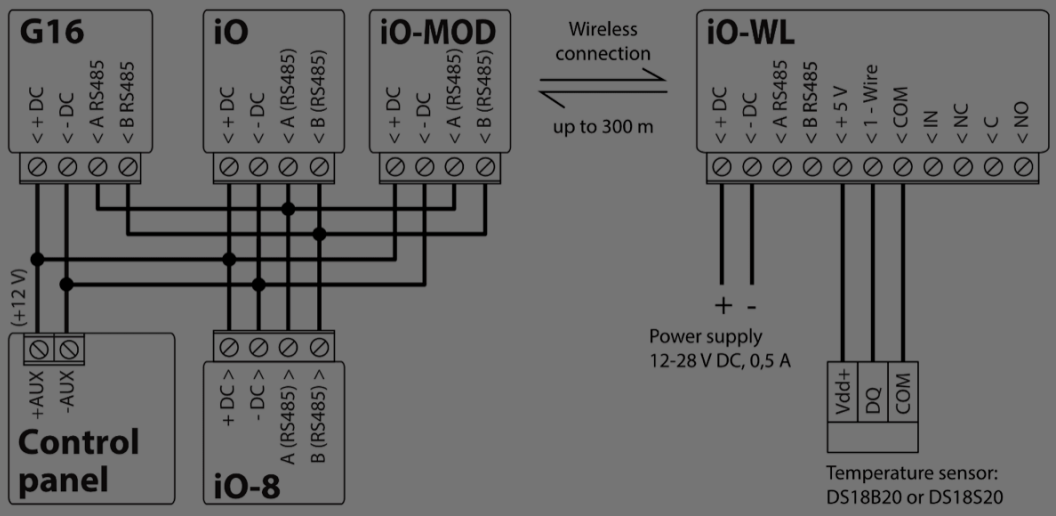
3.5 Schematics for wiring a relay

With relay contacts you can control (turn on/off) various electronic appliances.

Relay

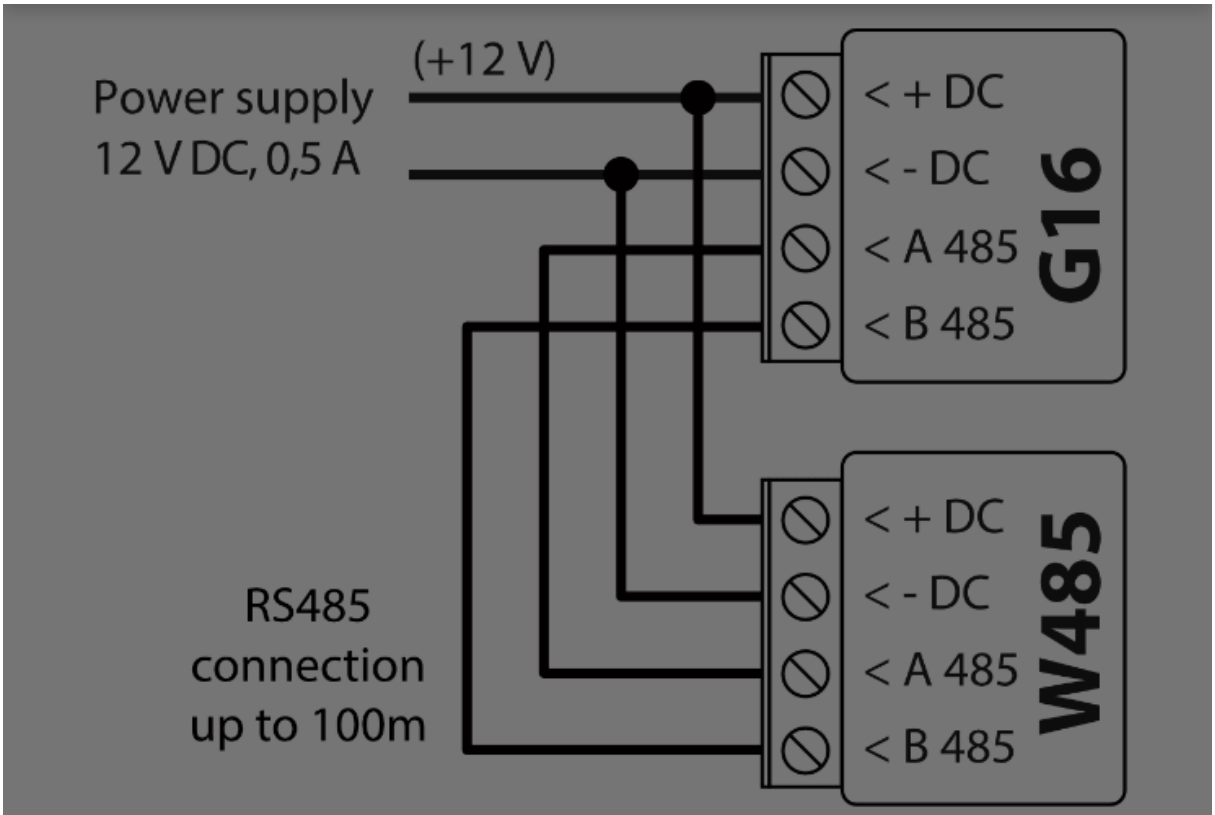
3.6 Schematics for connecting iO series expansion modules

If more inputs or outputs need to be connected to the communicator, or if you want to connect a temperature sensor, connect the TRIKDIS iO series wired or wireless output expander. Configuration of expander modules connected to the G16 is described in chapter 6.6. ““RS485 modules” window”.



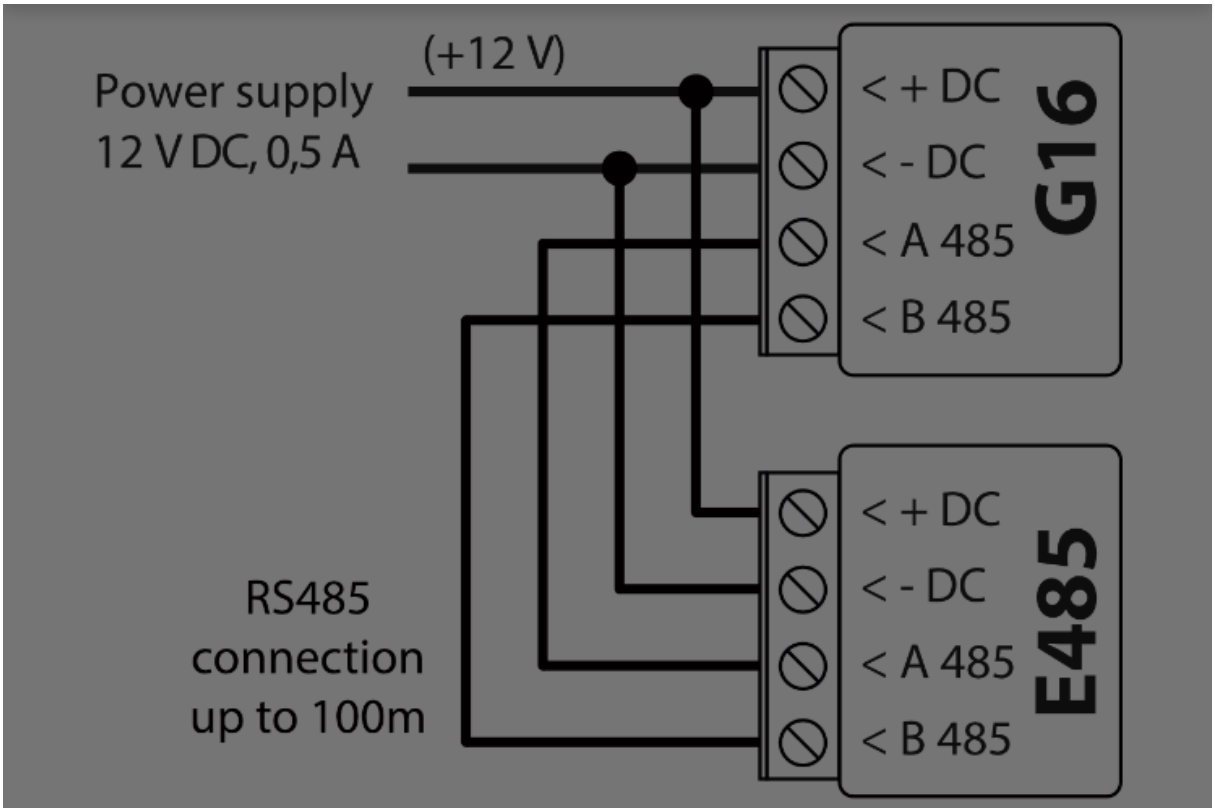
3.7 Schematic for connecting the *W485* WiFi module

The *W485* module sends messages to the CMS (Central Monitoring Station) and to Protegus using a WiFi internet router. When WiFi connectivity is available, the *G16* sends event messages via the *W485* module. When WiFi connectivity is disrupted, the *G16* sends messages via GPRS. When WiFi connectivity is re-established, the *G16* returns to sending messages via *W485*. / Configuration of the *W485* WiFi module to work with the *G16* is described in chapter 6.6. „„RS485 modules” window”. / Insert SIM card into the communicator *G16* for *W485* to work.



3.8 Schematic for connecting the E485 „Ethernet“ module

The *E485* sends messages to the CMS (Central Monitoring Station) and to Protegus using a wired internet connection. Using the *E485* with *G16*, CSP and *Protegus* messages are sent over wired Internet and mobile Internet is not used. If a wired internet connectivity is disrupted, the *G16* sends messages via the mobile Internet. When the wired Internet connectivity is re-established, *G16* starts sending messages via *E485*. / Configuration of the *E485* WiFi module to work with the *G16* is described in chapter 6.6. „„RS485 modules” window”. / Insert SIM card into the communicator *G16* for *E485* to work.



