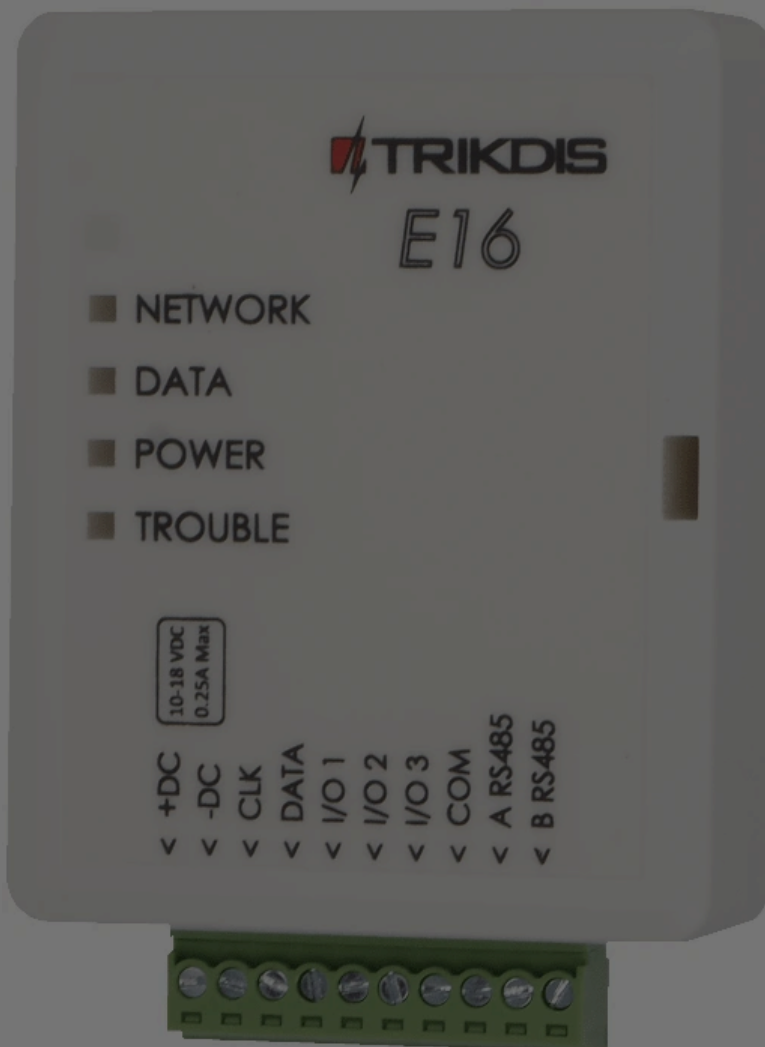


COMMUNICATORS

# Ethernet communicator E16



## I. Description

"Ethernet" communicator E16 directly connects to supported DSC, Paradox, UTC Interlogix

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics

Accept

Reject



For panels from other manufacturers use the E16T 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.
- 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 Protegus2 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 and installer.

### Notifies users:

- Users can be notified about events with Protegus2 app.

### Controllable outputs and inputs:

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



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

**Underlined** - Control panels directly controlled by E16. Firmware PARADOX security panels, which are directly controlled, must be V.4 or higher.

\*Connect control panels from other manufacturers to the E16T communicator.

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



## 1.3 Specifications

Parameter	Description
Dual purpose terminals [IN/OUT]	3, can be set as either NC; NO; NC/EOL; NO/EOL; NC/DEOL; NO/DEOL (2,2 kΩ) type inputs or open collector (OC) type outputs with current up to 0,15 A, 30 VDC max. Expandable with iO series expanders.
Power supply voltage	10-18 V DC
Current consumption	100 mA (on standby) Up to 250 mA (while sending data)
Ethernet connection	IEEE802.3, 10 Base-T, RJ45 socket
Transmission protocols	TRK, DC-09_2007, DC-09_2012, TL150
Message encryption	AES 128
Memory	Up to 60 messages
Changing settings	With TrikdisConfig computer program remotely or locally via USB Mini-B port
Operating environment	Temperature from -10 °C to 50 °C, relative humidity - up to 80% at +20 °C
Communicator dimensions	88 x 62 x 26 mm
Weight	80 g

## 1.4 Communicator elements

1. Light indicators.
2. Frontal case opening slot.
3. Terminal for external connections.
4. USB Mini-B port for communicator programming.
5. Ethernet connection RJ45 socket.



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



## 1.5 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
I/O 1	1st input/output terminal
I/O 2	2nd input/output terminal
I/O 3	3rd input/output terminal
COM	Common (negative) terminal
A RS485	RS485 bus A contact
B RS485	RS485 bus B contact

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics





## 1.6 LED indication of operation

Indicator	Light status	Description
NETWORK	Off	No connection to a computer network
NETWORK	Green solid	Communicator is connected to a computer network
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 ( $\leq 11.5V$ )
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	Connection error at the "physical" level (PHY Link status error), check LAN cable
TROUBLE	2 red blinks	DHCP error
TROUBLE	3 red blinks	DNS error
TROUBLE	6 red blinks	No connection with the receiver
TROUBLE	7 red blinks	Lost connection with control panel
TROUBLE	Red blinking	(Configuration mode) Memory fault
TROUBLE	Red solid	(Configuration mode) Firmware is corrupted

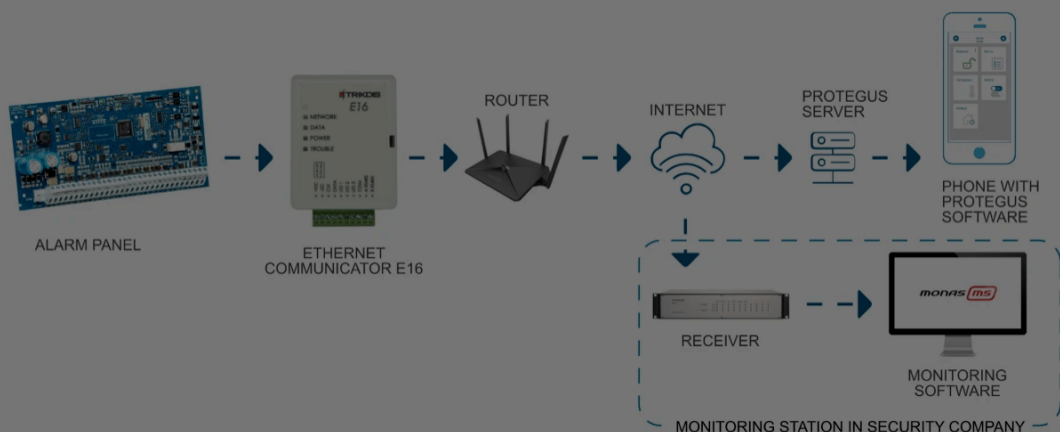
### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



## 1.7 Structural schematic with E16 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. 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](http://www.trikdis.com) (type "TrikdisConfig" in the search field) and install it.
2. Open the casing of the E16 with a flat-head screwdriver as shown below:

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics

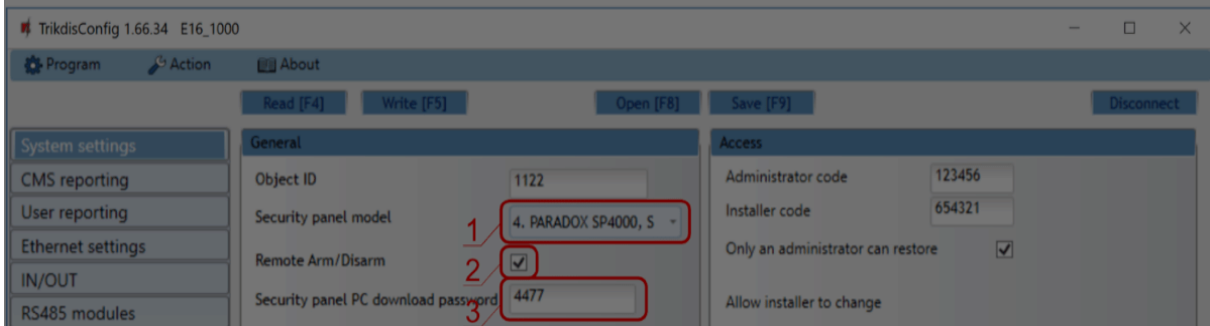


3. Using a USB Mini-B cable connect the E16 to the computer.
4. Run TrikdisConfig. The software will automatically recognize the connected communicator and will open a window for configuration.
5. Click **Read [F4]** to read the communicator's settings. If requested, enter the Administrator or Installer 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 CMS (central monitoring station) and to allow the security system to be controlled with the Protegus2 app.

