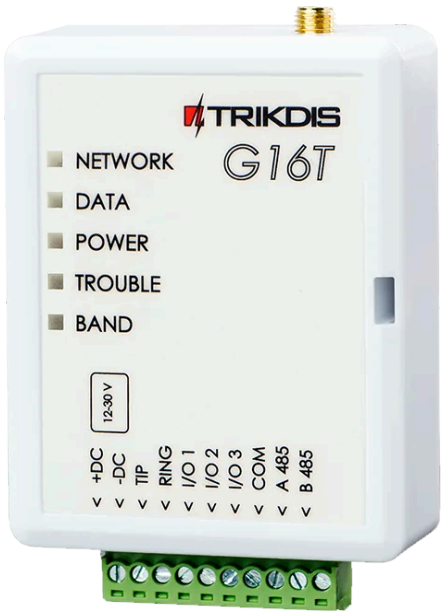
# Comunicatore G16T – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente del comunicatore Trikdis G16T: collegamento alla centrale d'allarme, scheda SIM e configurazione in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2, verifica e risoluzione dei problemi.




Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-g16t

# Indice


## 1. Panoramica

1.1 A cosa serve, come funziona
1.2 Versioni
1.3 Caratteristiche principali
1.4 Le parti del comunicatore
1.5 Morsetti
1.6 Segnalazioni LED
1.7 Dati tecnici

## 2. Messa in servizio rapida con TrikdisConfig

2.1 Preparativi
2.2 Collegamento all'app Protegus 2
2.3 Collegamento alla centrale di vigilanza

## 3. Installazione e collegamento

3.1 Fasi dell'installazione
3.2 Posizionamento e antenna
3.3 Collegamento alla centrale d'allarme
3.3.1 Se necessario: supervisione della linea
3.4 Collegamento della zona a chiave
3.5 Collegamento degli ingressi
3.6 Collegamento di un'uscita con relè
3.7 Collegamento dell'espansione iO-8
3.8 Collegamento dei moduli W485 ed E485
3.9 Accensione e primo controllo
A TRIKDIS átjelző elindítása

## 4. Programmazione della centrale d'allarme

4.1 Programmazione del combinatore Honeywell Vista
4.2 Centrali di altri produttori

## 5. Comando a distanza con l'app Protegus 2

5.1 Aggiunta del dispositivo
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Inserimento e disinserimento con un'uscita
5.3 Inserimento e disinserimento dall'app
5.4 Comando con messaggi SMS

## 6. TrikdisConfig – le impostazioni in dettaglio

6.1 La barra di stato
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 SIM card
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Ripristino delle impostazioni di fabbrica

**7. Programmazione a distanza**

**8. Verifica del funzionamento del comunicatore**

**9. Aggiornamento del firmware**

**10. Risoluzione dei problemi e domande frequenti**

**11. Norme di sicurezza**

**Vedi anche**

# 1. Panoramica

Il G16T è il **comunicatore cellulare universale** di Trikdis: si collega all'uscita della linea telefonica (TIP/RING) della centrale d'allarme e si comporta come una centrale telefonica. La centrale d'allarme „compone il numero", invia il messaggio Contact ID con toni DTMF, e il G16T risponde alla linea, decodifica il messaggio e lo inoltra tramite connessione dati mobile al ricevitore della centrale di vigilanza e al cloud Protegus, nell'app dell'utente. Così si può usare con **una centrale di qualsiasi marca** che abbia un combinatore Contact ID – non serve sostituire la centrale, basta impostarne il combinatore. I comunicatori G16T sono certificati per il grado di sicurezza più alto, **EN 50131 Grade 4**.

## 1.1 A cosa serve, come funziona

- **Trasmette alla centrale di vigilanza.** Invia gli eventi via IP al ricevitore software o hardware Trikdis (protocollo TRK) – questi funzionano con qualsiasi software di vigilanza – oppure a qualsiasi ricevitore universale (SIA DC-09 2007/2012, SUR-GARD TL150). Verso un ricevitore SUR-GARD converte i codici Contact ID ricevuti dalla centrale in codici SIA; la tabella di conversione si trova nell'appendice della documentazione Trikdis in inglese. Per impostazione predefinita controlla la connessione ogni 30 secondi (o all'intervallo impostato) e in caso di errore passa al canale di riserva.
- **Avvisa l'utente.** L'app Protegus 2 mostra gli eventi con notifiche push, con un suono dedicato e in un elenco eventi; dall'app l'utente può inserire e disinserire il sistema e comandare i dispositivi collegati (luci, cancello, ventilazione, riscaldamento, irrigazione ecc.). L'app funziona con tutte le centrali d'allarme a cui è collegato il comunicatore, indipendentemente dal produttore della centrale.
- **Insieme o separatamente** funziona con la centrale di vigilanza e con l'utente: si può usare solo con Protegus 2 (senza centrale di vigilanza), solo con la centrale di vigilanza, oppure con entrambe. Se sono impostate entrambe, l'evento viene inviato prima alla centrale di vigilanza, poi all'utente.
- **Riserva SMS.** Avvisa la centrale di vigilanza anche via SMS se la connessione dati nella rete dell'operatore non funziona; può inviare in parallelo a due ricevitori, ciascuno con un proprio canale di riserva.
- **Ha ingressi e uscite propri.** Tre morsetti I/O a doppia funzione si possono usare come ingresso (rilevatore, tamper) o come uscita comandabile (zona a chiave, relè). Sul bus RS485 della versione 4G, con l'espansione iO-8 si aggiungono altri 8 I/O (con altre espansioni cablate o senza fili della serie iO ulteriori ingressi e uscite, con l'espansione iO o iO-WL il monitoraggio remoto della temperatura), e con il modulo W485 o E485 può comunicare anche tramite WiFi o Internet cablato – in questo caso la rete mobile è la via di riserva.

La struttura del sistema è mostrata nella figura seguente: l'uscita della linea telefonica della centrale d'allarme si collega al G16T, il G16T raggiunge Internet tramite la rete mobile, da lì il ricevitore della centrale di vigilanza e il cloud Protegus, e l'utente vede il sistema nell'app Protegus 2.

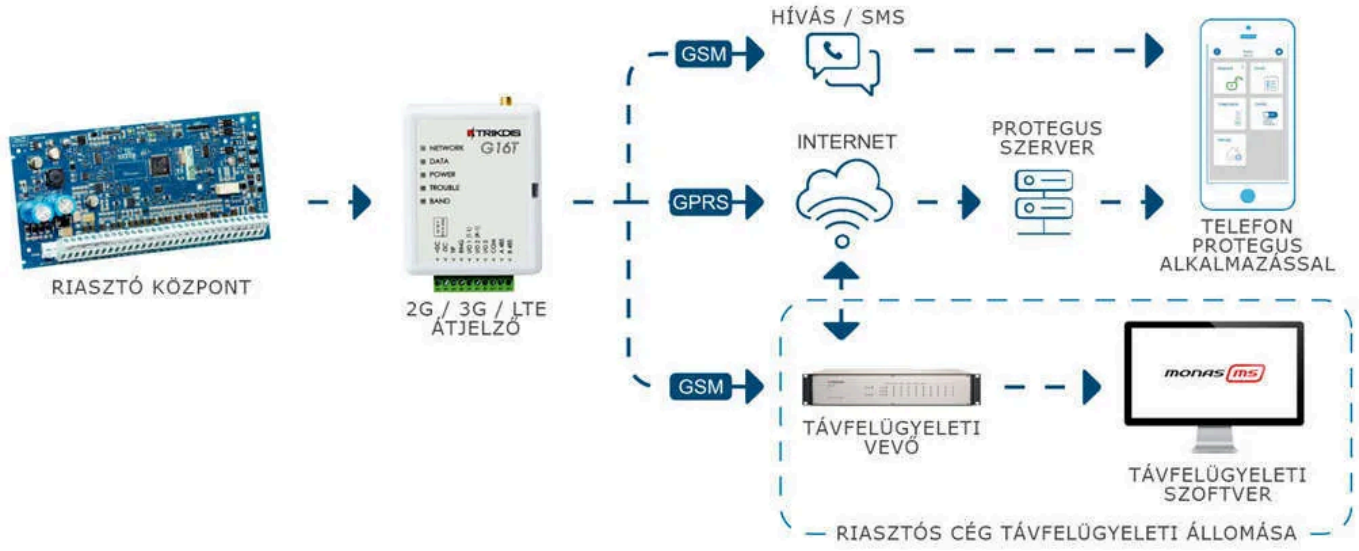



**Figura 1.** La posizione del G16T nel sistema: centrale d'allarme → G16T → rete mobile → ricevitore della centrale di vigilanza e cloud Protegus → app Protegus 2.