3.9 Turn on the communicator

To start the communicator, turn on the security control panel's power supply. This LED indication on the G16 communicator must show:

- "POWER" LED illuminates green when the power is on;
- "NETWORK" LED illuminates green and blinks yellow when the communicator is registered to the network.

NOTE

Sufficient strength of 2G cellular signal is level five (five "NETWORK" indicator flashes in yellow

4. Programming the control panel

Below it is described how to program the security control panel so that the G16 communicator could read events from the panel and control it remotely.

To enable remote control of the security panel, make sure that the checkbox **Remote Arm/Disarm** is selected in the TrikdisConfig window **“System settings”.**

4.1 DSC

DSC panels do not need to be programmed.

4.2 PARADOX

Paradox control panels need to be programmed only for direct control with Protegus. You do not need to program Paradox panels for reading events.

For remote control of Paradox panels, you need to set up a PC download password. This password must match the password which was set in the TrikdisConfig window **“System settings”**, when the checkbox next to **Remote Arm/Disarm** was selected.

To set this password, with the keyboard connected to the security control panel:

- For MAGELLAN, SPECTRA series: go to cell 911 and enter 4-digit PC download password.
- For DIGIPLEX EVO series: go to cell 3012 and enter 4-digit PC download password.

4.3 TEXECOM

Texecom control panels need to be programmed for both reading events and remote control.

You need to set the Texecom panel’s **UDL passcode**. This password must match the password which was set in the TrikdisConfig window **“System settings”,** when the box next to **Remote Arm/Disarm** was selected.

3) Press [7][6], and then [2]. Enter the 4-digit **UDL passcode** (**UDL passcode** must match the G16 communicator's **PC login password).**

4) Press [Yes] and leave the programming mode by pressing [Menu].

4.4 UTC INTERLOGIX (CADDX)

With the keyboard connected to the security control panel:

1) Press [*][8] and enter the installer's code (default - 9713).

2) Enter the device number assigned to the connected communicator (default - 0).

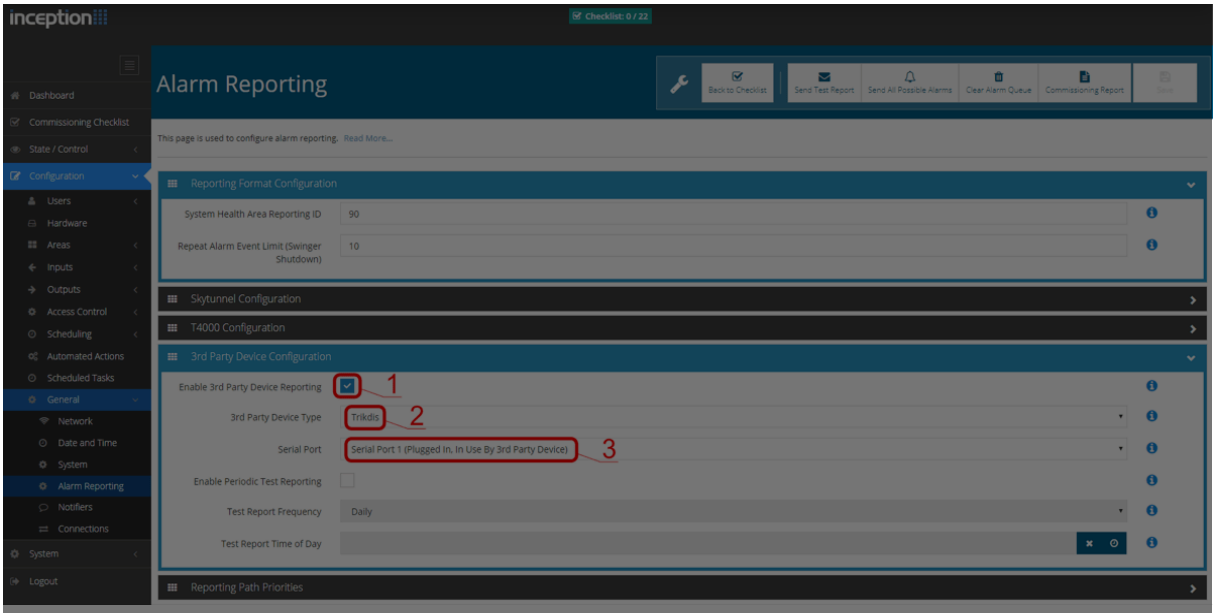
3) Set the settings below for each row. In sequence, enter the position, segment number and the required setting. Clicking [*] (asterisk) will return you to the local input field.

Position	Segment	Setting
23	3	12345678
37 (not necessary)	3	12345678
37 (not necessary)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

After having programmed all the fields listed, press [Exit] twice to exit the programming mode.

4.5 INNERRANGE

Innerrange Inception security control panel version must be **2.3.0.3507-r0** or higher.



1. **Enable 3rd Party Device Reporting** - select this checkbox.
2. **3rd Party Device Type** - set “Trikdis”.
3. **Serial port** - set “Serial Port 1 (Plugged In, In Use By 3rd Party Device)”.
4. Save settings and exit the application.

Innerrange Integriti security control panel version must be **19.1.0.36608** or higher, the professional software version **19.1.0.15396** or higher.

Specify the Trikdis communication protocol in the control panel configuration program. Contact ID data format. The port (TTL Port-0) of the security panel, to which the G16 communicator is connected, has the settings 19200, 8, N, 1. Save the settings and exit the program.

4.6 Honeywell Ademco Vista

Follow these steps for **Honeywell Ademco Vista-20** and **Honeywell Ademco Vista-48** panels. **The panel’s firmware version must be V5.3 or higher.** With a keypad that is connected to the panel:

Exit the programming mode. In keypad press [*][9][9]

Crow

There is no need to program Crow Runner 4/8 and Runner 8/16 panels.

5. Remote control

5.1 Adding the security system to Protegus app

With Protegus users will be able to control their alarm system remotely. They will see the status of the system and receive notifications about system events.

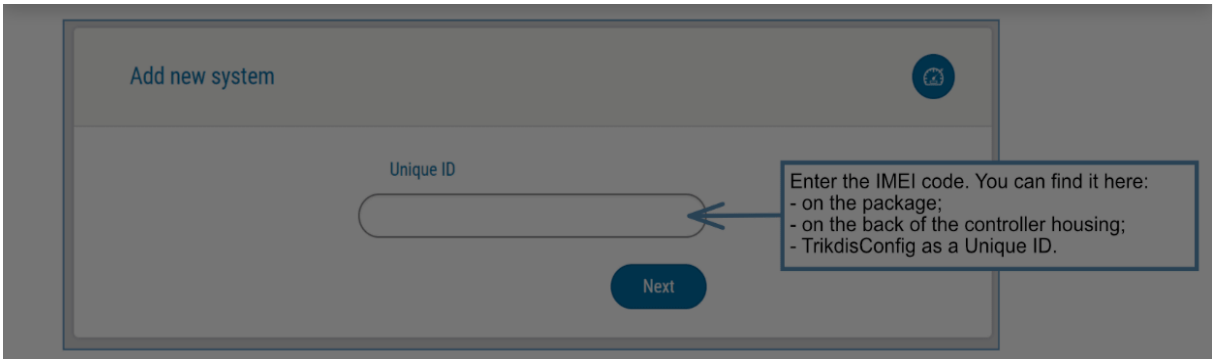
1. Download and launch the Protegus application or use the browser version: www.protegus.app.

2. Log in with your user name and password or register and create new account.

IMPORTANT

When adding the G16 to Protegus check if:

1. The inserted SIM card is activated and the PIN code is either entered or disabled;
2. Protegus cloud is enabled. See chapter **0 **
3. **"User reporting"** window;
4. Power supply is connected ("POWER" LED illuminates green);
5. Registered to the network ("NETWORK" LED illuminates green and blinks yellow).



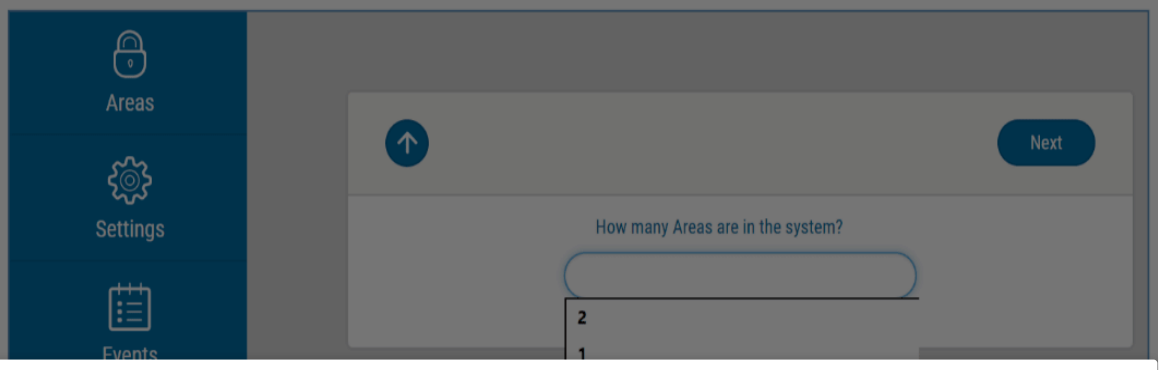
5.2 Additional settings to arm/disarm the system using the control panel's keyswitch zone