## 2.1 Settings for connection with Protegus2 app

In "System settings" window:



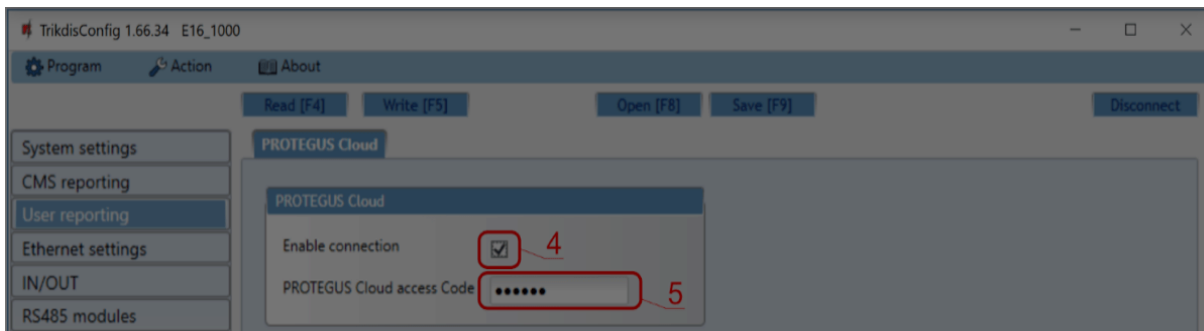
1. Select **Security panel model** that will be connected to the communicator.
2. Select **Remote Arm/Disarm** if you want users to be able to control the panel in Protegus2 app with their keypad code. This setting is only shown for directly controlled panels.
3. For the direct control of Paradox and Texecom panels enter **Security panel PC download password**. It must match the password that is entered in the control panel.

### NOTE

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



4. Tick the checkbox **Enable connection** to the Protegus Cloud.

5. Change the **Protegus Cloud access Code** for logging in to Protegus2 if you want users to be asked to enter it when adding the system to Protegus2 app (default password – 123456).

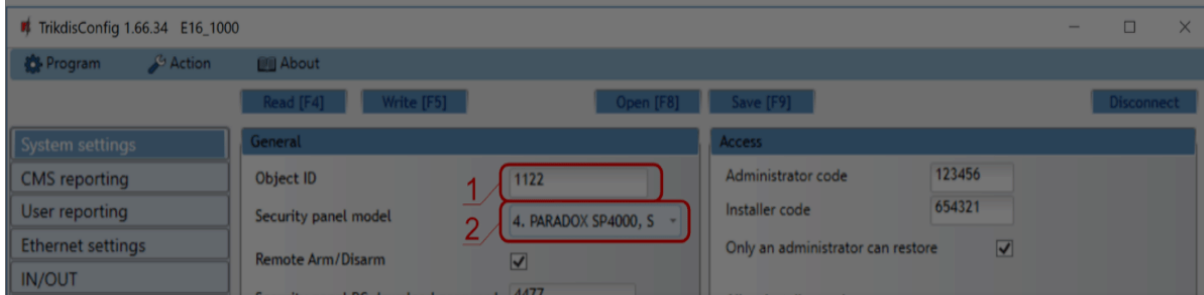
After finishing configuration, click the button **Write [F5]** and disconnect the USB cable.

#### NOTE

For more information about other E16 settings in TrikdConfig, see chapter 6 "[TrikdConfig window description](#)".

## 2.2 Settings for connection with Central Monitoring Station

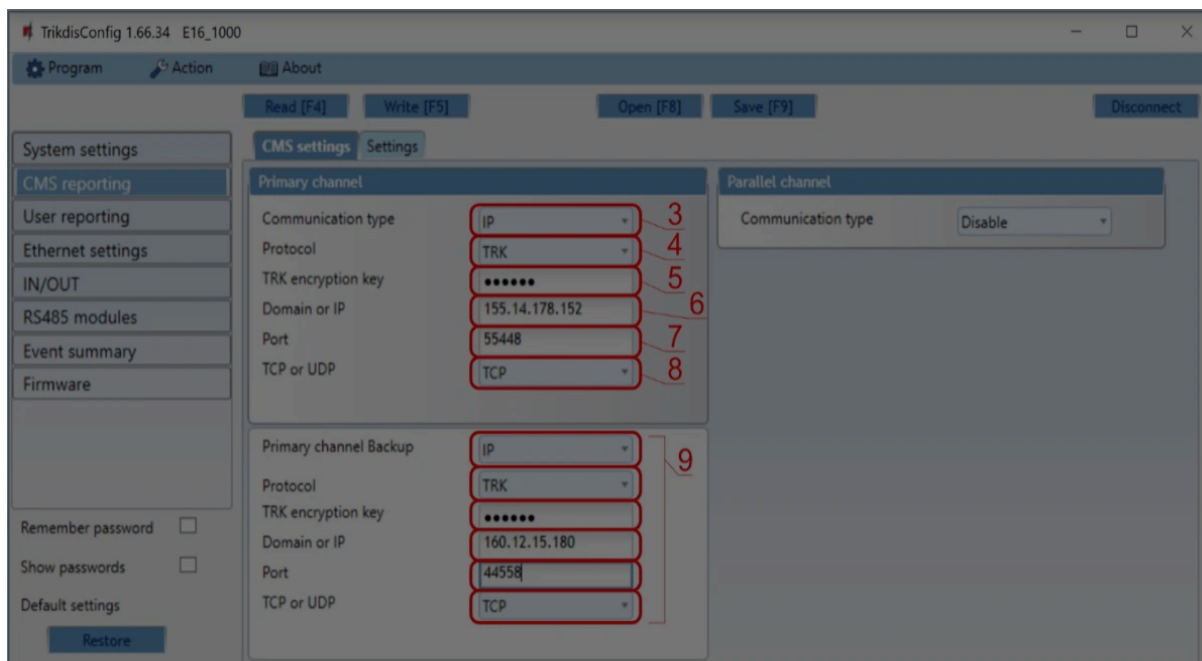
In "System settings" window:



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



3. **Communication type** - select the **IP** connection method.
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 selected the **DC-09** protocol, additionally enter object, line and receiver numbers in the **Settings** tab of the **CMS reporting** window.