## 1.2 Versioni

Questo manuale è stato scritto per la **versione hardware 4** del G16T, ma **si può usare anche per la versione hardware 3**: il collegamento, la configurazione e il funzionamento delle due versioni sono in gran parte identici. Le differenze sono riassunte nella tabella seguente; dove il testo riporta il dato della versione 4, per la versione 3 tieni conto di questa tabella.

| | **Hardware 3 (v3)** | **Hardware 4 (v4)** |
|---|---|---|
| Tipi | G16T_321x (2G), G16T_331x (3G), G16T_341x (4G), G16T_3M10 (LTE Cat-M1 + 2G) – tutti con 1 scheda SIM | G16T_G410 (2G), G16T_E120 (4G, con riserva 2G) |
| Ingressi/uscite | 2 ingressi di tipo selezionabile (T-1/IN1, R-1/IN2 – utilizzabili anche per la supervisione della linea telefonica) + 1 uscita open collector (OUT, max. 0,15 A) | 3 morsetti I/O a doppia funzione (I/O 1, I/O 2, I/O 3), ciascuno utilizzabile come ingresso o come uscita open collector (max. 0,15 A) |
| Assorbimento | 60–100 mA; durante l'invio al massimo 250 mA | 60–100 mA; durante l'invio al massimo 500 mA |
| Frequenze del modem | 2G: 850 / 900 / 1800 / 1900 MHz; 3G: 800 / 850 / 900 / 1900 / 2100 MHz; 4G: secondo la regione | 2G: 850 / 900 / 1800 / 1900 MHz; 4G: secondo la regione |
| Dimensioni | 92 × 62 × 26 mm | 92 × 65 × 26 mm |
| Bus RS485 (iO-8, W485, E485) | sì | solo sulla versione 4G (G16T_E120) |

La versione hardware 4 è disponibile con due modem:

| **Tipo** | **Modem** | **Frequenze** | **RS485 (iO-8, W485, E485)** |
|---|---|---|---|
| **G16T_G410** | 2G (GSM/GPRS) | 850 / 900 / 1800 / 1900 MHz | no |
| **G16T_E120** | 4G (LTE), con riserva 2G | secondo la regione | sì |

La versione hardware si trova nella barra di stato di TrikdisConfig (**HW**) e sull'etichetta sul retro del dispositivo.

## 1.3 Caratteristiche principali

### Collegamento con la centrale d'allarme

- Collegamento normale all'uscita della linea telefonica della centrale: DC+, DC−, TIP e RING. Se necessario, si può collegare anche con supervisione della linea (con i fili T-1 e R-1): in questo caso la connessione tra centrale e comunicatore è **supervisionata**, il comunicatore segnala l'interruzione del cavo.
- La centrale invia gli eventi in formato Contact ID, con composizione DTMF; il G16T inoltra l'informazione completa dell'evento (codice, area, zona o utente).

### Comunicazione con la centrale di vigilanza

- Connessione IP con i ricevitori Trikdis (ricevitore software IPcom, RL14, RM14) e con i ricevitori universali (SIA DC-09, TL150).
- Canale primario, di riserva e parallelo; notifica SMS di riserva al ricevitore SMS Trikdis (RL14, RM14, GM14).
- Crittografia dei messaggi AES-128; memoria eventi di 60 messaggi.

### Funzioni per l'utente

- App mobile e web Protegus 2: notifica push con suono dedicato, elenco eventi, inserimento e disinserimento, comando delle uscite.
- Monitoraggio remoto della temperatura (con espansione iO o iO-WL).
- Comando e configurazione di base anche con comandi SMS.
- Notifica via SMS e con chiamata telefonica, fino a 4 numeri di telefono.
- Diritti utente a più livelli nell'app (amministratore, installatore, utente).

### Installazione e configurazione

- Le impostazioni si possono salvare in un file e caricare in un altro comunicatore.
- Due livelli di accesso: amministratore (quello della centrale di vigilanza) e installatore.
- Configurabile e aggiornabile a distanza con il software TrikdisConfig.

## 1.4 Le parti del comunicatore

Il G16T ha il circuito stampato in una scatola di plastica bianca; il coperchio frontale è rimovibile, la morsettiera è estraibile. Nella figura seguente è mostrata la versione 4G; sulla versione 2G non ci sono il LED BAND e i morsetti A 485 / B 485.

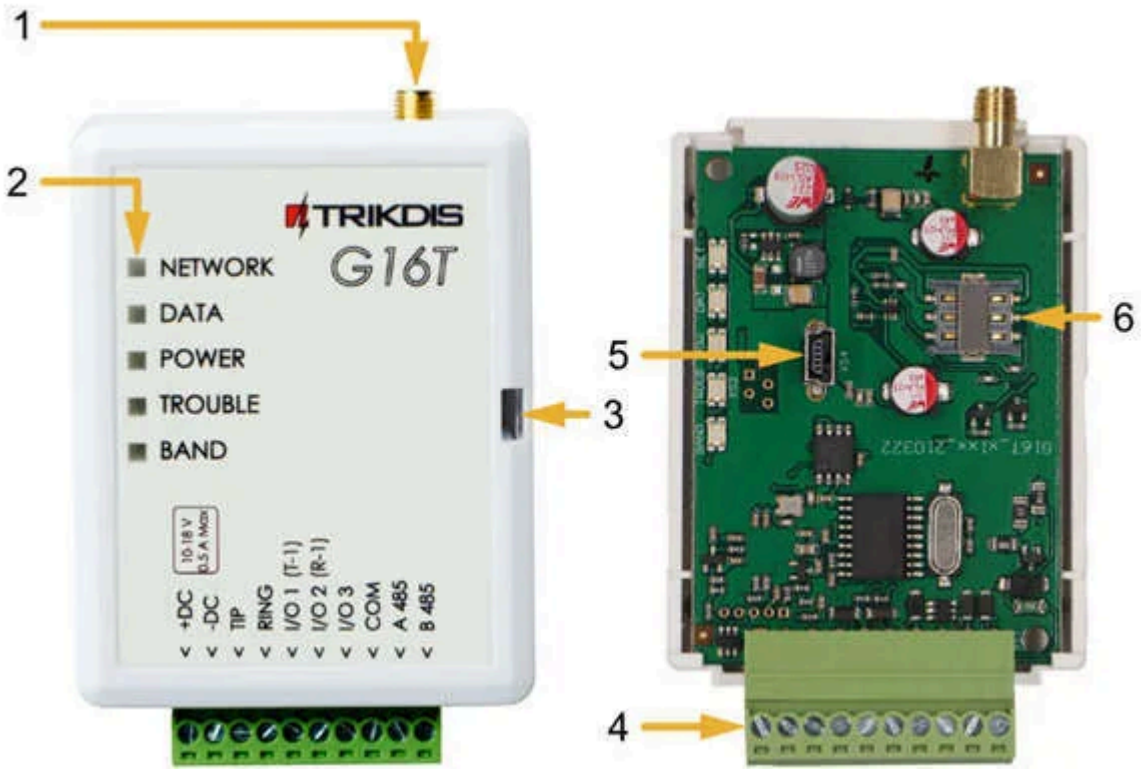



**Figura 2.** Le parti del G16T (versione 4G), di fronte e con la scatola aperta.

- 1 Connettore SMA dell'antenna GSM
- 2 LED di segnalazione (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Fessura per la rimozione del coperchio frontale
- 4 Morsettiera estraibile
- 5 Presa USB Mini-B per la programmazione
- 6 Alloggiamento della scheda Nano-SIM

La morsettiera è estraibile: così il dispositivo si può togliere dall'alimentazione o riavviare con un solo gesto, è più comodo da gestire durante il collegamento e, per la programmazione via USB, si può portare al computer.

## 1.5 Morsetti

| Morsetto | Funzione |
|---|---|
| **+DC** | Alimentazione, +10–18 V DC |
| **–DC** | Alimentazione, negativo |
| **TIP** | Morsetto TIP della centrale d'allarme |
| **RING** | Morsetto RING della centrale d'allarme |
| **I/O 1 (T-1)** | Ingresso/uscita 1, oppure punto T-1 della supervisione della linea telefonica |
| **I/O 2 (R-1)** | Ingresso/uscita 2, oppure punto R-1 della supervisione della linea telefonica |
| **I/O 3** | Ingresso/uscita 3 |
| **COM** | Punto comune (negativo) per ingressi e uscite |
| **A 485** | Filo A del bus RS485 (solo versione 4G) |
| **B 485** | Filo B del bus RS485 (solo versione 4G) |

La dicitura della morsettiera è riportata anche sul coperchio frontale, quindi durante il collegamento non serve togliere il coperchio.