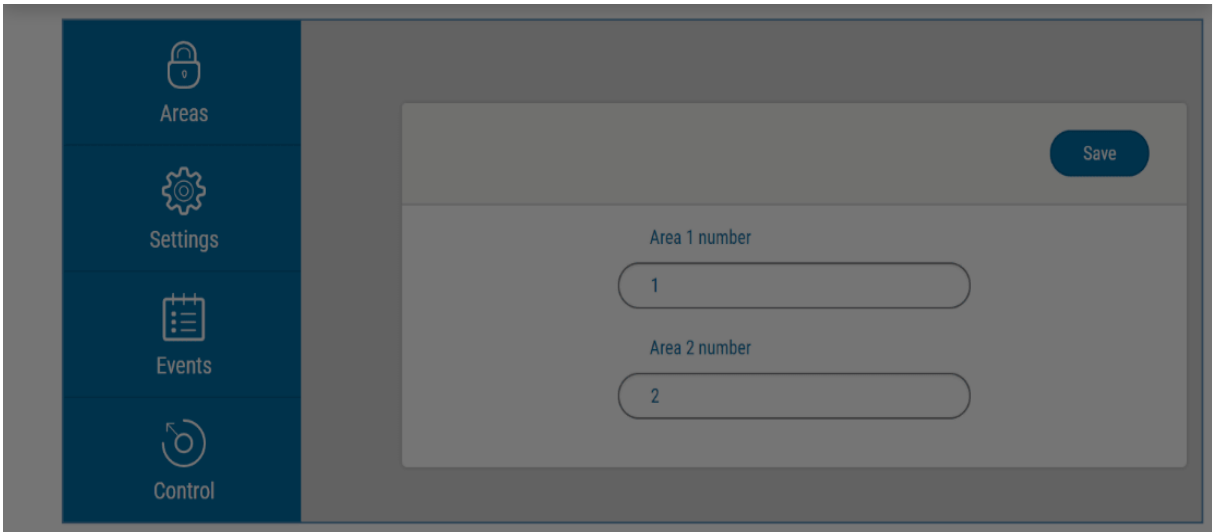
IMPORTANT

The control panel zone to which the G16 output OUT is connected to has to be set to keyswitch mode.

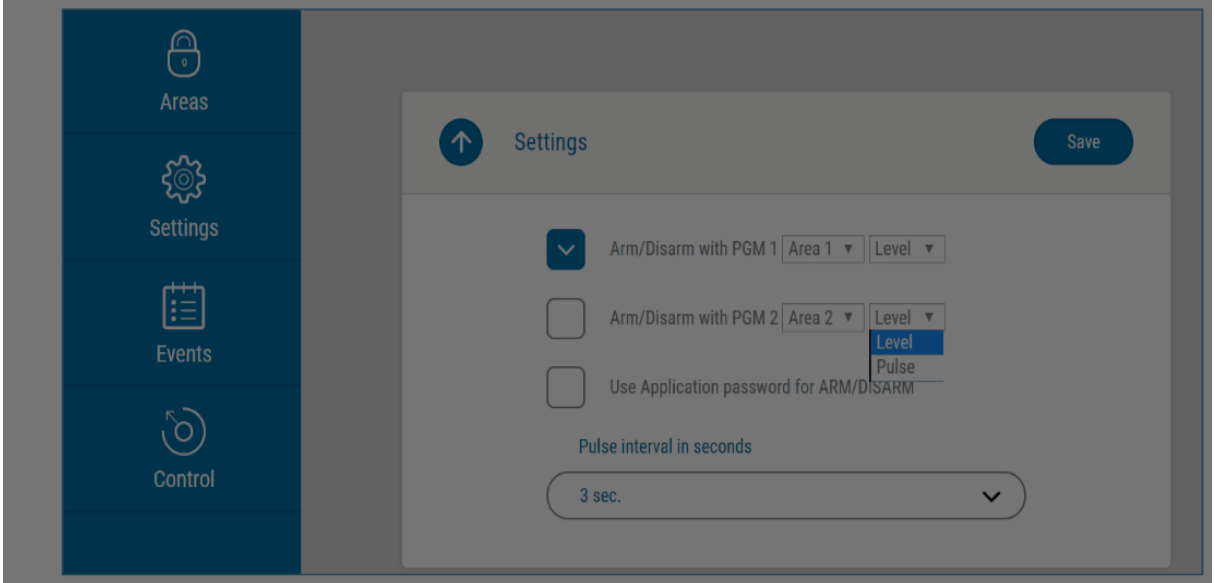
Follow the instructions below if the security control panel will be controlled with a G16 PGM output, turning on/off the control panel keyswitch zone.

1. In the new window, click **Areas** in the side menu. In the next window, specify how many alarm system areas (1 or 2) are in the system and press **Next**.



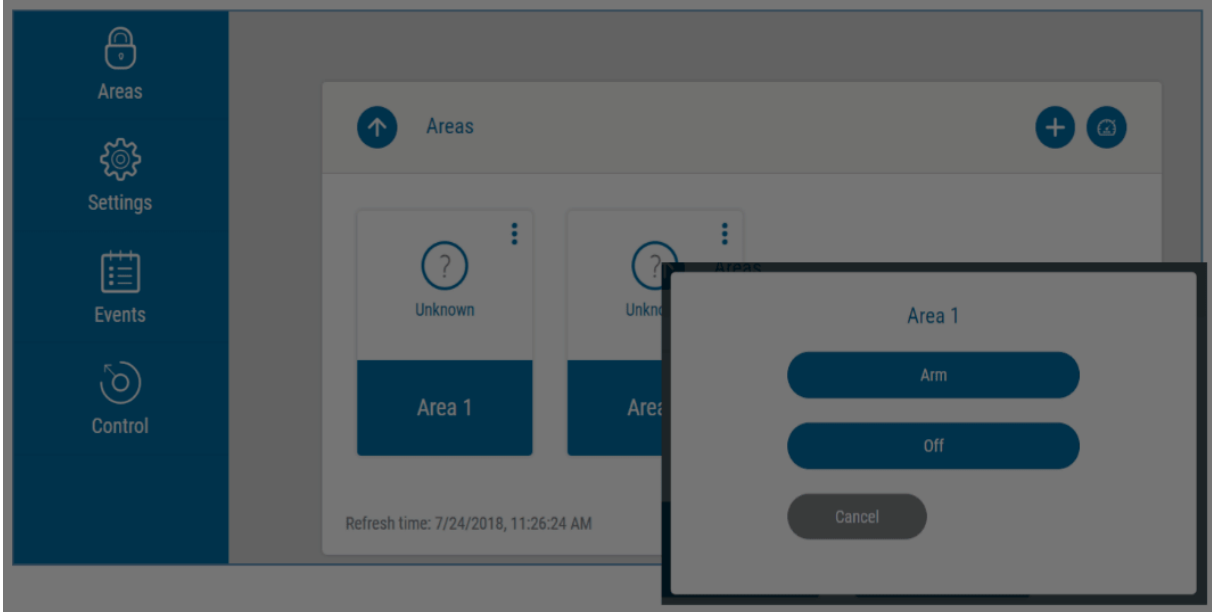


3. In the side menu press **Settings** and in the newly opened window press **Settings**. Select the box **Arm/Disarm with PGM** and specify which area the output will control. One PGM output can control only one area.



4. Select **Level** or **Pulse**, depending on the type of control panel keyswitch zone. You can also change the duration of the pulse interval if it is required for the connected control panel.

2. In the **Areas** window click the Area button. In the pop-up window select the action (arm or disarm the security system area).
3. If requested, enter the user code or Protegus password.



5.4 Configuration and control with SMS messages

You can remotely configure and control the communicator with SMS messages.

Message structure is: Password `[space]` Command `[space]` Data

For password use the **Administrator code** for *INFO, RESET, OUTPUTx, CONNECT* commands, and **Installer code** for *INFO, RESET, OUTPUTx* commands.

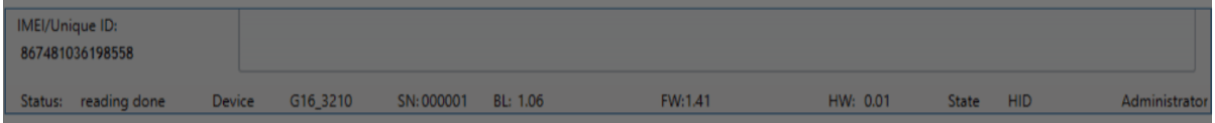
5.4.1 SMS command list

Command	Data	Description
INFO		Request information about the device. Response will be: communicator type, IMEI number, serial number and firmware version. E.g.: 123456 INFO
RESET		Restart the device. E.g.: 123456 RESET
OUTPUTx	ON	Turn on an output. x is the output number (1 or 2). E.g.: 123456 OUTPUT1 ON
OUTPUTx	OFF	Turn off an output. x is the output number (1 or 2). E.g.: 123456 OUTPUT1 OFF
OUTPUTx	PULSE=tttt	Turn on the output in impulse mode, for the specified time interval (sec). / “tttt” is the time duration of impulse in seconds, described in four digits. / E.g.: 123456 OUTPUT2 PULSE=0002
CONNECT	Protegus=ON	Enable access to Protegus service. E.g.: 123456 CONNECT PROTEGUS=ON
CONNECT	Protegus=OFF	Disable access to Protegus service E.g.: 123456 CONNECT PROTEGUS=OFF
CONNECT	IP=0.0.0.0:8000	Set primary channel IP address and Port number. / E.g.: 123456 CONNECT IP=192.120.120.255:8000
CONNECT	ENC=123456	Set TRK encryption key. E.g.: 123456 CONNECT ENC=123456
CONNECT	APN=Internet	Set APN name. E.g.: 123456 CONNECT APN=INTERNET
CONNECT	USER=user	Set APN user. E.g.: 123456 CONNECT USER=User
CONNECT	PASS=password	Set APN password. E.g.: 123456 CONNECT PASS=Password
CONNECT	CP=	Select security control panel from a list.