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics

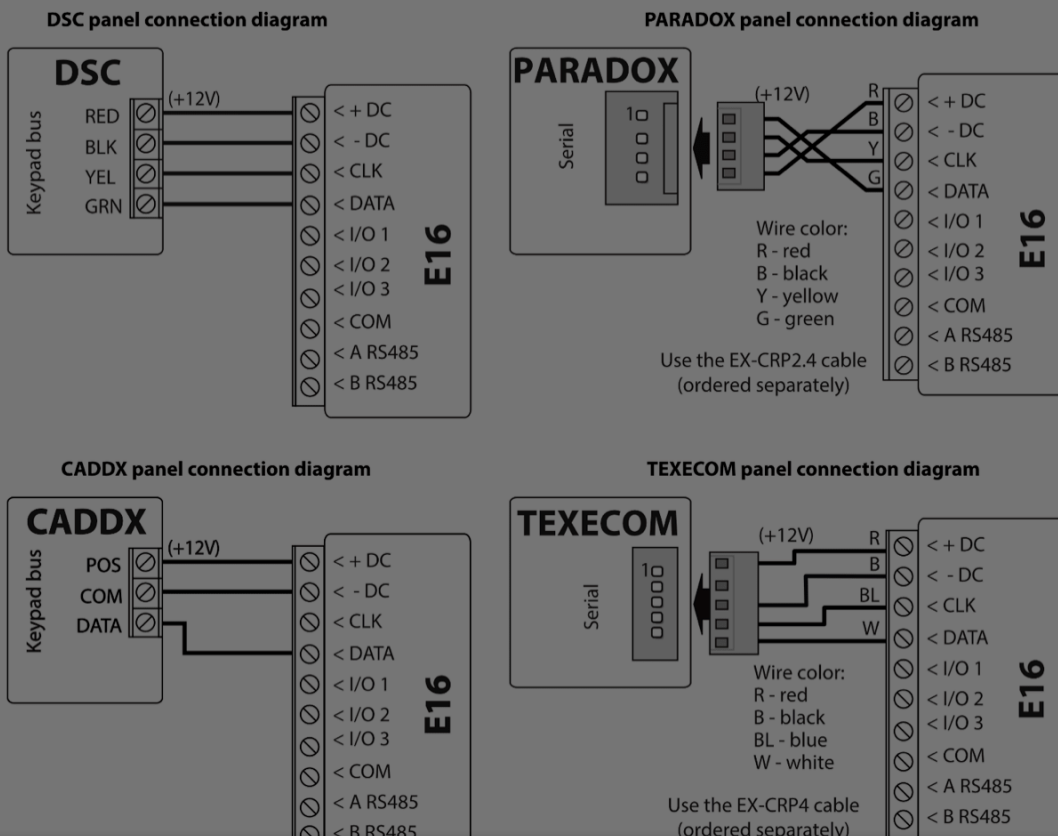
**NOTE**

For more information about other E16 settings in TrikdisConfig, see chapter 6 "TrikdisConfig window description".

## 3. Installation and wiring

### 3.1 Schematics for wiring the communicator to a security control panel

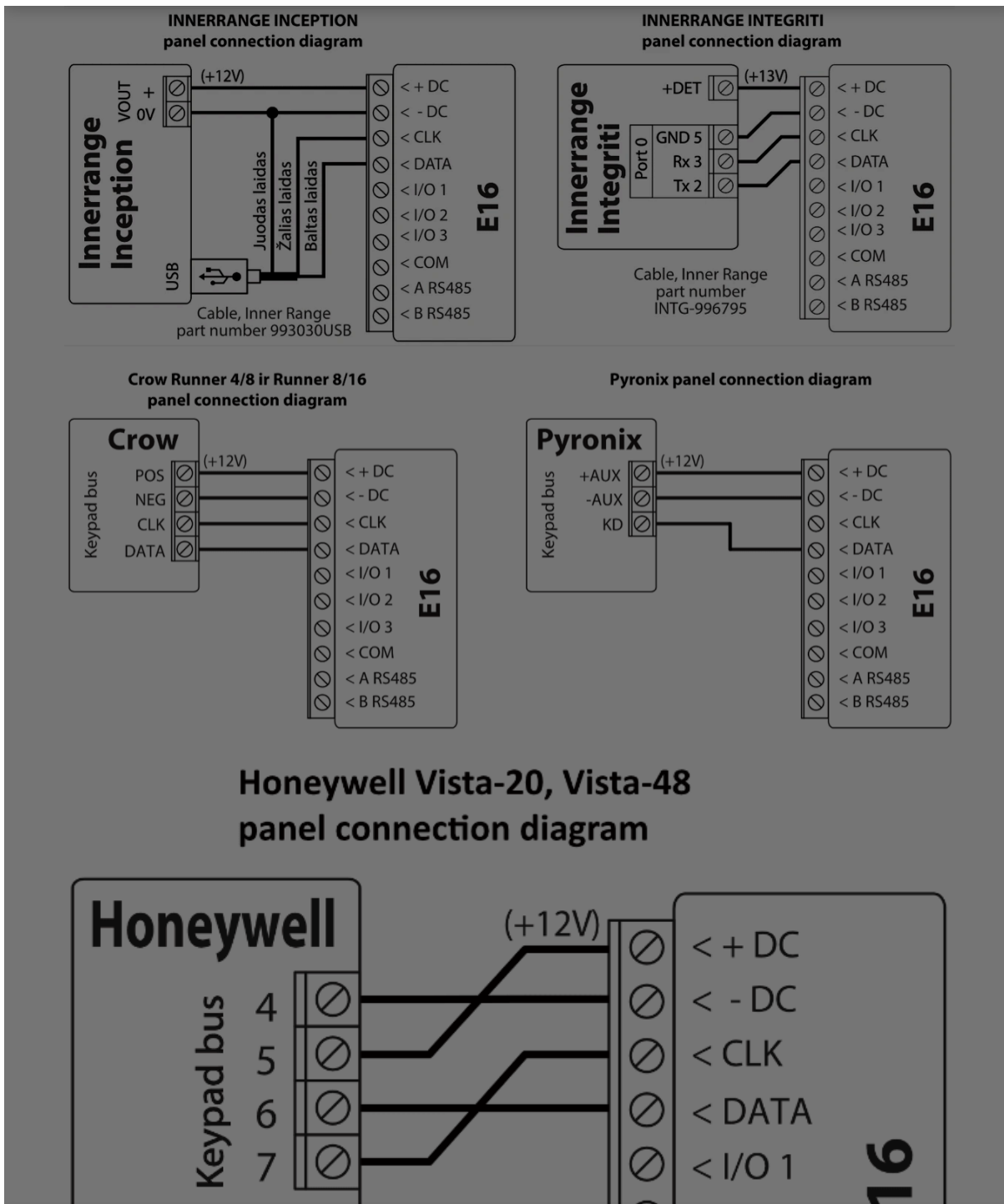
Following one of the schematics provided below, connect communicator to the control panel.



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



**Cookie consent**

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics

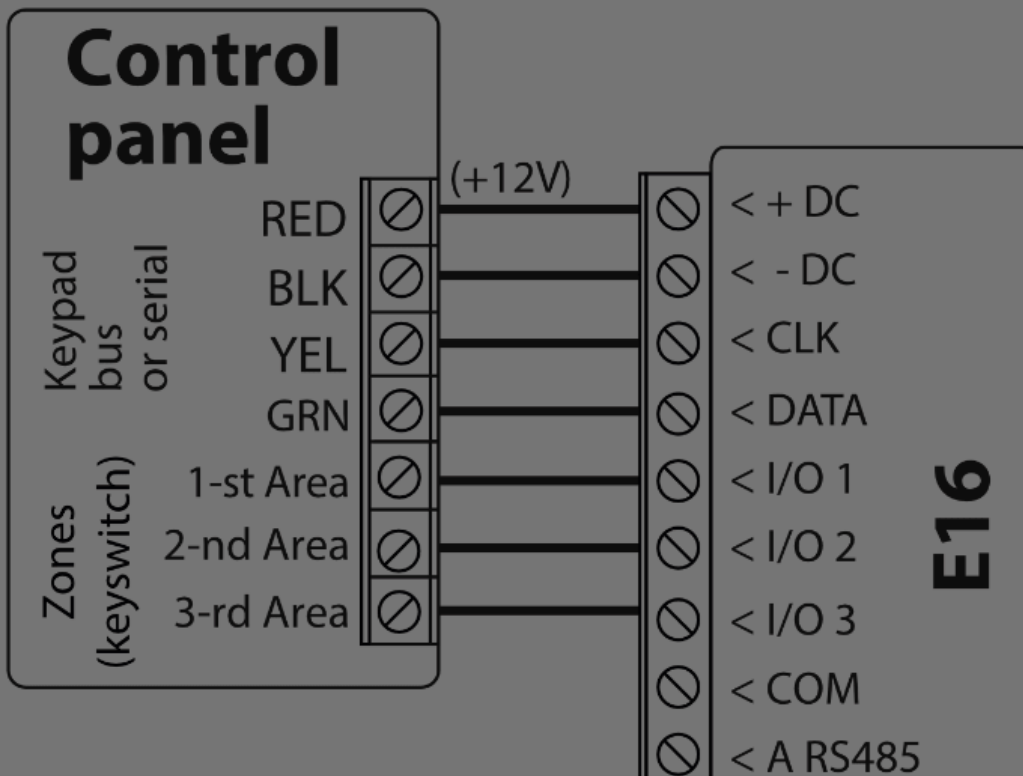


## 3.2 Schematic for connecting to panel keyswitch zone

Follow this schematic if the control panel will be armed/disarmed with a E16 PGM output turning on/off the panel's keyswitch zone.