## 1.6 Segnalazioni LED

I LED del frontale sono gli strumenti più importanti per la messa in servizio e per la ricerca guasti. Leggili insieme: POWER indica l'alimentazione, NETWORK la rete, TROUBLE il guasto, BAND (solo 4G) il tipo di rete.

### NETWORK – connessione di rete

| Segnalazione | Significato |
|---|---|
| spento | Nessuna connessione con la rete mobile |
| lampeggia giallo | Connessione alla rete mobile in corso |
| verde fisso | Connesso alla rete mobile |
| verde fisso, lampeggia giallo | Connesso; il numero di lampeggi gialli indica il **livello del segnale**: in 2G 5 lampeggi, in 3G/4G 3 lampeggi indicano un buon segnale |

### DATA – traffico dati

| Segnalazione | Significato |
|---|---|
| spento | Nessun messaggio in attesa di invio |
| verde fisso | Ci sono messaggi in attesa di invio nella memoria |
| lampeggia verde | Invio o ricezione dati in corso (durante la programmazione) |

Controllo rapido

**Il LED DATA è il modo più semplice per verificare la connessione Internet.** Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

### POWER – tensione di alimentazione

| Segnalazione | Significato |
|---|---|
| spento | Nessuna alimentazione, oppure l'alimentazione è scollegata |
| verde fisso | Acceso, la tensione di alimentazione è corretta |
| giallo fisso | Tensione di alimentazione non adeguata (al massimo 11,5 V) |
| verde fisso, lampeggia giallo | Pronto per la programmazione (cavo USB collegato) |
| giallo fisso (durante la programmazione) | Nessuna connessione con il computer |

### TROUBLE – guasto

| Segnalazione | Significato |
|---|---|
| spento | Nessun guasto |
| 1 lampeggio rosso | Nessuna scheda SIM |

| Segnalazione | Significato |
|---|---|
| 2 lampeggi rossi | Errore PIN della SIM (codice PIN errato) |
| 3 lampeggi rossi | Errore di programmazione (manca l'APN) |
| 4 lampeggi rossi | Non riesce a registrarsi sulla rete mobile (errore di registrazione) |
| 5 lampeggi rossi | Non riesce a connettersi alla rete dati (GPRS/UMTS/LTE) |
| 6 lampeggi rossi | Nessuna connessione con il ricevitore della centrale di vigilanza |
| 7 lampeggi rossi | Interrotta la connessione con la centrale d'allarme |
| lampeggia rosso (durante la programmazione) | Errore di memoria |
| rosso fisso (durante la programmazione) | Firmware danneggiato |

### BAND – tipo di rete (solo versione 4G)

| Lampeggi verdi | Rete |
|---|---|
| 1 | nessuna |
| 2 | GSM |
| 3 | GPRS |
| 4 | EDGE |
| 5 | 3G (HSDPA, HSUPA, HSPA+, WCDMA) |
| 6 | 4G (LTE TDD, LTE FDD) |

## 1.7 Dati tecnici

| Parametro | Valore |
|---|---|
| Collegamento con la centrale d'allarme | linea telefonica cablata (TIP/RING), Contact ID, DTMF |
| Ingressi/uscite | 3 I/O a doppia funzione (I/O 1, I/O 2, I/O 3): come ingresso NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistenza di fine linea 2,2 kΩ); come uscita open collector (OC), max. 0,15 A / 30 V DC |
| Espansione | sul bus RS485 (solo versione 4G): espansione iO-8 (+8 I/O) e altre espansioni della serie iO; modulo WiFi W485, modulo Ethernet E485 |
| Modem 2G | 850 / 900 / 1800 / 1900 MHz |
| Modem 4G | bande LTE secondo la regione |
| Tensione di alimentazione | 10–18 V DC |
| Assorbimento | 60–100 mA nominale; al massimo 500 mA durante l'invio |
| Protocolli di trasmissione | TRK, DC-09_2007, DC-09_2012, TL150 |
| Memoria eventi | 60 messaggi |
| Crittografia | AES-128 |
| Programmazione | TrikdisConfig (Windows) con cavo USB Mini-B o a distanza; comandi SMS |
| Ambiente di funzionamento | −10 … +50 °C, max. 80 % di umidità relativa (a +20 °C) |

| Parametro | Valore |
|---|---|
| Dimensioni | 92 × 65 × 26 mm |
| Peso | 80 g |

# 2. Messa in servizio rapida con TrikdisConfig

Tutte le impostazioni del G16T si effettuano con il programma **TrikdisConfig**, che funziona su Windows – tramite cavo USB o a distanza. In questo capitolo descriviamo la via più breve: configuri il dispositivo sul tavolo, prima del collegamento, e poi sul posto devi soltanto collegarlo. La spiegazione dettagliata delle impostazioni si trova nel capitolo 6.

## 2.1 Preparativi

Che cosa ti serve

Cavo USB Mini-B · cavo con almeno 4 conduttori verso la centrale · cacciavite piatto da 2,5 mm · antenna mobile con guadagno adeguato (se sul posto la copertura è debole) · scheda nano-SIM attiva con servizio dati mobile · manuale per l'installatore della centrale d'allarme.

Ordina separatamente gli accessori necessari presso il distributore.

**1. Scarica e installa il software TrikdisConfig.** Sul sito di Trikdis (www.trikdis.com) scrivi „TrikdisConfig" nel campo di ricerca.

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

**2. Apri il coperchio frontale del G16T.** Inserisci un cacciavite piatto nella fessura laterale e sgancia delicatamente il coperchio. La figura seguente mostra la posizione dell'aggancio e i fori per le viti sul fondo.

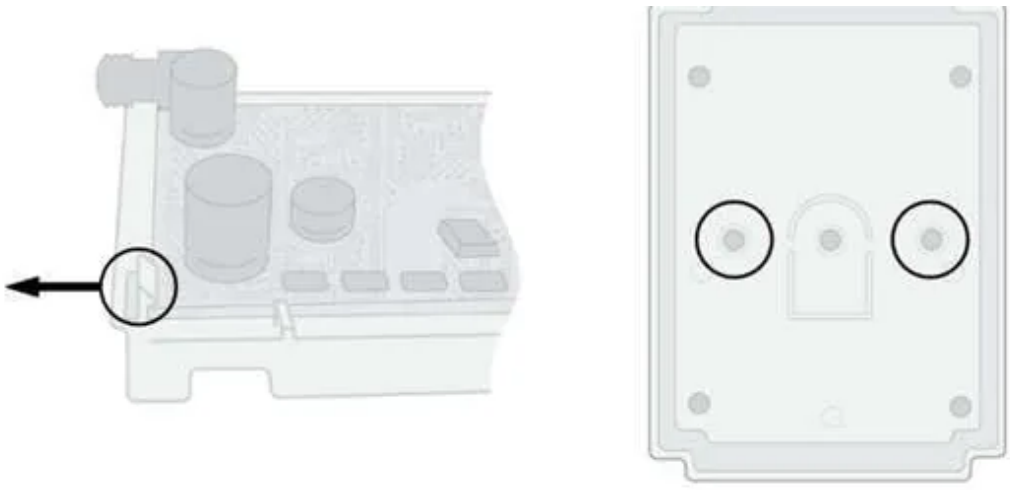


**Figura 3.** Sgancio del coperchio frontale (a sinistra) e fori di fissaggio del fondo (a destra).

**3. Inserisci la scheda nano-SIM** nell'alloggiamento, nel verso mostrato nella figura. La scheda deve essere attiva, avere il servizio dati mobile e, se possibile, disattiva la richiesta del PIN usando un telefono (così non serve inserire il PIN nel dispositivo).

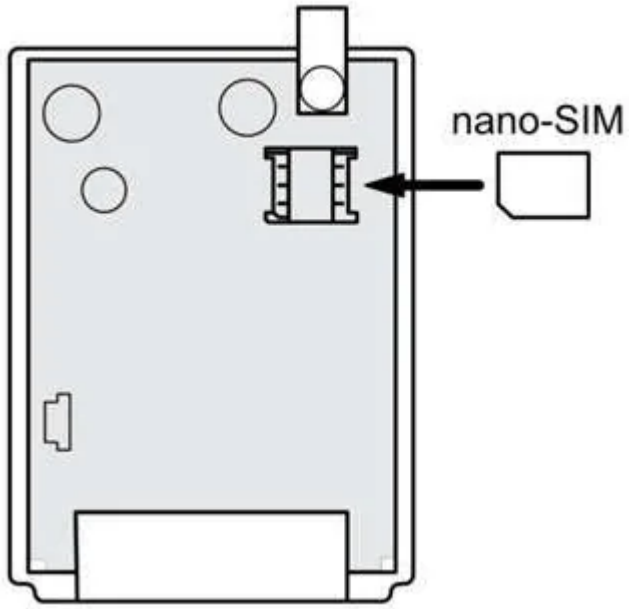



**Figura 4.** La posizione della scheda nano-SIM sul circuito stampato.

**4. Collega il G16T al computer** con un cavo USB Mini-B. L'USB fornisce alimentazione sufficiente per la programmazione, non serve un alimentatore separato.