6. TrikdisConfig window description

6.1 *TrikdisConfig* status bar description

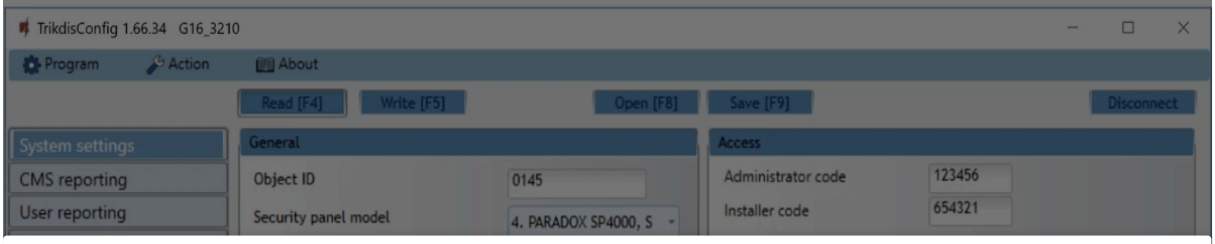
After connecting the G16 and clicking **Read [F4]**, ***TrikdisConfig*** will provide information about the connected device in the status bar:



Object	Description
Unique ID	Device IMEI number
Status	Operating condition
Device	Device type (G16 should be shown)
SN	Device serial number
BL	Browser version
FW	Device firmware version
HW	Device hardware version
Status	Connection to program type (via USB or remote)
Administrator	Access level (shown after access code is approved)

After pressing **Read [F4]**, the program will read and show the settings which are set in the ***G16.*** Set the necessary settings according to the TrikdisConfig window descriptions given below.

6.2 "System settings" window



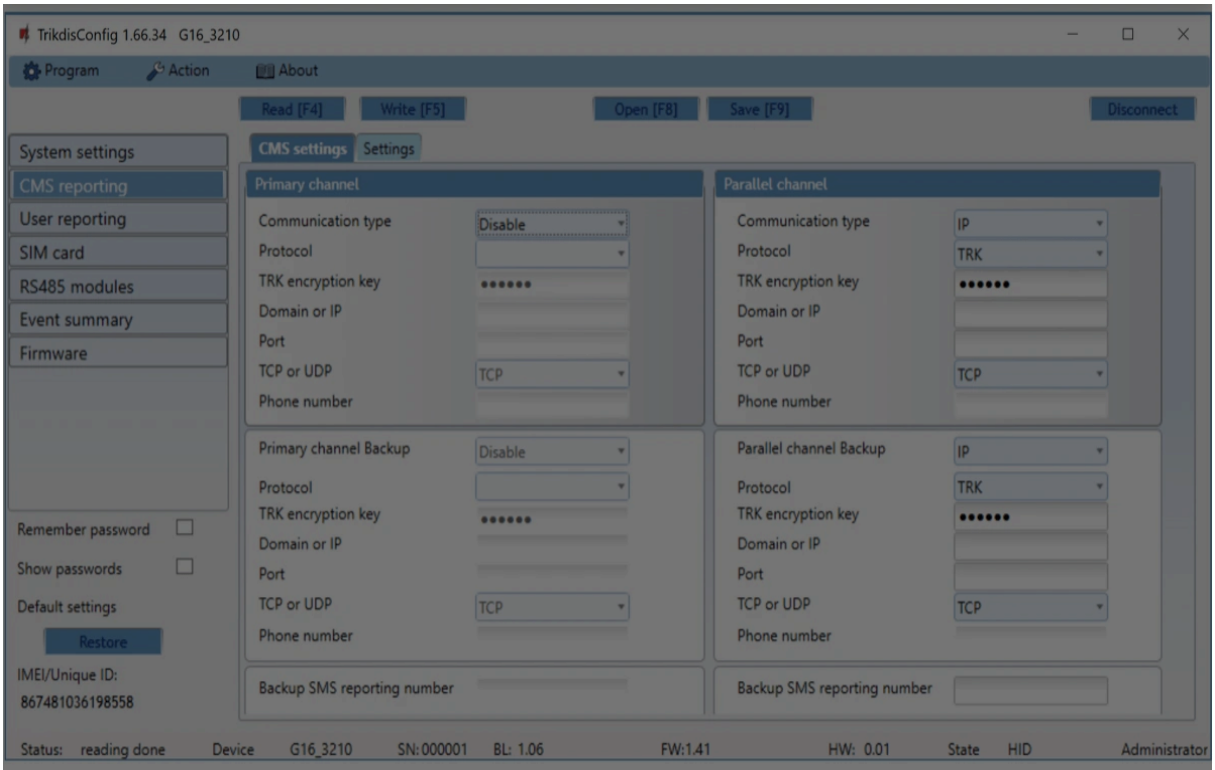
- **Object ID** – if the events will be sent to the CMS (Central Monitoring Station), enter the account number provided by the CMS (4 characters hexadecimal number, 0-9, A-F. **Do not use FFFE, FFFF Object ID**).
- Select the **Security panel model** that will be connected to the communicator.
- **Remote Arm/Disarm** - when the checkbox is selected, the G16 will directly control the control panel remotely. This setting will be visible only for directly controlled panels. For direct control of the control panels you need to change the panel settings, as described in section **4 "Programming the control panel".**
- **Security panel PC download/UDL password** - for the direct control of Paradox and Texecom control panels you need to enter the PC/UDL password. It must match the password that was entered in the control panel. How to change this password is described in section **4 "Programming the control panel"**.
- **Input IN type** - select the input type from the list (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL)**.**
- **Output OUT1 & OUT2 mode** - select the output operation mode from the list.
- **Time set -** select which server to use for time synchronization.

"Access" settings group

When setting up the communicator G16 there are two levels of access for, the administrator and the installer:

- **Administrator code -** allows you to access all configuration fields (default code - 123456).
- **Installer code** - limited access for configuring the communicator (default code - 654321).
- **Only an administrator can restore** - if the box is checked, factory settings can be restored only by entering the administrator code.
- **Allow installer to change** – the administrator can specify which settings can be changed by the installer.

6.3 "CMS reporting" window



The communicator sends events to the monitoring station via cellular internet (IP) or with SMS messages.

Events can be sent over several channels of communication. The primary and parallel communication channels can operate simultaneously, this way the communicator can send events to two receivers at the same time. Backup channels can be assigned for both primary and parallel channels, which will be used when the connection via the primary or parallel channel is interrupted.

Communication is encoded and password protected. A TRIKDIS receiver is required for receiving and sending event information to the monitoring programs:

- For connection over IP - software receiver IPcom Windows/Linux, hardware IP/SMS receiver RL14 or multichannel receiver RM14.
- To receive SMS messages - hardware IP/SMS receiver RL14, multichannel receiver RM14 or SMS receiver GM14.

- **Protocol** - select in which coding the events should be sent: **TRK** (to TRIKDIS receivers), **DC-09_2007** or **DC-09_2012** (to universal receivers), **TL150** (to SUR-GARD receivers).
- **TRK encryption key** - 6-digit message encryption key. The key written to the communicator must match the receiver's key.
- **Domain or IP** - enter the domain or IP address of the receiver.
- **Port** - enter the network port number of the receiver.
- **TCP or UDP** - select in which protocol (TCP or UDP) the events should be sent.
- **Phone number** (only for SMS messages) - enter the telephone number of a TRIKDIS SMS receiver. The phone number must begin with the country code (e.g., 370xxxxxxxx).

"Primary channel Backup" settings group

Enable the backup channel mode to send events via backup channel if connection via primary channel is lost. Backup channel settings are same as described above.

"Parallel channel" settings group

Events are transmitted in parallel with the first channel through this channel. When the second channel is enabled, events can be sent simultaneously to two receivers (e.g., local and centralized monitoring stations). Parallel channel settings are the same as described above.

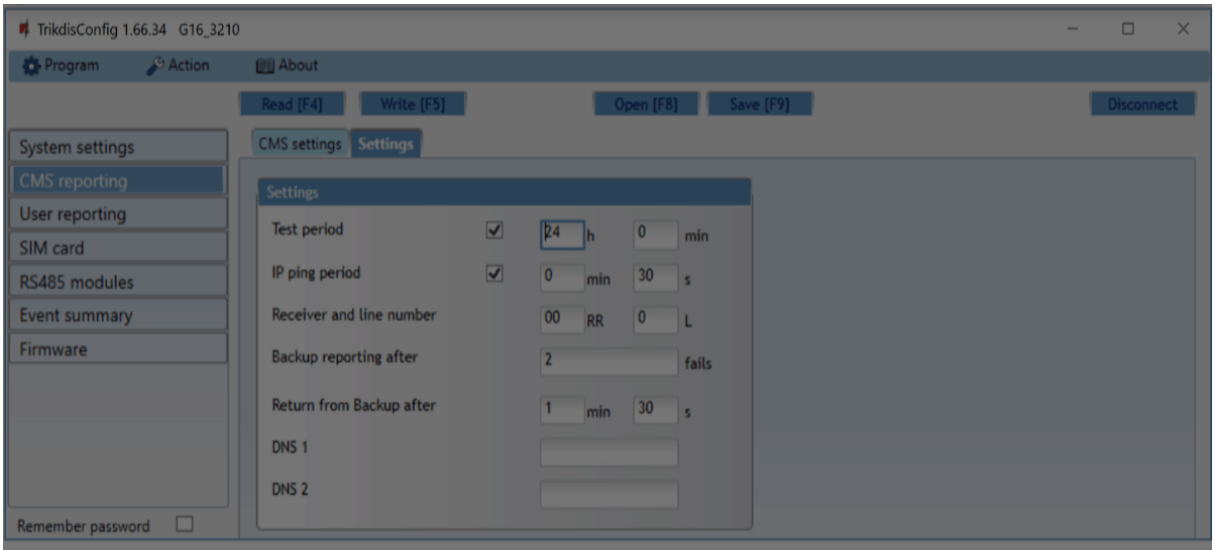
Backup SMS reporting number

Backup SMS messages are sent when they cannot be transmitted via the primary, parallel and backup channels. It is especially useful because it works even when there is no IP connection in the mobile operator network.

This channel is operational only when IP mode is set for the first channel and its backup channel.

SMS notifications will be sent to the Central Monitoring Station SMS receiver: 1) immediately after the first time when communicator starts operating; and 2) if the TCP / IP or UDP / IP connection is interrupted in the first channel and its backup channel.