### NOTE

E16 communicator has 3 universal input / output terminals that can be set to the OUT (PGM) operating mode. The outputs (OUT) can control three areas of the security system. If you want to control the system in this way, in TrikdisConfig, in the "System settings" window, uncheck **Remote Arm/Disarm**. The Protegus2 apps must be configured with the settings described in chapter 5.2 "Additional settings to arm/disarm the system using the control panel's keyswitch zone".



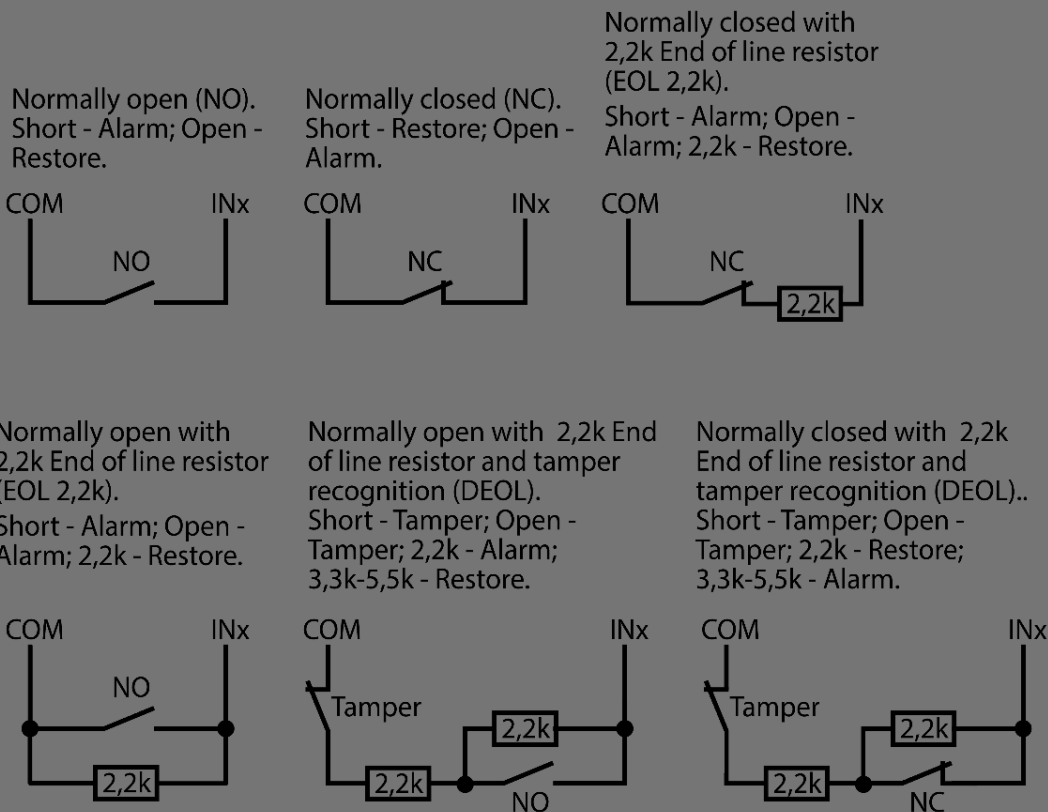
### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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".

### 3.4 Connect LAN cable

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

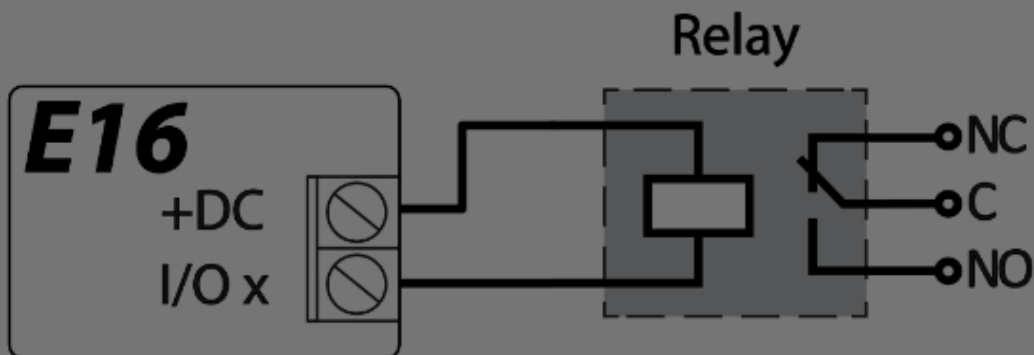
- Google Analytics





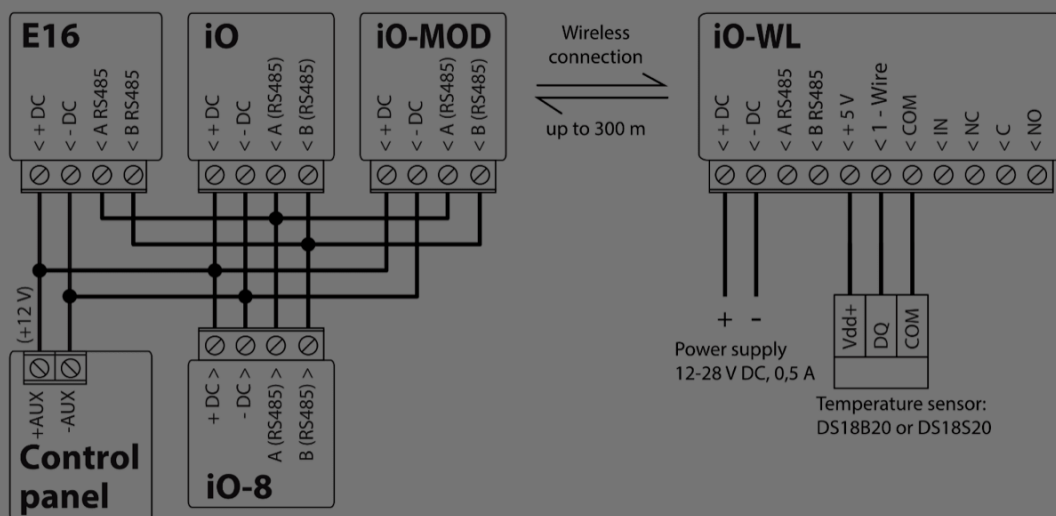
### 3.5 Schematics for wiring a relay

With relay contacts you can control (turn on/off) various electronic appliances. The I/O terminal of the communicator must be set to an output (OUT) mode.



### 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 E16 is described in chapter 6.6 "RS485 modules" window".



#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



#### NOTE

If you see a different LED indication, it indicates a certain malfunction. Diagnose it by following the LED indication table in chapter 1.5 "LED indication of operation". / If the E16 indication does not illuminate at all, check the power supply and connections.

## 4. Programming the control panel

Below it is described how to program the security control panel so that the E16 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.

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



The security control panel can be programmed with Texecom software - Wintex. Enter **UDL passcode** (4-digit code) in the **Communication Options** window, **Options** tab.

Also, you can program with a keypad connected to the security control panel:

1. Enter the 4-digit installer's code and press the [Menu] button to enter the programming menu.
2. Press the [9] key immediately afterwards.
3. Press [7][6], and then [2]. Enter the 4-digit **UDL passcode** (**UDL passcode** must match the E16 communicator's **PC login password**).
4. Press [Yes] and leave the programming mode by pressing [Menu].

#### 4.4 UTC INTERLOGIX (CADDX)

Security control panel version must be **V2** or higher 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

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



The control panel must be connected to the internet. Connect to **Innerrange Inception** by entering: <https://skytunnel.com.au/inception/SERIALNUMBER>, where SERIALNUMBER is the number of the controller that you can find on the panel's enclosure.