**Figura 5.** Collegamento al computer con cavo USB Mini-B.

Avvertenza

Finché il dispositivo è collegato al computer con il cavo USB, è in modalità di programmazione: il funzionamento normale si interrompe, non sorveglia, non trasmette, non può essere comandato, è alimentato dalla porta USB e si riavvia quando il cavo viene scollegato. Per questo il dispositivo non deve essere liberamente accessibile: deve trovarsi in un contenitore metallico chiuso, con protezione antimanomissione (tamper) o con un rilevatore di movimento che sorveglia il contenitore. Dettagli nelle FAQ

**5. Avvia TrikdisConfig.** Il programma riconosce il dispositivo e apre la finestra di programmazione. Fai clic sul pulsante **Read [F4]** (lettura): il programma legge le impostazioni attuali del dispositivo. Se chiede una password, inserisci il codice di 6 cifre dell'amministratore (di fabbrica `123456`) o dell'installatore (di fabbrica `654321`).

## 2.2 Collegamento all'app Protegus 2

Se l'utente vuole vedere e comandare il sistema dall'app Protegus 2, nella pagina **User reporting**, sulla scheda **PROTEGUS Cloud**, imposta quanto segue.

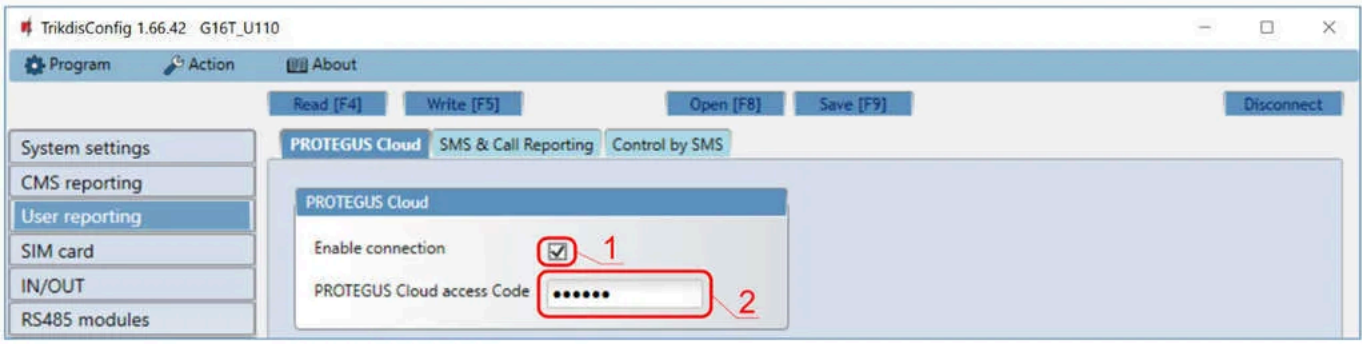



**Figura 6.** TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- 1 **Enable connection** – spunta la casella: abilita la connessione con il cloud Protegus.
- 2 **Protegus Cloud access code** – cambia la password di fabbrica `123456`. Questa andrà inserita nell'app al momento della creazione del sistema; **dopo la creazione del sistema non si può più modificare.**

Poi, nella pagina **SIM card**, inserisci i dati della scheda.




**Figura 7.** TrikdisConfig – pagina SIM card.

- 3 **SIM card PIN** – il codice PIN della scheda (se la richiesta del PIN è disattivata, può restare il valore di fabbrica).
- 4 **APN** – il punto di accesso dati dell'operatore (vedi sotto).

L'APN (Access Point Name) è il punto di accesso dati dell'operatore mobile; senza di esso il dispositivo non riesce a connettersi a Internet. Il valore esatto te lo fornisce l'operatore della scheda SIM. Gli APN noti degli operatori europei sono raccolti in un articolo separato: Impostazione APN – elenco degli operatori mobili europei. Se dall'operatore non hai altre informazioni, prova l'APN `internet`: è generico e funziona nella rete di molti operatori.

Per una scheda dati IoT / M2M (comunicazione tra macchine) l'operatore di solito **fornisce un APN diverso da quello delle schede per privati** – con l'APN per privati il dispositivo non si connette. Anche questo valore si trova nell'articolo sugli APN, oppure chiedilo all'operatore; se l'operatore fornisce anche nome utente e password, inserisci anche quelli.

Se il dispositivo non trasmette a una centrale di vigilanza, la configurazione è finita: premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB.

Non dimenticare di attivare e impostare il combinatore telefonico della centrale d'allarme, altrimenti la centrale non invia eventi. L'impostazione della centrale è descritta nel capitolo 4.

## 2.3 Collegamento alla centrale di vigilanza

Se il dispositivo trasmette anche a un ricevitore della centrale di vigilanza, nella pagina **System settings** inserisci prima il codice impianto.

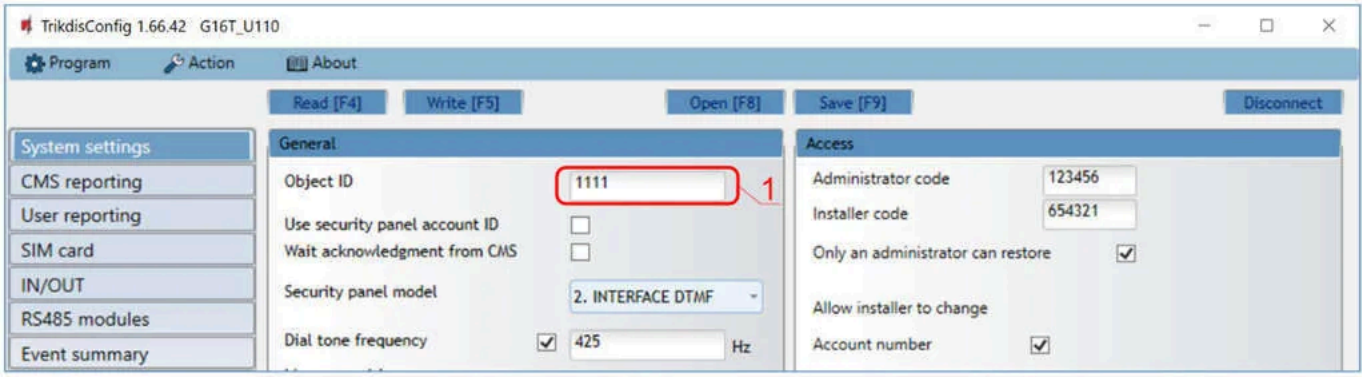



**Figura 8.** TrikdisConfig – pagina System settings, gruppo General.

- 1 **Object ID** – il codice impianto ricevuto dalla centrale di vigilanza (4 caratteri esadecimali, 0–9, A–F). `FFFE` e `FFFF` non si possono usare.

Poi, nella pagina **CMS reporting**, nella parte **Primary channel** (canale primario), imposta i dati del ricevitore.