- **Backup SMS reporting number** - enter the phone number for TRIKDIS alarm receiving



"Settings" tab **"Settings" settings group**

- **Test period** - TEST event period for testing the connection. Test events are sent as Contact ID messages and forwarded to the monitoring software.
- **IP ping period** – period for sending internal PING heartbeats. These messages are only sent via IP channel. The receiver will not forward PING messages to the monitoring software to avoid overloading it. Notifications will only be sent to the monitoring software if the receiver fails to receive PING messages from the device within the set time.

By default, the "*Connection lost"* notification will be transmitted to the monitoring software if the PING message is not received by the receiver over a time period three times longer than set in the device. E.g. if the PING period is set for 3 minutes, the receiver will transfer the *"Connection lost"* notification if a PING message is not received within 9 minutes.

PING heartbeats keep the active communication session between the device and the receiver. An active session is required for remote connection, control and configuration of the device. We recommend setting the PING period for no more than 5 minutes.

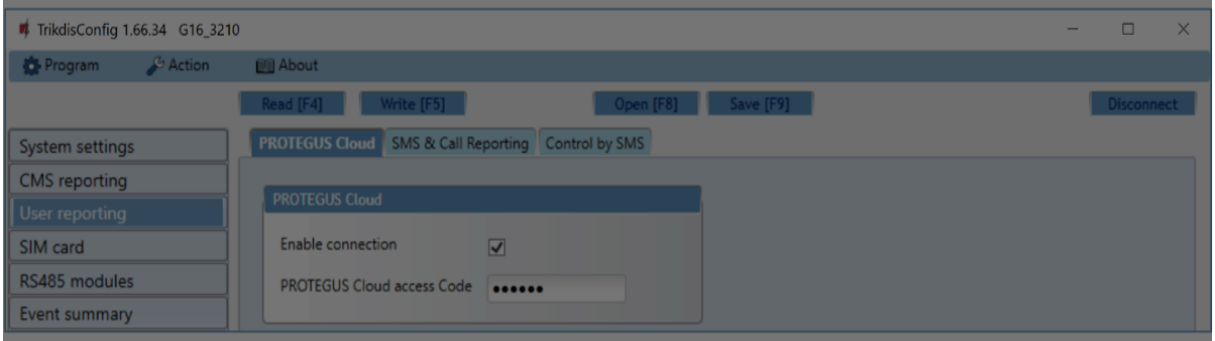
- **Backup reporting after** - indicates the number of unsuccessful attempts to send the message via Primary channel. If device fails to transmit specified number of times, the

The settings are displayed when the **DC-09_2007** or **DC-09_2012** protocol is set in the communication channel **Protocol** field for sending events to universal receivers.

- **Object ID in DC-09** - enter the object number. The object number entered in this field will be used if DC-09 encoding is selected. A hexadecimal number from 3 to 16 characters can be entered. This Number is provided by the Alarm Receiving Center.
- **DC-09-line No**. - enter line number of the receiver.
- **DC-09 receiver No.** - enter the receiver number.

6.4 "User reporting" window

"PROTEGUS cloud" tab

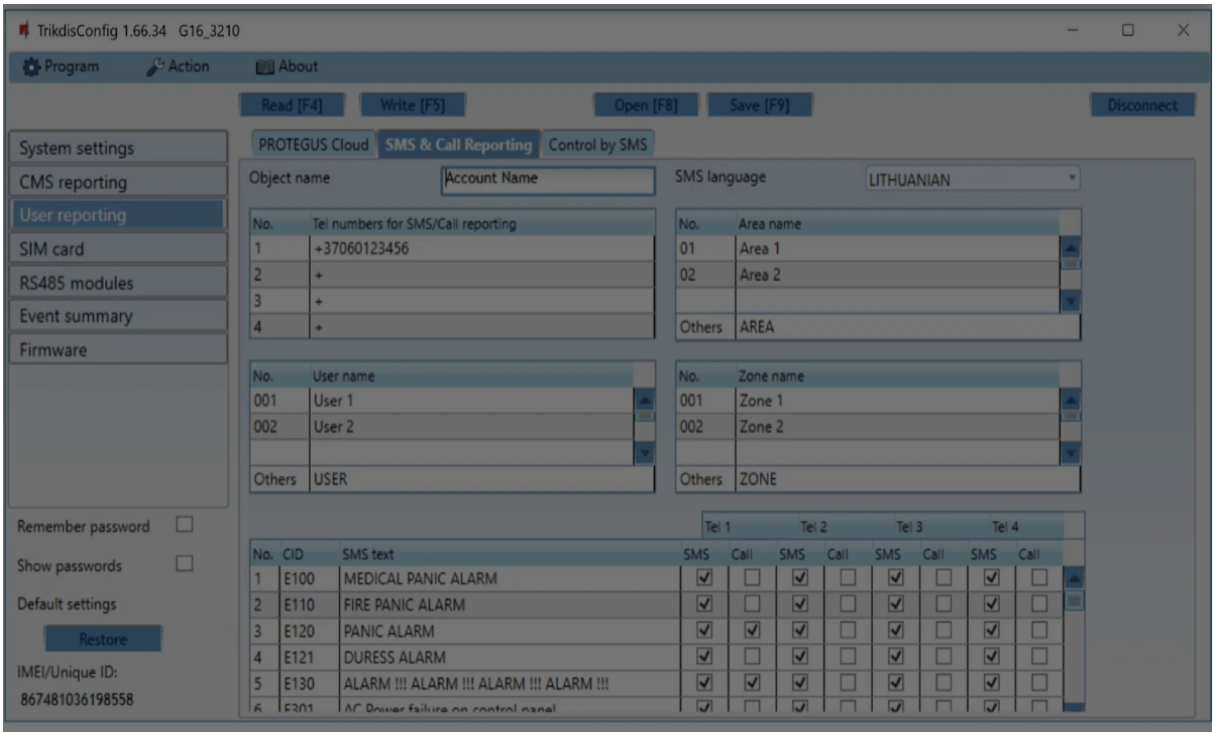


Protegus service allows users to remotely monitor and control the communicator. For more information about Protegus service, visit www.protegus.app.

"Protegus Cloud" settings group

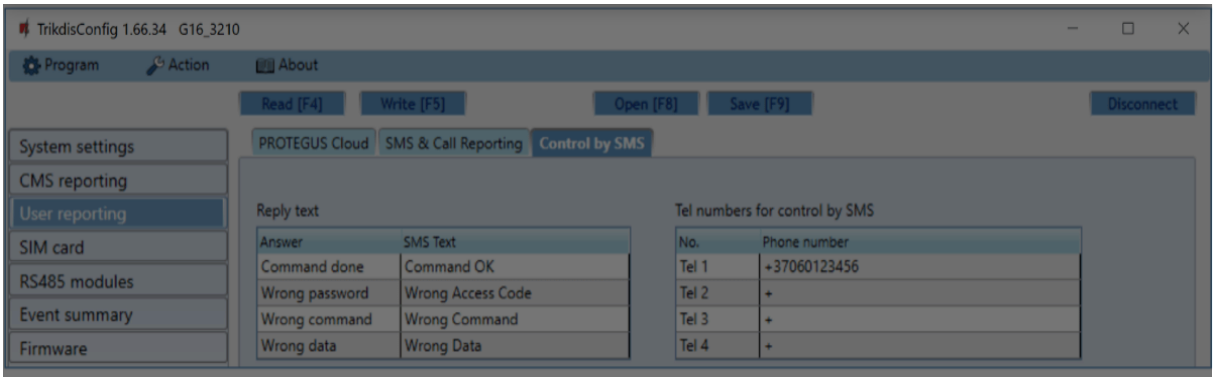
- **Enable connection** – enable the Protegus service, the G16 will be able to exchange data with Protegus app and to be remotely configured via ***TrikdisConfig***.
- **Protegus Cloud access Code -** 6-digit code for connecting to the Protegus app (default - 123456).

"SMS & Call Reporting" tab



Notifications about system events can be transmitted to users' mobile phones via SMS messages or phone calls.

- **Object name** - name the system to which the communicator is connected. Every SMS notification will include the name of the object.
- **SMS language** - choose the language for SMS messages (SMS messages can be sent with language-specific characters).
- **Tel numbers for SMS/Call reporting** - enter up to 4 user phone numbers that will receive event SMS messages or calls. Phone numbers must begin with the country code, for example +370xxxxxxxx, 00370xxxxxxxx or 370xxxxxxxx.
- **Area name, User name, Zone name tables** - each area, user and zone may have a name that will be used in SMS event messages. Enter the area, user or zone number in the appropriate table and enter the name next to the number.
- **CID event table** - you can change which phone numbers receive SMS messages or phone calls notifying about the events on the list.



You can send SMS commands to the communicator that will control the basic functions of the device. Find the control commands in chapter **5.4 Configuration and control with SMS messages**.

- **Reply text** - SMS text that the user receives after sending an SMS command. SMS text can be edited.
- **Tel numbers for control by SMS** - you can enter phone numbers from which the communicator will accept commands.

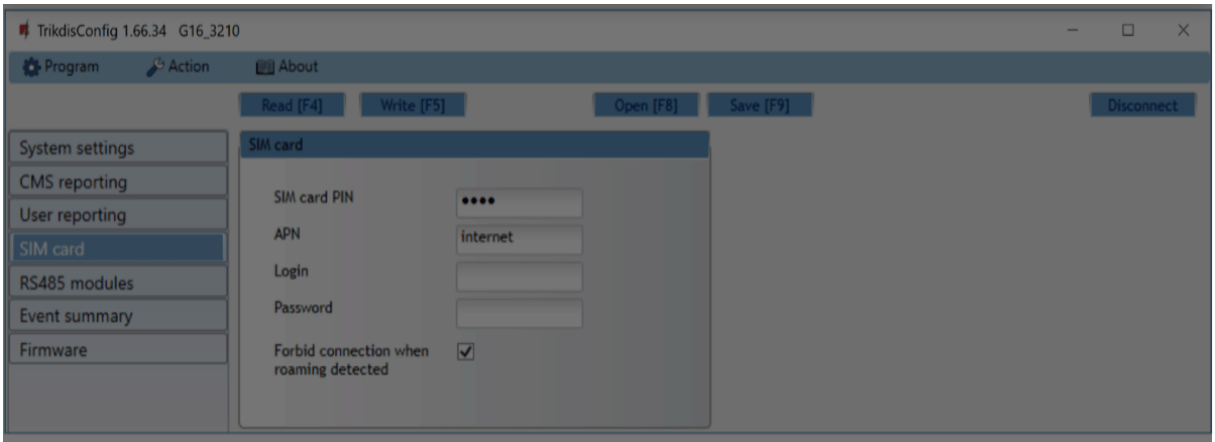
NOTE

If no phone number is entered, the device will accept commands from any phone number. In any case, security is guaranteed by the requirement to enter administrator or installer password in the SMS command.