Open **Configuration > General > Alarm Reporting**. In the **3rd Party Device Configuration** settings group you need to enter:

The screenshot shows the 'Alarm Reporting' configuration page in the Inception web interface. The left sidebar contains a navigation menu with 'Configuration' selected. The main content area is titled 'Alarm Reporting' and includes a 'Reporting Format Configuration' section with fields for 'System Health Area Reporting ID' (90) and 'Repeat Alarm Event Limit (Swinger Shutdown)' (10). Below this is the '3rd Party Device Configuration' section, which is highlighted with red boxes and numbered 1, 2, and 3. Box 1 points to the 'Enable 3rd Party Device Reporting' checkbox, which is checked. Box 2 points to the '3rd Party Device Type' dropdown menu, which is set to 'Trikidis'. Box 3 points to the 'Serial Port' dropdown menu, which is set to 'Serial Port 1 (Plugged In, In Use By 3rd Party Device)'. Other settings in the '3rd Party Device Configuration' section include 'Enable Periodic Test Reporting' (unchecked), 'Test Report Frequency' (Daily), and 'Test Report Time of Day'. The bottom of the page shows 'Reporting Path Priorities'.

1. **Enable 3rd Party Device Reporting** - select this checkbox.
2. **3rd Party System Device Type** - set "Trikidis".
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 Trikidis communication protocol in the control panel configuration program. Contact ID data format. The port (TTL Port-0) of the security panel, to which the E16 communicator is connected, has the settings 19200, 8, N, 1. Save the settings and exit the program.

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



1. Enter the programming mode. Enter the installer code 4][1][1][2] and after that [8][0][0] . Alternatively, turn on the panel's power supply. In 50 seconds after the power supply is turned on, press the buttons [\*] and [#] at the same time (this method can be used when programming mode was exited by pressing in keypad [\*][9][8] ).
2. Turn on the sending of Contact ID events via LRR. Press [\*][2][9][1][#] in keypad.
3. When using the „Remote Arm/Disarm“ function, allow to use the 2nd AUI address. In keypad press [\*][1][8][9][1][1][#] .

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

### Crow

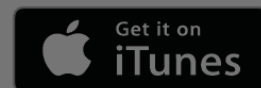
There is no need to program Crow Runner 4/8 and Runner 8/16 panels.

## 5. Remote control

### 5.1 Adding the security system to Protegus2 app

With Protegus2 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 Protegus2 application or use the browser version: [www.protegus.app](http://www.protegus.app).



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

#### IMPORTANT

When adding the E16 to Protegus2 check if:

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



4. Enter the system „Name“. Click "Next".

Scan QR code

Unique ID/IMEI

OR

Scan QR code

trikdis.com Made in EU CE

PRODUCT NAME

IMEI: XXXXXXXXXX

SN: XXXXXXXXXX

9-10V AC 0.2A  
10-18V DC 0.1A

Scan the QR code or fill in the text field.

Cancel Next

Enter the MAC address. You can find it here:  
- on the package;  
- on the PCB board;  
- TrikdisConfig as a Unique ID.

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

### ⚠ IMPORTANT

The control panel zone to which the E16 output OUT is connected to has to be set to keyswitch mode.

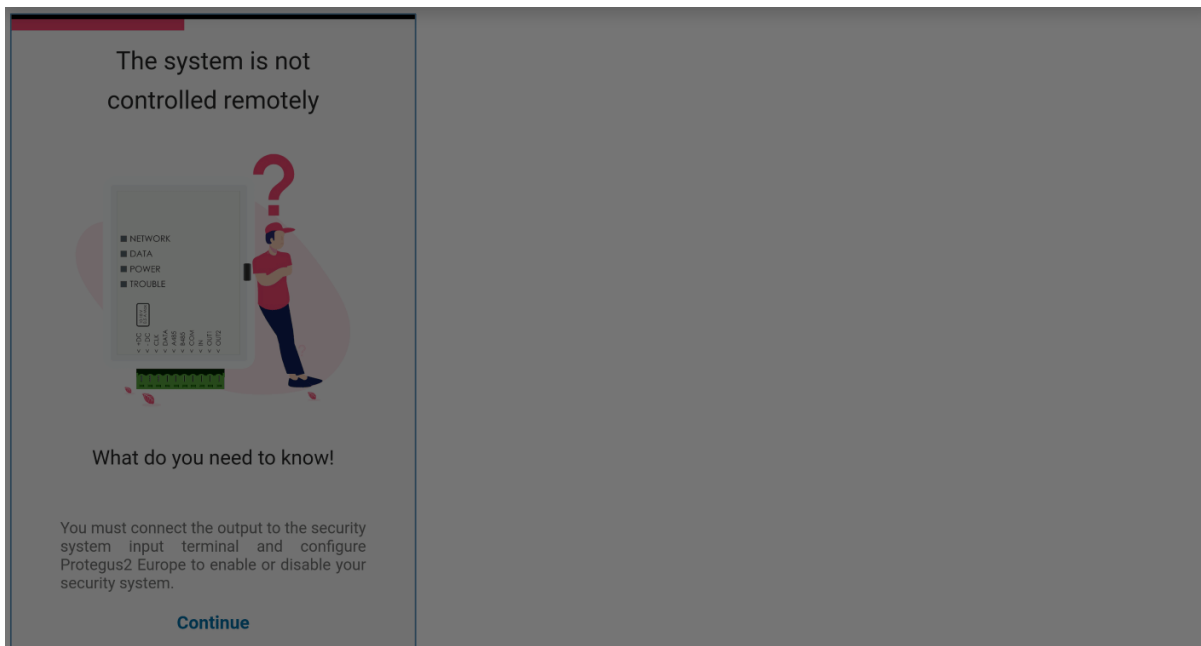
Follow the instructions below if the security control panel will be controlled with a E16 PGM output, turning on/off the control panel keyswitch zone.

1. Click „**Continue**“.

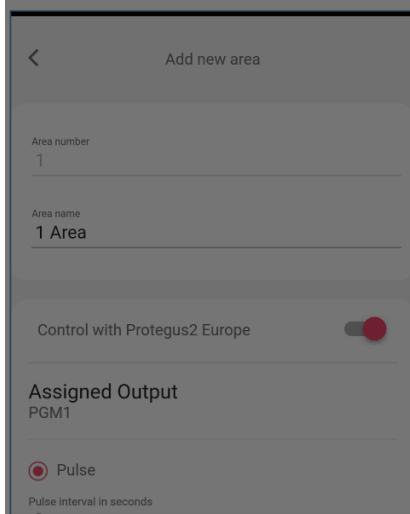
### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



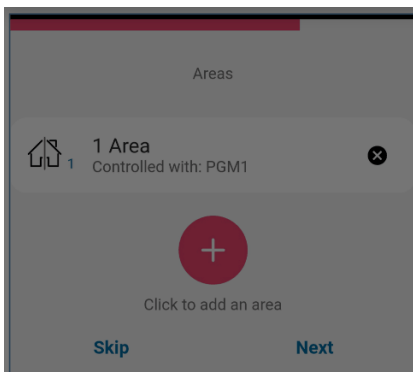
2. Enter **"Area name"**. Enable PGM output control using the Protegus2 application.
3. Select **"Pulse"** or **"Level"**, depending on how the keyswitch zone type is configured. If necessary, you can change the **"Pulse"** interval.
4. Click **"Save"**.



## Cookie consent

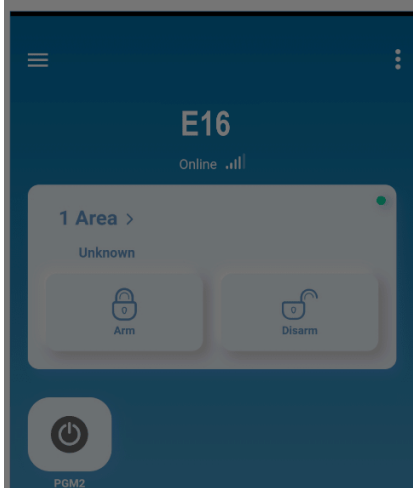
We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



## 5.3 Arming/disarming the alarm system with Protegus2

1. In the "System Home Screen" window, click on the "Disarm" status icon.
2. *Protegus2* will receive a message about a change in the status of the security system and the status icon will change its state.