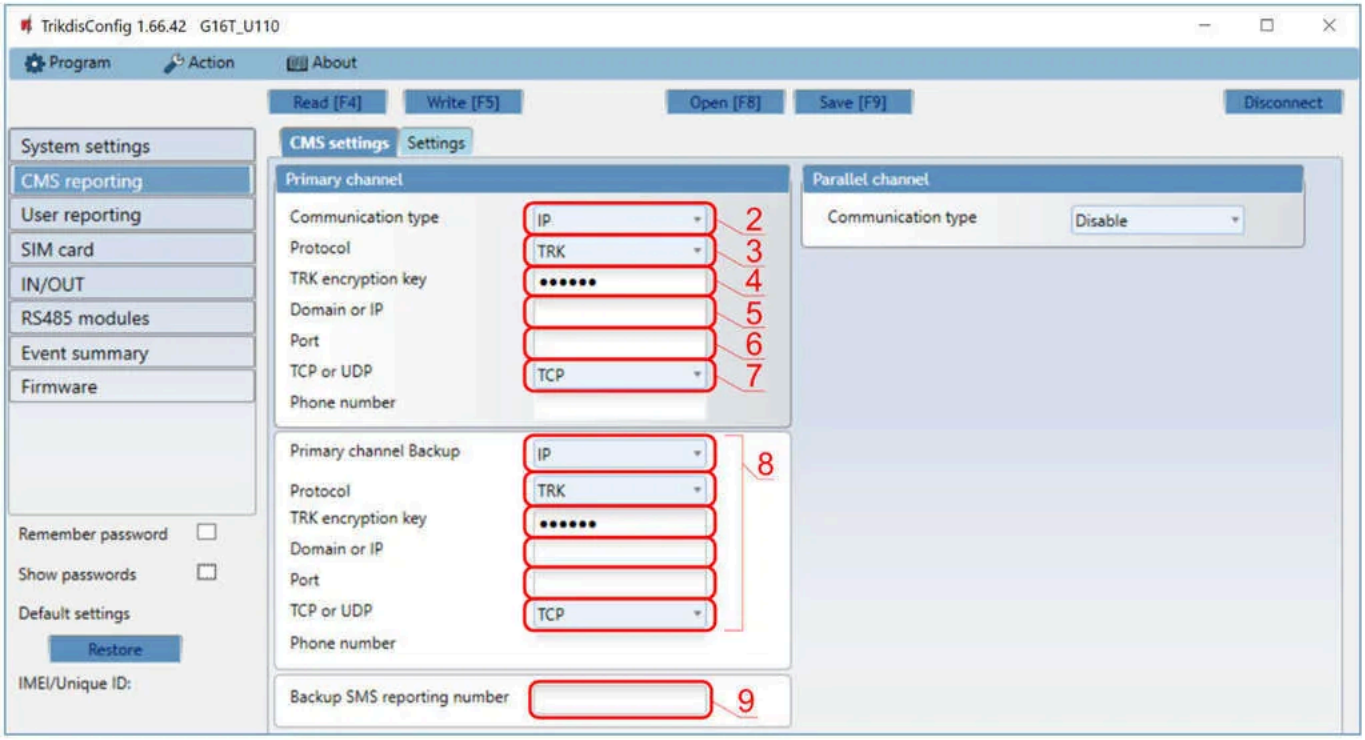



**Figura 9.** TrikdisConfig – CMS reporting, scheda CMS settings.

- 2 **Communication type** – scegli la connessione **IP** (l'SMS non è consigliato come canale primario).
- 3 **Protocol** – **TRK** per un ricevitore Trikdis, **DC-09_2007** o **DC-09_2012** per un ricevitore universale, **TL150** per un ricevitore SUR-GARD.
- 4 **TRK encryption key** – la chiave di crittografia di 6 cifre impostata nel ricevitore.
- 5 **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- 6 **Port** – il numero di porta del ricevitore.
- 7 **TCP or UDP** – il protocollo di trasmissione; si adegua all'impostazione del ricevitore.
- 8 **Primary channel Backup** – canale di riserva in caso di guasto del primario; compilalo allo stesso modo, è consigliato impostarlo.
- 9 **Backup SMS reporting number** – se c'è un ricevitore SMS Trikdis, inserisci qui il suo numero di telefono: il dispositivo, subito dopo il primo avvio, invia un SMS a questo numero, e in seguito trasmette via SMS quando nessuno dei canali IP funziona.

Infine, nella pagina **SIM card**, inserisci i dati della scheda, se non l'hai già fatto al punto 2.2.

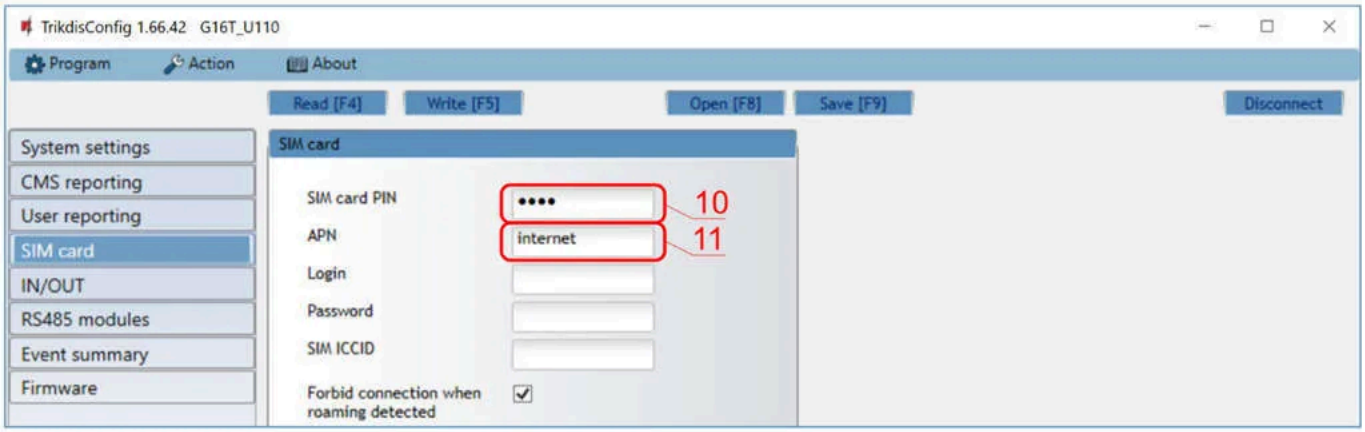



**Figura 10.** TrikdisConfig – pagina SIM card.

- 10 **SIM card PIN** – il codice PIN della scheda.
- 11 **APN** – il punto di accesso dell'operatore (vedi il punto 2.2).

La **trasmissione SMS** alla centrale di vigilanza funziona solo con un ricevitore Trikdis (ricevitore IP/SMS RL14, ricevitore multicanale RM14 o ricevitore SMS GM14); in questo caso servono solo la chiave di crittografia e il numero di telefono. Con il protocollo **DC-09**, sulla scheda **Settings** inserisci anche il numero impianto, il numero di linea e il numero di ricevitore DC-09.

Alla fine delle impostazioni premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB. Il dispositivo è così pronto per il collegamento. Anche in questo caso il combinatore telefonico della centrale d'allarme deve essere attivato e impostato, altrimenti la centrale non invia eventi (capitolo 4).

# 3. Installazione e collegamento

**Figyelem!**

Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

## 3.1 Fasi dell'installazione

1. Togli il coperchio frontale (vedi il punto 2.1) ed estrai la morsettiera.
2. Inserisci la scheda nano-SIM, se non l'hai già fatto durante la messa in servizio.
3. Estrai il circuito stampato dal fondo: apri l'aggancio nell'angolo (vedi la figura del punto 2.1).
4. Fissa il fondo con le viti nel punto scelto.
5. Rimetti il circuito stampato nel fondo e reinserisci la morsettiera.
6. Avvita l'antenna GSM.
7. Rimetti il coperchio frontale.

La scheda SIM deve essere attiva e, per l'uso via IP, deve avere la connessione dati mobile funzionante. Se non vuoi che TrikdisConfig chieda il codice PIN, disattiva la richiesta del PIN sulla scheda usando un telefono.

## 3.2 Posizionamento e antenna

- Metti il comunicatore in un luogo **asciutto, al chiuso**, possibilmente vicino alla scatola della centrale d'allarme, in modo che i cavi siano corti.
- In una **scatola metallica** il segnale mobile si indebolisce molto. Se il comunicatore va nel contenitore metallico della centrale, porta l'antenna fuori dalla scatola, oppure usa un'antenna con cavo più lungo.
- Prima del fissaggio definitivo **controlla il livello del segnale**: il numero di lampeggi gialli del LED NETWORK deve essere almeno 5 in 2G e almeno 3 in 4G (vedi il punto 1.6). Se è inferiore, cerca un punto migliore, oppure passa a un'antenna più sensibile che si possa posizionare più lontano.
- Tieni l'antenna e il comunicatore lontani dal trasformatore della centrale e dai cavi della rete elettrica.



A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna használata.

## 3.3 Collegamento alla centrale d'allarme

Il G16T va collegato all'uscita della linea telefonica (TIP/RING) della centrale, e l'alimentazione la riceve dall'uscita di alimentazione ausiliaria a 12 V (AUX) della centrale.

**Collegamento consigliato, normale: DC+, DC−, TIP e RING.** In questo caso il comunicatore non rileva l'interruzione del cavo.