6.5 “SIM card” window

IMPORTANT

1. Ensure that the SIM card is activated and working before using it. / 2. If mobile internet connection will be used for sending events via IP channel or to Protegus, ensure that mobile



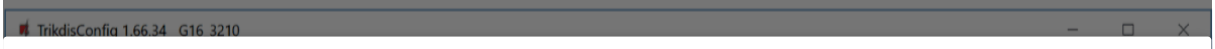
"SIM card" settings group

- **SIM card PIN** - enter the SIM card PIN code. This code can be disabled by inserting the SIM card into a mobile phone and disabling the request. If you disabled the SIM card PIN request, leave the default value in this field.
- **APN** - enter APN (Access Point Name). It is required for connecting the communicator to the internet. APN can be found on the website of the SIM card operator ("internet" is universal and works in the networks of many operators).
- **Login, Password** - if required, enter the user name (login) and password for connection to the internet.
- **Forbid connection when roaming detected** - you can use this function when the security system is installed near the country border. This function prevents the communicator from operating in the other country's mobile network.

6.6 "RS485 modules" window

"Modules list" tab

iO series expanders can be connected to the communicator to add additional inputs, outputs and serial buses for temperature sensors. Connected expanders must be added to the **Modules list** table.



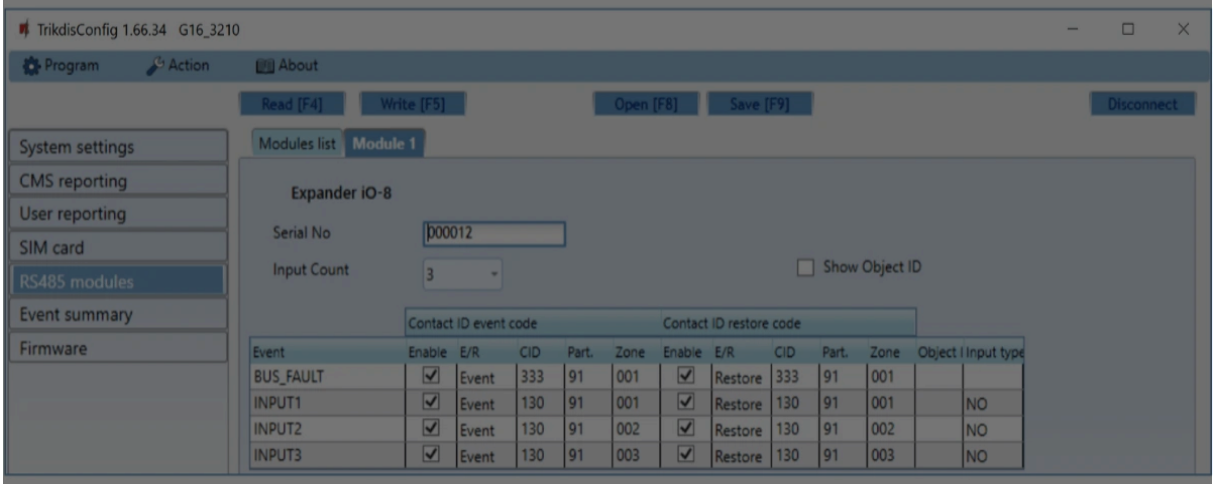
- **Module type** – select the module that is connected to the communicator via RS485 from the list.
- **Serial No –** enter the module serial number (6 digits), which is indicated on stickers on the module's case and packaging.

After selecting the connected module and entering its serial number, press the **Write [F5]** button. When the change is written, disconnect the USB Mini-B cable from the communicator. Wait one minute (the communicator has to register the connected module). Connect the USB Mini-B cable to the communicator. Click the **Read [F4]** button. Go to **RS485 modules → Module.**

"Module" tabs

After adding the expander to the communicator as described above, in the **RS485 modules** window a new tab will appear with this module's settings. The tab will be given a number. Bellow we describe the settings for **iO-8** and **iO** series expanders, for the WiFi module W485, for the „Ethernet" module E485.

iO-8 expander settings window



Expander iO-8 has 8 universal (input/output) terminal contacts. Up to four iO-8 expanders can be connected.

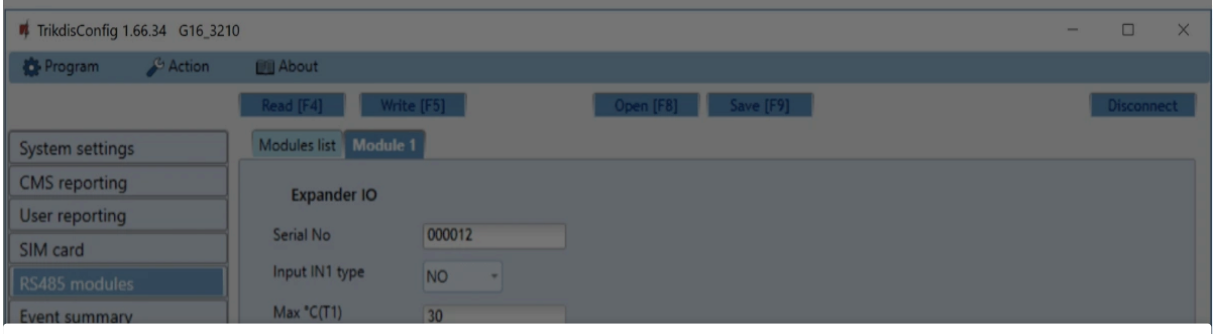
- **Enable** – allow message transmission, when the input is triggered.
- **E/R** – choose what type of event will be sent when input is triggered – **Event** or **Restore**.
- **CID** – assign a Contact ID event code to the input.
- **Part.** – assign the partition (area) to the input. It is set automatically: if the module no. is 1, then the area is 91; if the module no. is 4, then the area is 94.
- **Zone** – set the zone number for the input.

***Contact ID restore code*:**

- **Enable** – allow message transmission when the input is restored.
- **E/R** – choose what type of event will be sent when input is restored – **Restore** or **Event**.
- **CID** – assign the Contact ID restore code to the input.
- **Part.** – assign the partition (area) to the input. It is set automatically: if the module no. is 1, then the area is 91; if the module no. is 4, then the area is 94.
- **Zone** – set the zone number for the input.
- **Object ID** - the input (IN) can be assigned an Object ID, which will differ from the Object ID of the communicator G16.
- **Input type** – select the type of the input (NO or NC).

For customers to receive SMS messages or calls about input triggers, enter the Contact ID event code that is assigned to the input to the table in **"SMS & Call Reporting"** tab.

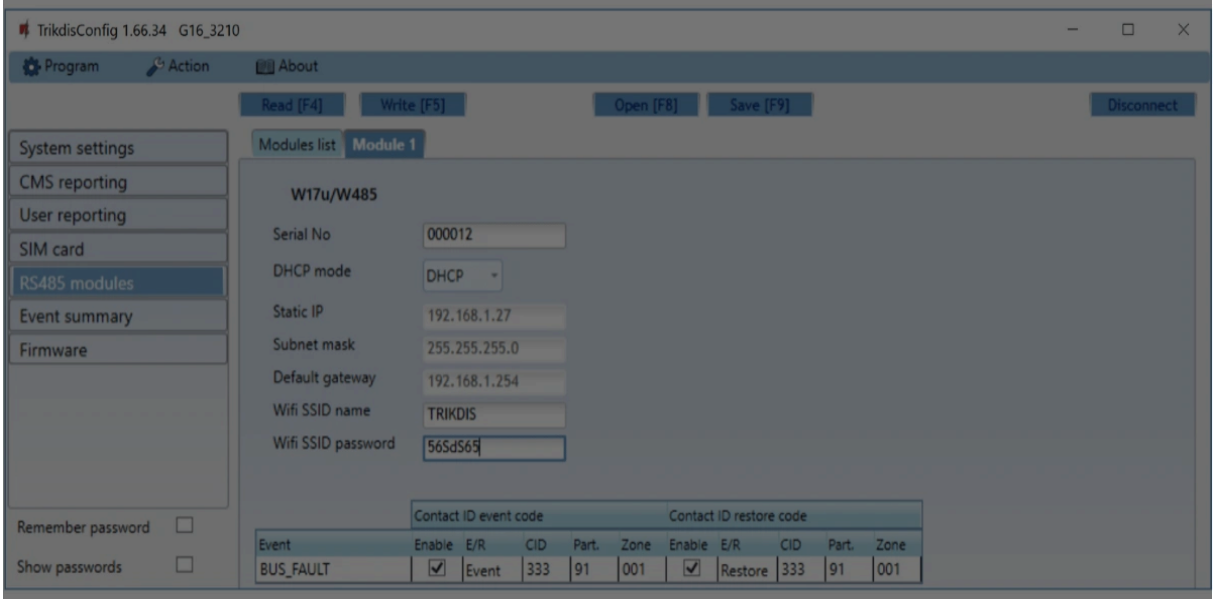
iO expander settings window



- **Input IN1 type** – set the input type (NO or NC).
- **Max °C(T1)** – when the temperature is higher than this setting, an event message will be generated. For an event message to be generated, it must be enabled in the table.
- **Min °C(T2)** – when the temperature is lower than this setting, an event message will be generated. For an event message to be generated, it must be enabled in the table.