## 6. TrikdisConfig window description

### 6.1 *TrikdisConfig* status bar description

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

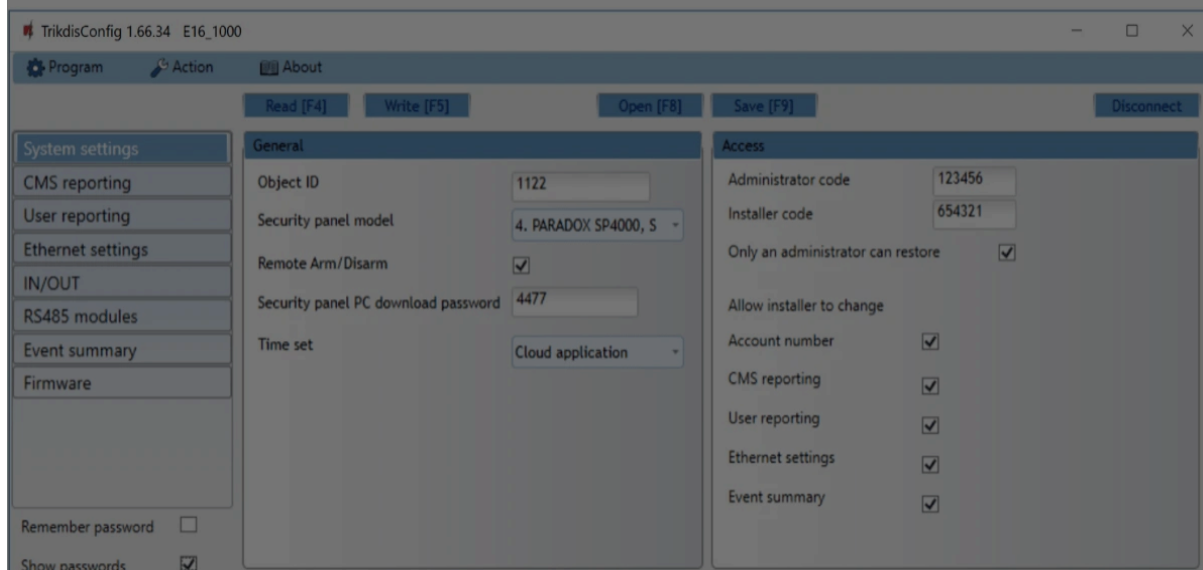
Google Analytics



Object	Description
MAC/Unique ID	Device MAC number
Status	Operating condition
Device	Device type (E16 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 **E16**. Set the necessary settings according to the TrikdConfig window descriptions given below.

## 6.2 "System settings" window



### "General" settings group

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



- **Security panel PC download 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".
- **Time set** - select which server to use for time synchronization.

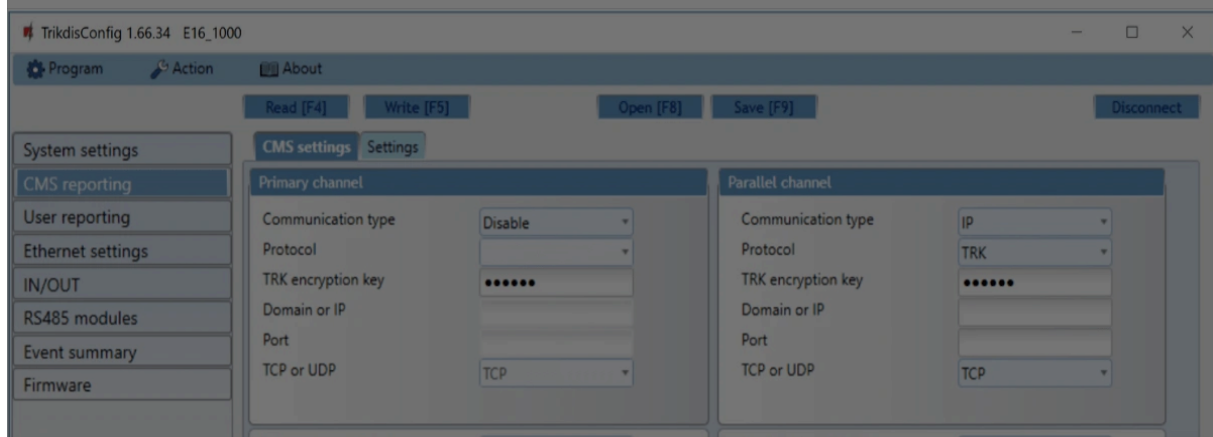
"Access" settings group

When setting up the communicator E16 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

### "CMS settings" tab



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



The communicator sends events to the monitoring station via a wired internet (IP) connection.

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.

#### “Primary channel” settings group

- **Communication type** - select which method for connecting to the monitoring station receiver will be used (IP).
- **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.

#### “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.

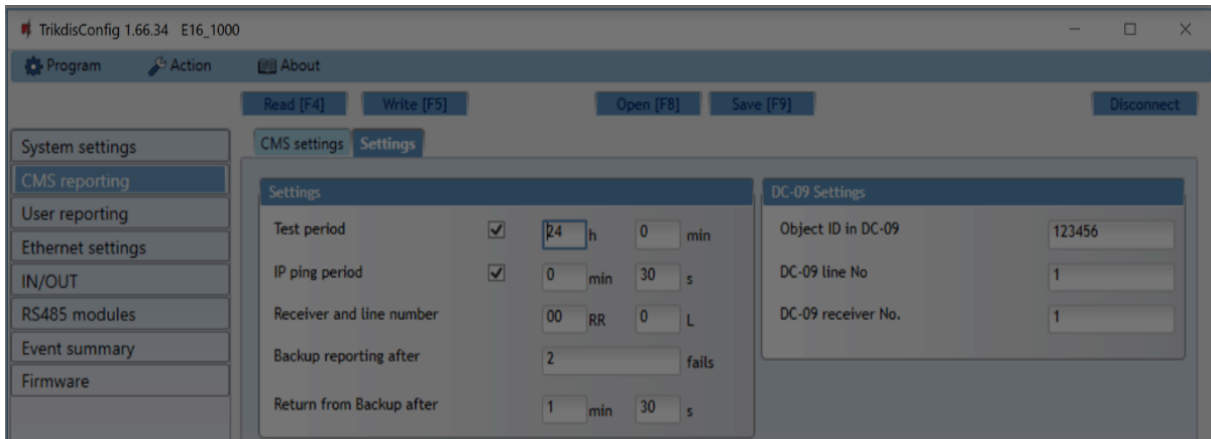
#### “Parallel channel” settings group

Events are transmitted in parallel with the first channel through this channel. When the

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



### **\*\*“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 device will connect to transmit the messages via Backup channel.
- **Return from backup after** - time after which the E16 will attempt to reconnect and

### **Cookie consent**

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics

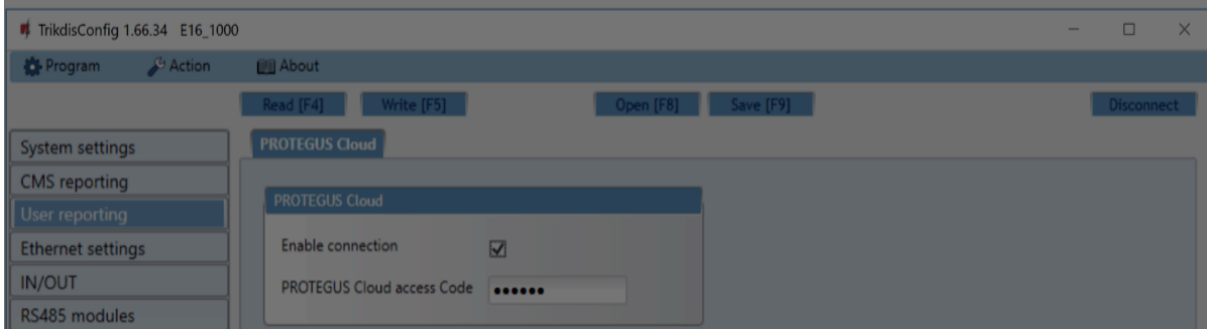


station).

- **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

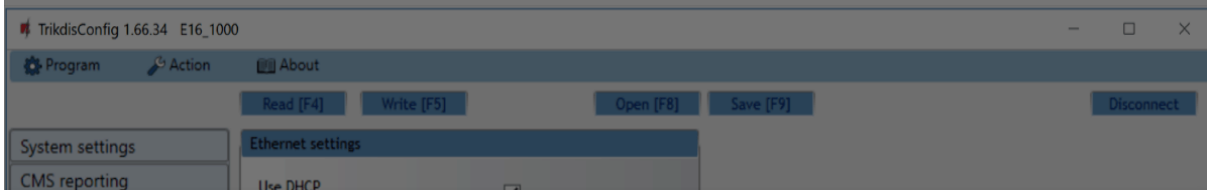


Protegeus service allows users to remotely monitor and control the communicator. For more information about Protegeus service, visit [www.protegeus.app](http://www.protegeus.app).