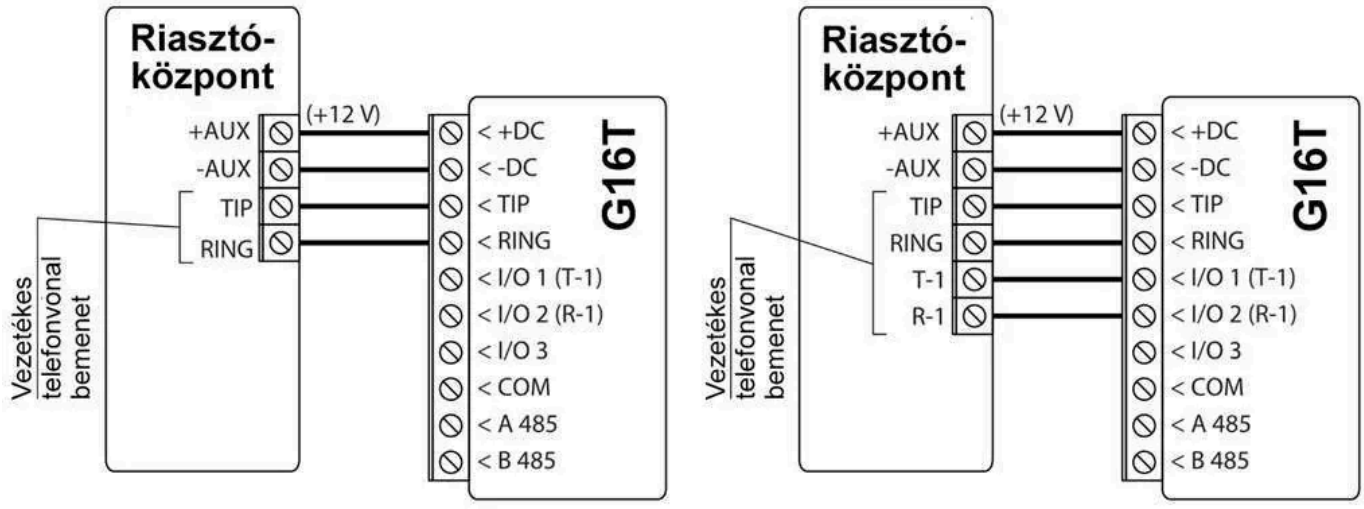



**Figura 11.** Collegamento all'uscita della linea telefonica della centrale: a sinistra il collegamento normale, a destra il collegamento con supervisione della linea.

Durante l'invio il G16T può assorbire fino a 500 mA. Verifica che l'uscita AUX della centrale lo sopporti insieme agli altri dispositivi collegati. Poiché l'alimentazione è fornita dalla centrale, in caso di mancanza di rete la batteria della centrale alimenta anche il comunicatore.

### 3.3.1 Se necessario: supervisione della linea

Serve solo se è richiesta la supervisione della linea: il comunicatore segnala allora l'interruzione del collegamento tra sé e la centrale d'allarme.

1. Oltre al collegamento normale, collega anche questi due fili: il morsetto **T-1** della centrale al morsetto **I/O 1 (T-1)** del comunicatore, il morsetto **R-1** della centrale al morsetto **I/O 2 (R-1)**.
2. Nella pagina **System settings** di TrikdisConfig attiva l'opzione **Line supervision**.
3. Verifica le impostazioni necessarie sul lato della centrale d'allarme nel manuale di installazione della centrale.

In questo caso I/O 1 e I/O 2 non possono essere usati per altri scopi.

## 3.4 Collegamento della zona a chiave

Se vuoi inserire e disinserire la centrale a distanza, dall'app Protegus 2, imposta uno dei morsetti I/O del comunicatore come **uscita** e collegalo a una **zona a chiave** della centrale. All'attivazione l'uscita porta la zona su COM (negativo); collega la resistenza di fine linea della zona secondo il tipo di zona della centrale. Poiché il G16T ha tre morsetti I/O, si possono gestire fino a tre aree con uscite separate. Imposta il morsetto usato per la chiave sulla funzione **OUT** nella pagina **IN/OUT** di TrikdisConfig (punto 6.6). Sull'hardware 3 c'è una sola uscita programmabile (OUT), che può comandare un'area; lì il campo **Output OUT1 mode** della pagina **System settings** deve essere **Remote control** (è l'impostazione di fabbrica).

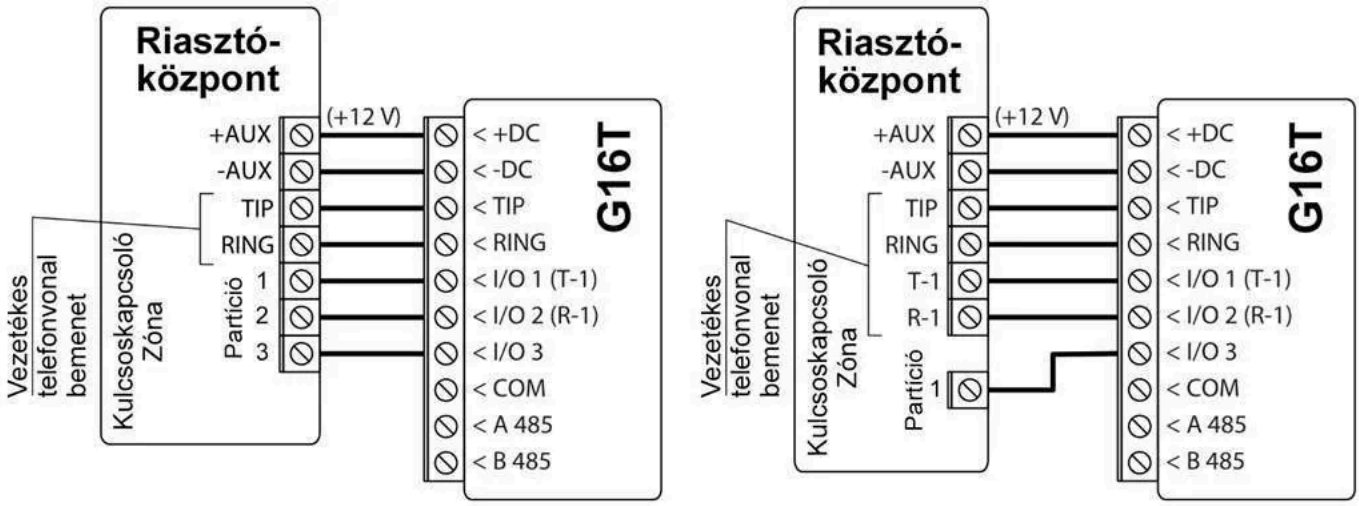



**Figura 12.** Inserimento e disinserimento con zona chiave: a sinistra il collegamento normale, a destra il collegamento con supervisione della linea (in questo caso per la zona chiave resta I/O 3).

La zona a chiave può essere a impulso o bistabile – nell'app Protegus 2 bisogna impostare la stessa modalità (punto 5.2). I dettagli e le insidie dell'inserimento tramite zona a chiave sono trattati in un articolo separato: Inserimento a distanza con zona a chiave dall'app Protegus 2.

## 3.5 Collegamento degli ingressi

I morsetti I/O del comunicatore, come ingressi, si possono usare anche per collegare altri rilevatori (ad es. interruttore tamper, pulsante di panico, termostato), indipendentemente dalla centrale d'allarme. L'ingresso va collegato tra l'I/O scelto e il morsetto COM.

Gli ingressi accettano i seguenti tipi di circuito: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La resistenza di fine linea è **2,2 kΩ**. Con la terminazione singola (EOL) sia il cortocircuito sia l'interruzione contano come allarme; la doppia terminazione (DEOL), con due resistenze, riconosce separatamente l'allarme

e il sabotaggio (cortocircuito o interruzione). L'impostazione di fabbrica è NO (normalmente aperto); il tipo di ingresso si imposta nella pagina **IN/OUT** di TrikdisConfig, in base al collegamento.

| Tipo | Stato di riposo | Allarme | Sabotaggio |
|---|---|---|---|
| NC | chiuso | aperto | – |
| NO | aperto | chiuso | – |
| NC/EOL | 2,2 kΩ | interruzione o cortocircuito | – |
| NO/EOL | 2,2 kΩ | cortocircuito o interruzione | – |
| NC/DEOL | 2,2 kΩ | 3,3–5,5 kΩ (2 × 2,2 kΩ) | interruzione o cortocircuito |
| NO/DEOL | 3,3–5,5 kΩ (2 × 2,2 kΩ) | 2,2 kΩ | interruzione o cortocircuito |

Quando l'ingresso viene violato, il comunicatore invia un proprio evento alla centrale di vigilanza e a Protegus 2; il codice Contact ID dell'evento, il numero di area e di zona si impostano nella pagina **IN/OUT**.

Collegamento dei circuiti di ingresso: tipi NC, NO, EOL e DEOL con resistenza di fine linea da 2,2 kΩ, per i tipi DEOL con circuito tamper.