In the table inputs can be assigned Contact ID event and restore codes. After an input is triggered, the communicator will send an event with the set event code to the monitoring station receiver and to Protegus app. Set as described in the previous page about **iO-8 expander settings window**.

WiFi module W485 settings window

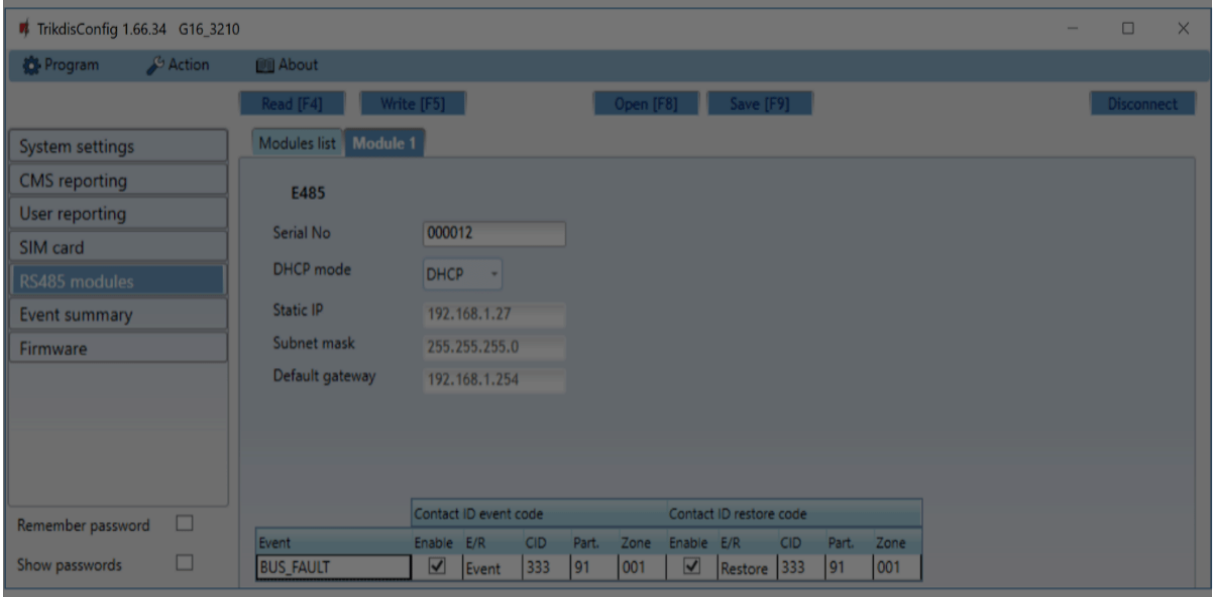


- **DHCP mode** – WiFi module's mode for registering to network (DHCP or Static).
- **Static IP** – static IP address for when static registering mode is set.
- **Subnet mask** – subnet mask for when static registering mode is set.
- **Default gateway** – gateway address for when static registering mode is set.
- **Wifi SSID name** – name of the WiFi network that the W485 will connect to

NOTE

You must configure the G16 to send messages to CMS and Protegus, see chapters 2.2 "Settings for connection with Central Monitoring Station" and 2.1 "Settings for connection with Protegus app". / **Insert SIM card into the communicator *G16* for *W485* to work.**

6.6.1 "Ethernet" module E485 settings window

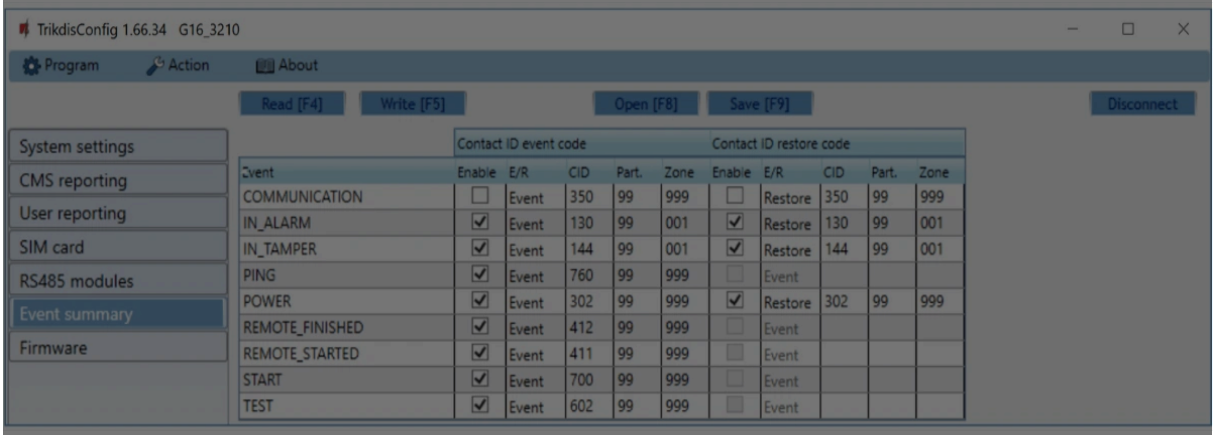


- **DHCP mode** – ethernet module's mode for registering to network (DHCP or Static).
- **Static IP** – static IP address for when static registering mode is set.
- **Subnet mask** – subnet mask for when static registering mode is set.
- **Default gateway** – gateway address for when static registering mode is set.

In the table, you can assign Contact ID event and restore codes to the RS485 data bus fault event. When connection between the E485 and G16 is disrupted or re-established, the G16 will send a message with the assigned CID code to the CMS and Protegus app.

6.7 “Event summary” window

This window allows you to turn on, off, and modify internal messages sent by your device. Disabling an internal message in this window will prevent it from being sent regardless of other settings.



In this window, you can turn on, turn off or change the internal event messages sent by the device. After turning off the internal event in this window, it will not be sent irrespective of other settings.

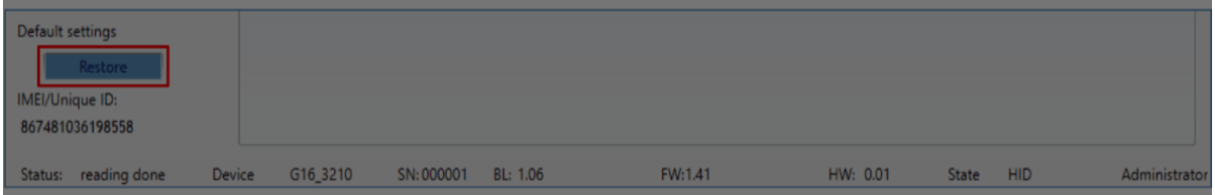
- **COMMUNICATION** – message about connection error between the control panel and G16.
- **IN_ALARM** – message about input (IN) circuit trigger.
- **IN_TAMPER** – message about input (IN) circuit tamper trigger.
- **PING** – PING heartbeat signal.
- **POWER** – message about low power supply voltage.
- **REMOTE_STARTED** – message about remote connection to configure G16 with TrikdisConfig.
- **REMOTE_FINISHED** – message about disconnection from remote configuration with TrikdisConfig.
- **START** – message about G16 connecting to the network.

- **Enable** – when selected, the sending of messages is enabled.

You can change the Contact ID code for each event, and also the zone and partition number.

6.8 Restoring factory settings

To restore the communicator's factory settings, you need to click the **Restore** button in the TrikdisConfig window.



7. Remote configuration

IMPORTANT

Remote configuration will work only if:

1. The inserted SIM card is activated and the PIN code is either entered or disabled;
2. Protegus cloud is enabled. How to enable cloud is described in section **0 **
3. **"User reporting"** window;
4. Power supply is connected ("POWER" LED illuminates green);
5. Registered to the network ("NETWORK" LED illuminates green and blinks yellow).

1. Start the configuration program TrikdisConfig.

3. (Optional) in the **System name** field, enter the desired name for the G16 with this Unique ID.
4. Press **Configure**.
5. In the newly opened window click **Read [F4]**. If required, enter the administrator or installer code. To save the password, select **"Remember password"**.
6. Set the necessary settings and when finished, click **Write [F5]**.

8. Test communicator performance

When the configuration and installation is complete, perform a system check:

1. Generate an event:

- by arming/disarming the system with the control panel's keypad;
- by triggering a zone alarm when the security system is armed.

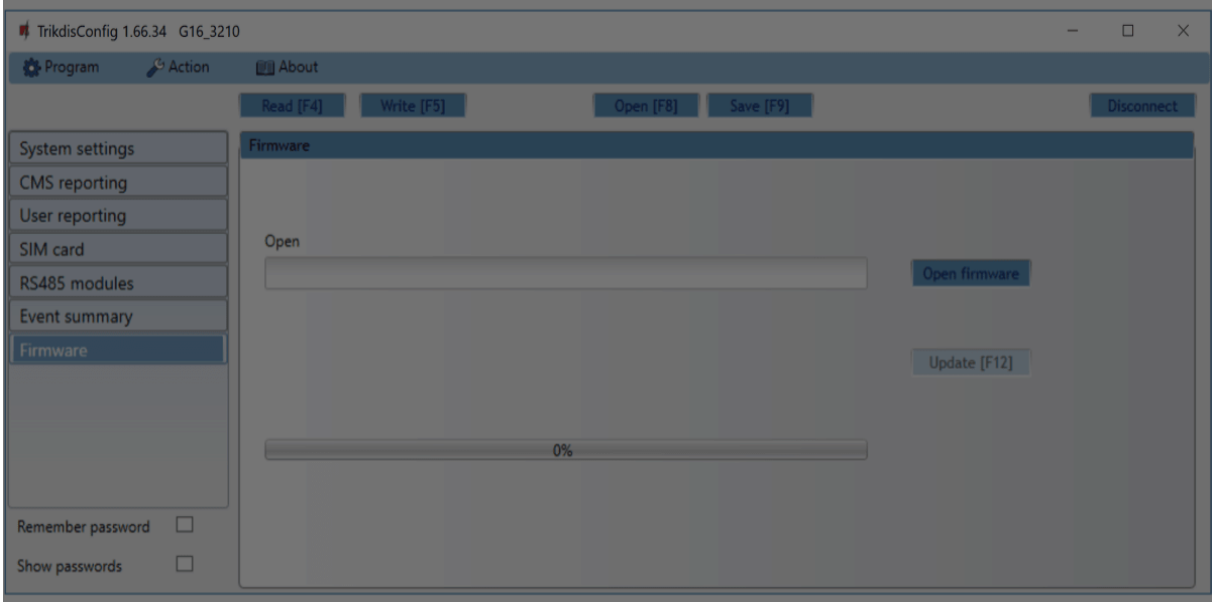
1. Make sure that the event arrives to the alarm receiving center and/or is received in the Protegus application.
2. To test communicator input, trigger it and make sure to receive the correct event.
3. To test the communicator outputs, activate them remotely and check their operation.
4. If the security control panel will be controlled remotely, arm/disarm the security system remotely by using the Protegus app.