### “Protegeus Cloud” settings group

- **Enable connection** – enable the Protegeus service, the E16 will be able to exchange data with Protegeus2 app and to be remotely configured via ***TrikdConfig***.
- **Protegeus Cloud access Code** - 6-digit code for connecting to the Protegeus2 app (default - 123456).

## 6.5 “Ethernet settings” window



### Cookie consent

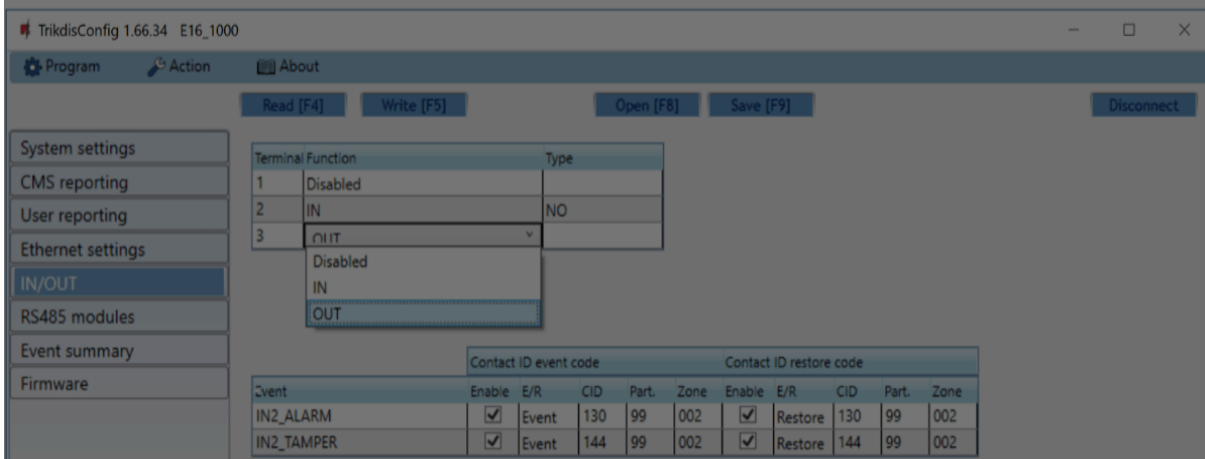
We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



- **Static IP** – static IP address for when manual registering mode is set.
- **Subnet mask** – subnet mask for when manual registering mode is set.
- **Default gateway** – gateway address for when manual registering mode is set.
- **DNS1, DNS2** - (Domain Name System) identifies the server that specifies the IP address of the domain. Used when domain is set in the communication channel **Domain or IP** field (not IP address). Google DNS server is set by default.

## 6.6 “IN/OUT” windows



The communicator has 3 universal (input / output) terminals. The table can set the terminal operating mode (Off, IN, OUT). The input must specify the type of circuit to be connected NC, NO, NO / EOL, NC / EOL, NO / DEOL, NC / DEOL.

Additional sensors can be connected to the communicator inputs. When the sensor is triggered, the communicator will send an event message. The input is assigned a Contact ID code, which will be sent to CMS and Protegus2.

- **Enable** – checked event fields where messages will be sent to CMS and Protegus2.
- **E/R** – choose what type of event will be sent when input is triggered – **Event** or **Restore**.
- **CID** – enter the event code or leave the default value. Upon entering the event, the event code will be sent to Protegus2 and CMS.

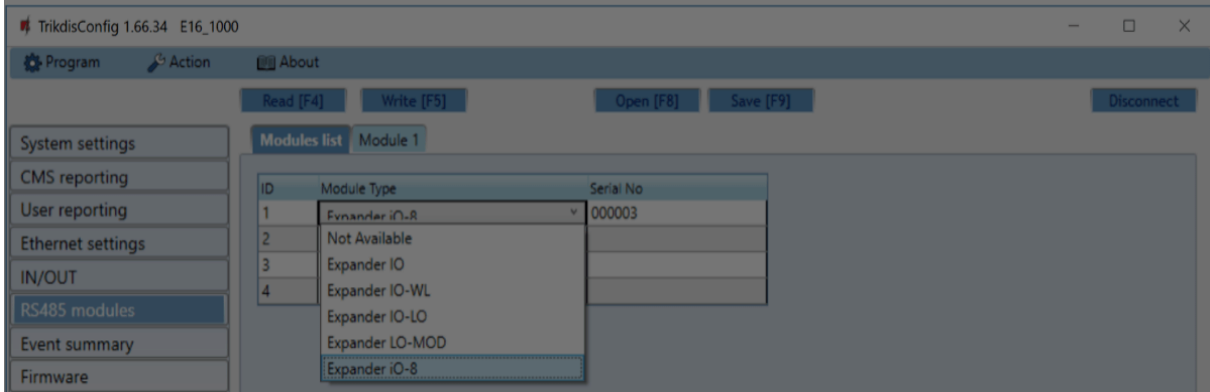
### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



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.



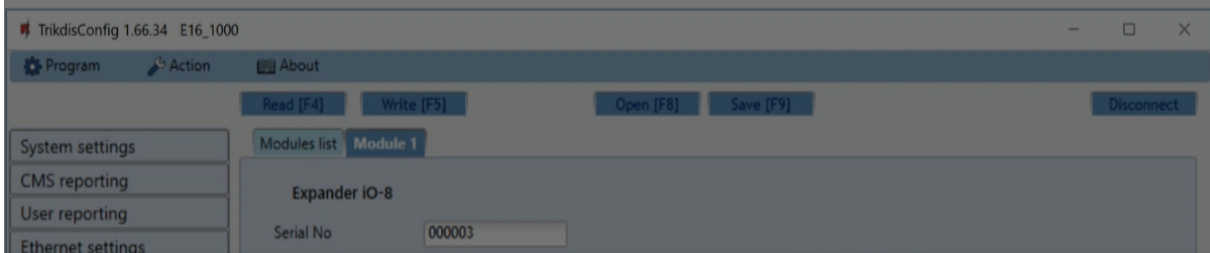
- **Module type** – select the module that is connected to the communicator via RS485 from the list.
- **Serial No** – enter the module serial number (6 digits), which is indicated on stickers on the module's case and packaging.

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. Below we describe the settings for iO-8 and iO series expanders.

### iO-8 expander settings window



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



- **Input Count** – select what number of terminal contacts should be set to input (IN) mode. The rest of the terminal contacts will become outputs (OUT).

Settings for controllable outputs are set directly in Protegus2 app. There you can assign an output for arming/disarming the alarm system or for remote control of devices.

In the table inputs can be assigned Contact ID event and restore codes. After input is triggered, the communicator will send an event with set event code to monitoring station receiver, Protegus2 app.