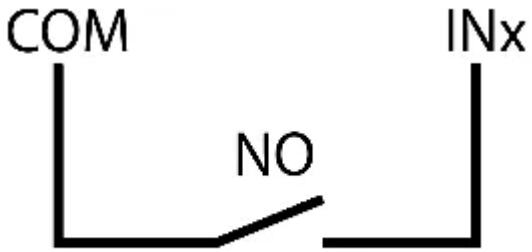



**Figura 13. NO** – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

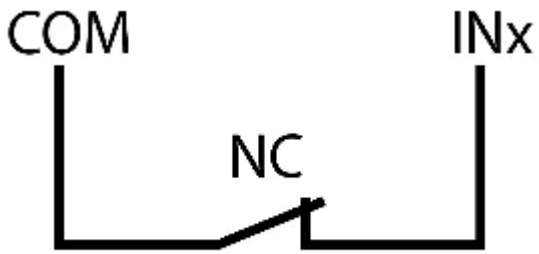



**Figura 14. NC** – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

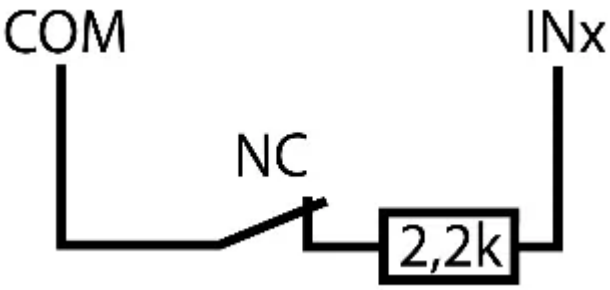



**Figura 15. NC/EOL** – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

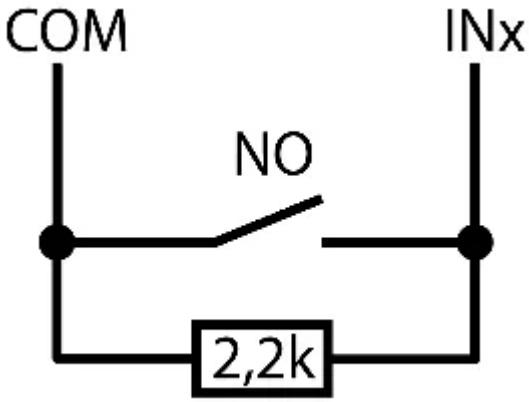



**Figura 16. NO/EOL** – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

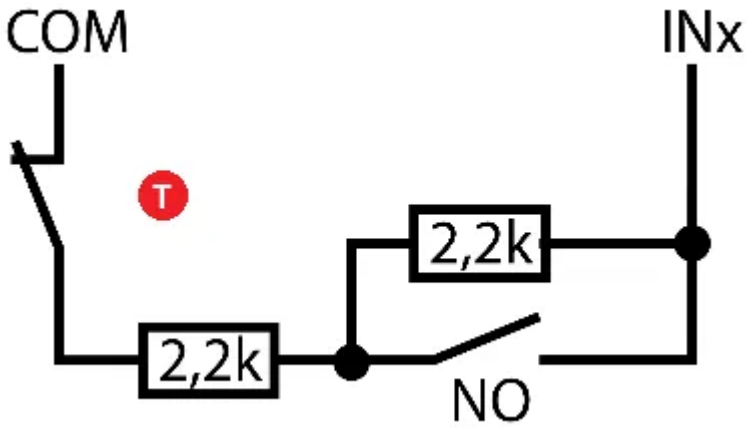



**Figura 17. NO/DEOL** – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento tamper: cortocircuito o interruzione – tamper, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

- T contatto tamper („Tamper"), segnala l'apertura dell'involucro del rilevatore

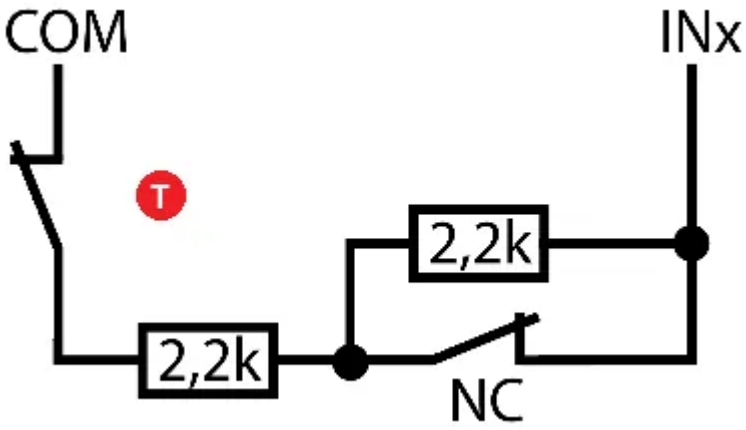



**Figura 18. NC/DEOL** – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento tamper: cortocircuito o interruzione – tamper, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

- T contatto tamper („Tamper"), segnala l'apertura dell'involucro del rilevatore

## 3.6 Collegamento di un'uscita con relè

I morsetti I/O, come uscite, sono uscite open collector (OC): nello stato attivo portano a negativo il carico collegato, con al massimo 0,15 A, fino a 30 V DC. Un carico maggiore o un dispositivo a tensione di rete va comandato **tramite un relè**: un capo della bobina del relè va al +DC, l'altro al morsetto I/O.

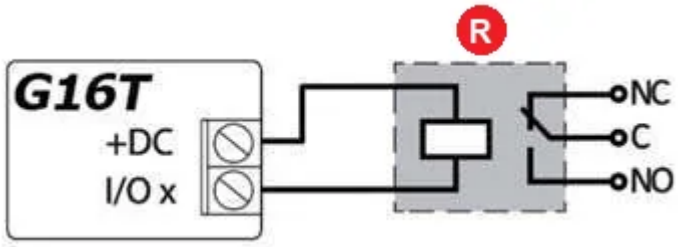



**Figura 19.** Collegamento di un relè all'uscita del comunicatore: la bobina va tra il +DC e il morsetto I/O x, i contatti (NC, C, NO) comandano il carico.

- R relè („Relay")

Le uscite si possono comandare dall'app Protegus 2 o con un comando SMS (capitolo 5).

## 3.7 Collegamento dell'espansione iO-8

Se servono più ingressi o uscite, sul bus RS485 della **versione 4G** si possono collegare al massimo quattro espansioni **iO-8**; ciascuna aggiunge 8 I/O a doppia funzione. Sullo stesso bus si possono collegare anche le altre espansioni cablate o senza fili della serie iO di Trikdis, ad esempio se vuoi collegare un sensore di temperatura: l'espansione **iO** ha 1 ingresso, 1 uscita relè e un bus 1-Wire per sensori di temperatura (configurazione al punto 6.7). Collega i morsetti A 485 e B 485 ai morsetti A e B del modulo, e prendi l'alimentazione del modulo dai 12 V della centrale. Il modulo va aggiunto nella pagina **RS485 modules** di TrikdisConfig (punto 6.7).

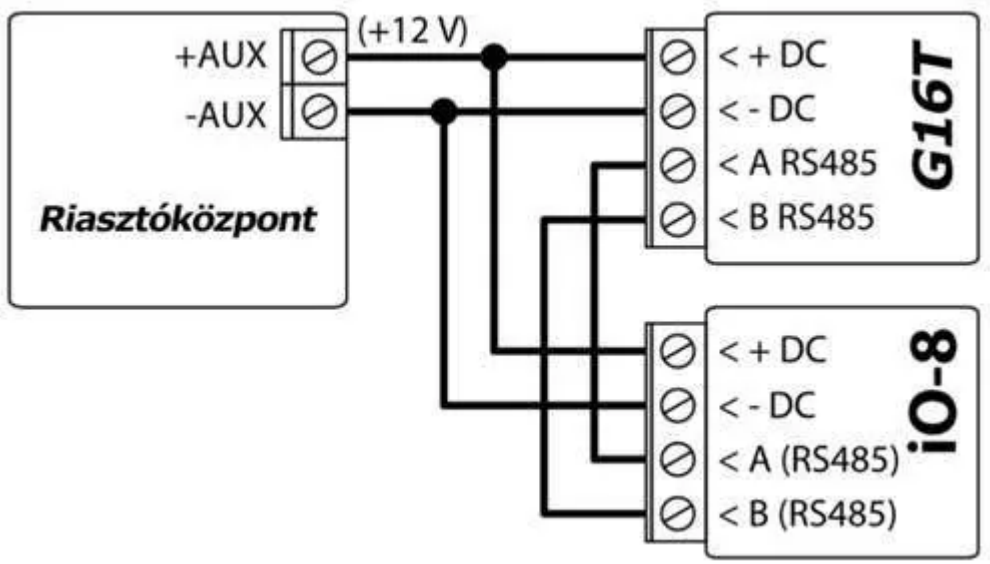



**Figura 20.** Collegamento dell'espansione iO-8 al bus RS485 del G16T; alimentazione dall'uscita AUX della centrale d'allarme.

Il G16T con modem 2G (G16T_G410) non ha il bus RS485, quindi non vi si possono collegare i moduli iO-8, W485 ed E485.

## 3.8 Collegamento dei moduli W485 ed E485

**Espansione Ethernet o Wi-Fi – W485 ed E485.** Il comunicatore può essere completato con il modulo Wi-Fi W485 o con il modulo Ethernet E485: gli eventi arrivano alla centrale di vigilanza e all'app Protegus 2 tramite Internet cablato o Wi-Fi.