9. Firmware update

NOTE

When the communicator is connected to TrikdisConfig, the program will automatically offer to update the device's firmware if updates are present. Updates require an internet connection.

2. Connect the communicator via USB cable to the computer or connect to the communicator remotely.
    - If a newer firmware version exists, the software will offer to download the newer firmware version file.
3. Select the menu branch **Firmware**.



4. Press **Open firmware** and select the required firmware file. If you do not have the file, the newest firmware file can be downloaded by registered users from www.trikdis.com , under the download section of the G16 communicator.
5. Press **Update [F12]**.
6. Wait for the update to complete.

10. Safety requirements

The communicator should be installed and maintained by qualified personnel.

Prior to installation, please read this manual carefully in order to avoid mistakes that can

11. Annex

The communicator can work with a SUR-GARD receiver. The communicator converts Contact ID codes received from the alarm control panel into SIA codes.

Contact ID to SIA code conversion table

System Event	CID Report Code	SIA Report Code
Medical alarm	E100	"MA"
Personal emergency	E101	"QA"
Fire in zone:	E110	"FA"
Water flow detected in zone:	E113	"SA"
Pull station alarm in zone:	E115	"FA"
Panic in zone:	E120	"PA"
Panic alarm by user:	E121	"HA"
Panic alarm in zone:	E122	"PA"
Panic alarm in zone:	E123	"PA"
Panic alarm in zone:	E124	"HA"
Panic alarm in zone:	E125	"HA"
Alarm active in zone:	E130	"BA"
Alarm active in zone:	E131	"BA"
Alarm active in zone:	E132	"BA"
Alarm active in zone:	E133	"BA"
Alarm active in zone:	E134	"BA"
Alarm active in zone:	E135	"BA"
Tamper active in zone:	E137	"TA"
Intrusion verified in zone:	E139	"BV"
Alarm active in zone:	E140	"UA"
System failure (143)	E143	"ET"
Tamper active in zone:	E144	"TA"
Tamper active in zone:	E145	"TA"
Alarm active in zone:	E146	"BA"
Alarm active in zone:	E150	"UA"
Gas detected in zone:	E151	"GA"
Water leakage detected in zone:	E154	"WA"
Foil break detected in zone:	E155	"BA"
High temperature at sensor:	E158	"KA"
Low temperature at sensor:	E159	"ZA"

System Event	CID Report Code	SIA Report Code
System shutdown	E308	"RR"
Battery failure (309)	E309	"YT"
Ground fault	E310	"US"
Battery failure (311)	E311	"YM"
Power supply overcurrent (312)	E312	"YP"
Engineer reset by user: (313)	E313	"RR"
Sounder/Relay failure	E320	"RC"
System failure (321)	E321	"YA"
System failure (330)	E330	"ET"
System failure (332)	E332	"ET"
System failure (333)	E333	"ET"
System failure (336)	E336	"VT"
System failure (338)	E338	"ET"
System failure (341)	E341	"ET"
System failure (342)	E342	"ET"
System failure (343)	E343	"ET"
System failure (344)	E344	"XQ"
System communication failure (350)	E350	"YC"
System communication failure (351)	E351	"LT"
System communication failure (352)	E352	"LT"
System failure (353)	E353	"YC"
System communication failure (354)	E354	"YC"
System failure (355)	E355	"UT"
Fire trouble in zone:	E373	"FT"
Trouble in zone:	E374	"EE"
Trouble in zone:	E378	"BG"
Trouble in zone:	E380	"UT"
Wireless zone fault:	E381	"US"

System Event	CID Report Code	SIA Report Code
Deferred disarm user	E405	"OR"
Alarm cancelled by user:	E406	"BC"
User disarmed remotely	E407	"OP"
Quick disarm	E408	"OP"
Remote disarm	E409	"OS"
Callback request made by CMS	E411	"RB"
Successful data download	E412	"RS"
Entry access denied for user	E421	"JA"
Entry by user	E422	"DG"
Forced Access zone	E423	"DF"
Exit access denied for user	E424	"DD"
Exit by user	E425	"DR"
User disarmed too early	E451	"OK"
User armed too late	E452	"OJ"
User Failed to Disarm	E453	"CT"
User Failed to Arm	E454	"CI"
Auto arm failed	E455	"CI"
Partial arm by user:	E456	"CG"
Exit violation by user:	E457	"EE"
System disarmed after alarm by user:	E458	"OR"
Recent arm user	E459	"CR"
Wrong code entered	E461	"JA"
Auto-arm time extended by user:	E464	"CE"
Device disabled (501)	E501	"RL"
Device disabled (520)	E520	"RO"
Wireless sensor disabled in zone: (552)	E552	"YS"
Zone bypassed	E570	"UB"
Zone bypassed	E571	"FB"
Zone bypassed	E572	"MB"

System Event	CID Report Code	SIA Report Code
System event (605)	E605	"JL"
System event (606)	E606	"LF"
Periodic test report with trouble	E608	"RY"
System event (622)	E622	"JL"
System event (623)	E623	"JL"
Time/Date was reset by user	E625	"JT"
Inaccurate Time/Date	E626	"JT"
System programming started	E627	"LB"
System programming finished	E628	"LS"
System event (631)	E631	"JS"
System event (632)	E632	"JS"
System not active (654)	E654	"CD"
Medical alarm restored	R100	"MH"
Personal emergency restored	R101	"QH"
No more fire alarm in zone :	R110	"FH"
No more water flow alarm in zone:	R113	"SH"
Panic alarm restored in zone:	R120	"PH"
Panic alarm cancelled by user:	R121	"HH"
Panic alarm restored in zone:	R122	"PH"
Panic alarm restored in zone:	R123	"PH"
Panic alarm restored in zone:	R124	"HH"
Panic alarm restored in zone:	R125	"HH"
No more alarm in zone:	R130	"BH"
No more alarm in zone:	R131	"BH"
No more alarm in zone:	R132	"BH"
No more alarm in zone:	R133	"BH"
No more alarm in zone:	R134	"BH"
No more alarm in zone:	R135	"BH"
No more tamper in zone:	R137	"TA"

System Event	CID Report Code	SIA Report Code
Foil break restored in zone:	R155	"BH"
Temperature has normalized at sensor:	R158	"KH"
Temperature has normalized at sensor:	R159	"ZH"
No more CO alarm in zone:	R162	"GH"
No more fire failure in zone:	R200	"FV"
Monitored restore alarm	R220	"BH"
No more system failure (300)	R300	"YA"
AC power supply OK	R301	"AR"
Battery OK	R302	"YR"
No more system failure (304)	R304	"YG"
System reset restored in zone:	R305	"RR"
No more battery failure (309)	R309	"YR"
Restore ground fault	R310	"UR"
No more battery failure (311)	R311	"YR"
Restore power supply overcurrent (312)	R312	"YQ"
No more sounder/Relay failure	R320	"RO"
No more system failure (321)	R321	"YH"
No more system failure (330)	R330	"ER"
No more system failure (332)	R332	"ER"
No more system failure (333)	R333	"ER"
No more system failure (336)	R336	"VR"
No more system failure (338)	R338	"ER"
No more system failure (341)	R341	"ER"
No more system failure (342)	R342	"ER"
No more system failure (344)	R344	"XH"
No more system communication failure (350)	R350	"YK"
No more system communication failure (351)	R351	"LR"
No more system	R352	"LR"

System Event	CID Report Code	SIA Report Code
No more wireless module failure (382)	R382	"BR"
No more tamper in zone:	R383	"TR"
Battery OK in wireless zone:	R384	"XR"
No more trouble in zone: (391)	R391	"NS"
No more trouble in zone: (393)	R393	"NS"
User armed the system	R400	"CL"
User armed the system	R401	"CL"
Automatic arm	R403	"CA"
User armed remotely	R407	"CL"
Quick arm	R408	"CL"
Remote arm	R409	“CS”
User armed to Stay mode	R441	"CG"
User armed too early	R451	“CK”
User disarmed too late	R452	“CJ”
User Failed to Disarm	R454	“CI”
Partial Arm by user:	R456	"CG"
Recent disarm user	R459	“CR”
Device enabled (501)	R501	"RG"
Device enabled (520)	R520	"RC"
Wireless sensor enabled in zone: (552)	R552	"YK"
Zone bypass cancelled	R570	"UU"
Zone bypass cancelled	R571	"FU"
Zone bypass cancelled	R572	"MU"
Zone bypass cancelled	R573	"BU"
Group bypass by user: cancelled	R574	"CF"
Zone bypass cancelled	R576	"UU"
Zone bypass cancelled	R577	"UU"
Vent zone bypass cancelled	R579	"UU"
Walk test deactivated by user	R607	"TE"