#### **Contact ID event code:**

- **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\*:**

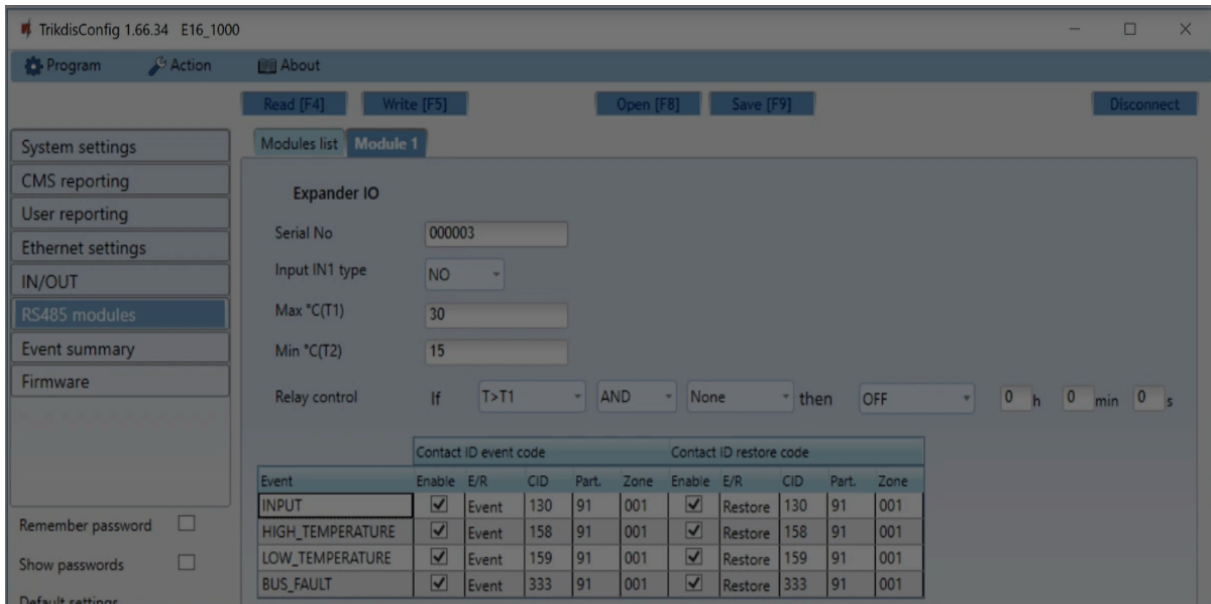
- **Enable** – allow message transmission when the input is restored.
- **E/R** – choose what type of event will be sent when input is restored – **Restore** or **Event**.
- **CID** – assign the Contact ID restore code to the input.
- **Part.** – assign the partition (area) to the input. It is set automatically: 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.
- **Input type** – select the type of the input (NO or NC).

#### **iO expander settings window**

#### **Cookie consent**

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



Expander iO has: terminals for 1 input, 1 output (relay contacts) and 1-Wire serial bus for connecting temperature sensors.

Relay output can be controlled according to logical (AND, OR, XOR) conditions.

- **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.
- **Relay control** – set logical (AND, OR, XOR) conditions, upon which the relay output will be controlled.

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 Protegus2 app. Set as described in the previous page about **iO-8 expander settings window**.

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



TrikdisConfig 1.66.34 E16_1000											
Program Action About											
Read [F4] Write [F5] Open [F8] Save [F9] Disconnect											
System settings	Contact ID event code						Contact ID restore code				
Event	Enable	E/R	CID	Part.	Zone	Enable	E/R	CID	Part.	Zone	
COMMUNICATION	<input type="checkbox"/>	Event	350	99	999	<input type="checkbox"/>	Restore	350	99	999	
POWER	<input checked="" type="checkbox"/>	Event	302	99	999	<input checked="" type="checkbox"/>	Restore	302	99	999	
REMOTE_FINISHED	<input checked="" type="checkbox"/>	Event	412	99	999	<input type="checkbox"/>	Event				
REMOTE_STARTED	<input checked="" type="checkbox"/>	Event	411	99	999	<input type="checkbox"/>	Event				
START	<input checked="" type="checkbox"/>	Event	700	99	999	<input type="checkbox"/>	Event				
TEST	<input checked="" type="checkbox"/>	Event	602	99	999	<input type="checkbox"/>	Event				

- **COMMUNICATION** – message about connection error between the control panel and E16.
- **POWER** – message about low power supply voltage.
- **REMOTE\_STARTED** – message about remote connection to configure E16 with TrikdisConfig.
- **REMOTE\_FINISHED** – message about disconnection from remote configuration with TrikdisConfig.
- **START** – message about E16 connecting to the network.
- **TEST** – periodic test message.

#### NOTE

To enable periodic TEST messages and set their period, go to **CMS reporting** -> **Settings** -> **Test period**.

- **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.

## 9.0 Restoring factory settings

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



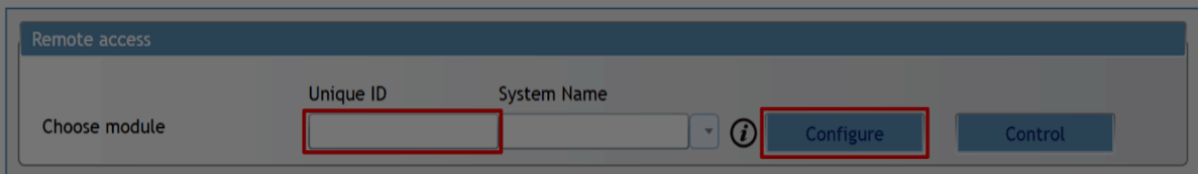
## 7. Remote configuration

### IMPORTANT

Remote configuration will work only if:

1. Protegus cloud is enabled. How to enable cloud is described in section 6.4 "User reporting" window";
2. Power supply is connected ("POWER" LED illuminates green);
3. Registered to the network ("NETWORK" LED illuminates green).

1. Start the configuration program TrikdisConfig.
2. In the **Remote access** section enter the communicator's **MAC** number. This number can be found on the device and the packaging sticker.



3. (Optional) in the **System name** field, enter the desired name for the E16 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

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



1. Make sure that the event arrives to the CMS (central monitoring station) and/or is received in the Protegus2 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 Protegus2 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. Antivirus software, firewall or strict access to internet settings can block the automatic firmware updates. In this case, you will need to reconfigure your antivirus program.

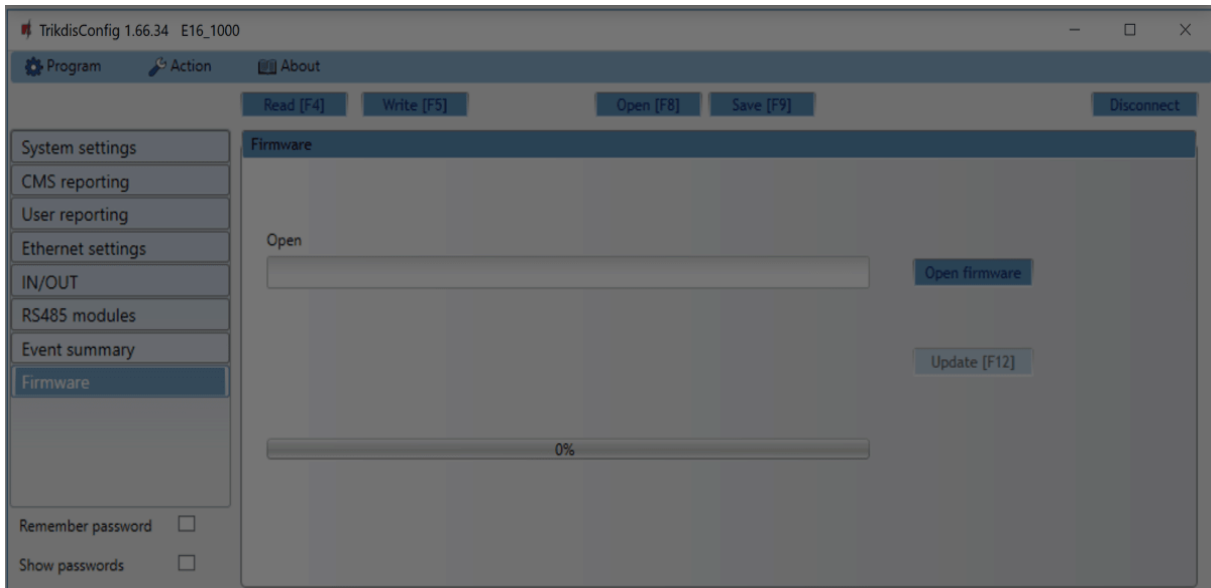
The communicator's firmware can also be updated or changed manually. After an update, all previously set settings will remain unchanged. When writing firmware manually, it can be changed to a newer or older version. To update:

1. Run ***TrikdisConfig***.
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**.

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

- Google Analytics



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](http://www.trikdis.com), under the download section of the E16 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 lead to malfunction or even damage to the equipment.

Disconnect the power supply before making any electrical connections.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.



### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



## 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

#### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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"

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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"

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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"

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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"

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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 communication failure (352)	R352	"LR"

## Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics



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	"TF"

### Cookie consent

We use cookies to measure the effectiveness of our documentation and whether users find what they're searching for. With your consent, you're helping us to make our documentation better.

Google Analytics