- **Collegamento:** sul bus RS485, con alimentazione comune al comunicatore (ingresso di alimentazione del modulo 9–28 V DC); non serve un alimentatore separato.
- **Internet è il canale primario:** finché funziona, tutto passa da lì. Se si interrompe, il comunicatore passa da solo alla rete mobile e, non appena Internet ritorna, torna su IP.
- **Non solo trasmissione allarmi:** anche l'app Protegus 2 (notifiche, controllo da remoto) funziona su questo canale.
- **E485** – Ethernet cablato (RJ45). **W485** – Wi-Fi 2,4 GHz (WPA / WPA2), dove non è stato posato un cavo UTP.
- Se necessario, utilizzabile anche senza scheda SIM. Configurazione: con il software TrikdisConfig, via USB.

**Trikdis E485 modulo Ethernet (RS485)** **Trikdis W485 modulo WiFi (RS485)**

Finché la connessione WiFi o Ethernet è attiva, il G16T comunica attraverso di essa (i messaggi per la centrale di vigilanza e per Protegus passano dal router WiFi o da Internet cablato, la connessione dati mobile in questo caso non viene usata); se si interrompe, passa alla connessione dati mobile e, quando la connessione si ripristina, torna al modulo. Per il funzionamento del modulo **nel G16T deve esserci una scheda SIM**.

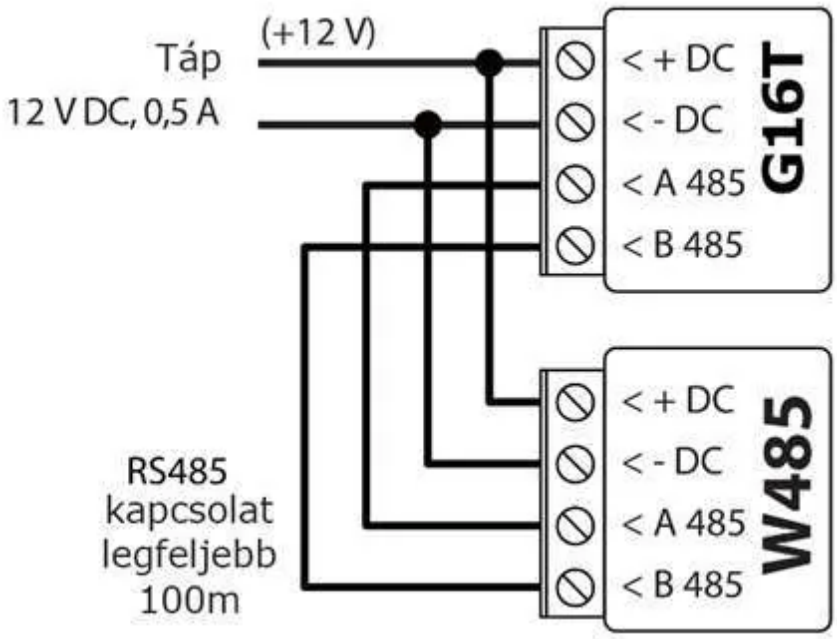



**Figura 21.** Collegamento del modulo WiFi W485 al G16T tramite bus RS485. I due dispositivi funzionano con un'alimentazione comune a 12 V DC (almeno 0,5 A) (l'ingresso di alimentazione del modulo è 9–28 V DC); il cavo RS485 può essere lungo al massimo 100 m.

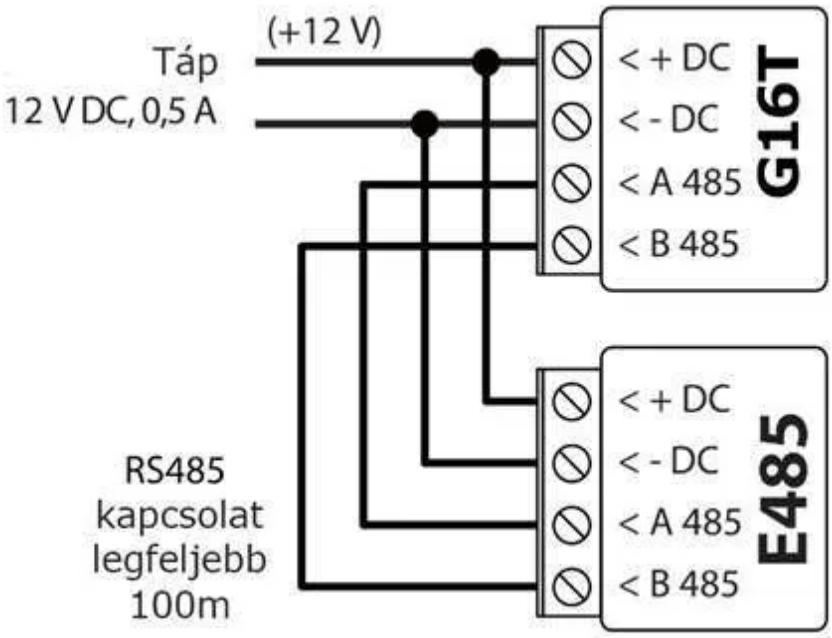



**Figura 22.** Collegamento del modulo Ethernet E485 al G16T tramite bus RS485. I due dispositivi funzionano con un'alimentazione comune a 12 V DC (almeno 0,5 A) (l'ingresso di alimentazione del modulo è 9–28 V DC); il cavo RS485 può essere lungo al massimo 100 m.

**Le distanze «fino a … m»** sono valori massimi teorici, raggiungibili in condizioni ideali. In pratica la qualità e il percorso del cavo, le fonti di disturbo e, nei collegamenti radio, i muri e il terreno danno una portata nettamente inferiore. Prevedi un margine e, sulle lunghe distanze, verifica il collegamento alla messa in servizio.

Le impostazioni di rete dei moduli si effettuano nella pagina **RS485 modules** di TrikdisConfig (punto 6.7).

### 3.9 Accensione e primo controllo

### A TRIKDIS átjelző elindítása

1. SIM kártyás átjelző esetén a SIM kártyát az elindítás előtt helyezd be a készülékbe.
2. Ethernetes eszköz esetén az Ethernet kábelt elindítás előtt vagy utána is csatlakoztathatod
3. Az indításhoz húzd ki az USB kábelt és csatlakoztasd a lehúzott sorkapcsot

Akkor léphetsz tovább a következő fejezetre, ha az eszköz megfelelően elindul és nem jelez hibát.

- A Power LED zölden világít
- A Trouble LED nem villog pirosan
- A Network LED zölden világít (ha közben sárgán villog az rendben van)
- Ha Data LED nem alszik ki, az azt jelenti, hogy az eszköz nem tud elküldeni valamilyen eseményt. Ez internet / adat kapcsolat hibára utal.

Dopo il collegamento, accendendo la centrale d'allarme si avvia anche il comunicatore. Sul frontale devi vedere:

- **POWER** verde fisso – l'alimentazione è corretta;
- **NETWORK** verde fisso e lampeggia giallo – connesso alla rete; il numero di lampeggi indica il livello del segnale (5 in 2G, 3 in 4G è buono); se ne conti di meno, il segnale è debole: cerca un altro punto per il comunicatore, oppure usa un'antenna più sensibile (punto 3.2);
- **TROUBLE** spento.

Se TROUBLE lampeggia, il numero di lampeggi indica la causa (punto 1.6); anche ogni altra segnalazione LED diversa da questa indica un guasto, cercane la causa con le tabelle del punto 1.6. Se nessun LED è acceso, controlla l'alimentazione e i collegamenti.

## 4. Programmazione della centrale d'allarme

Perché la centrale d'allarme invii gli eventi sulla sua uscita per linea telefonica, il combinatore della centrale va attivato e configurato. Le locazioni di programma esatte si trovano nel manuale di installazione della centrale; la sostanza della configurazione è la stessa per tutti i produttori:

1. **Attiva il comunicatore su linea telefonica (PSTN)** nella centrale.
2. **Come numero di telefono inserisci** `1234` per il ricevitore della centrale di vigilanza – sia che il comunicatore sia collegato ai morsetti RING/TIP della centrale, sia alla linea telefonica. Con un altro numero può succedere che la centrale componga il numero ma il comunicatore non riceva comunque gli eventi: anche con una centrale DSC PowerSeries NEO la trasmissione è partita solo dopo aver cambiato il numero in `1234`.
3. **Modalità di composizione:** DTMF (tone), non a impulsi.
4. **Protocollo:** Contact ID.

Se vuoi inserire e disinserire la centrale da remoto con l'uscita del comunicatore, la zona collegata all'uscita va impostata nella centrale come **zona a chiave**.

La zona a chiave può essere a impulso o bistabile. L'uscita del comunicatore fornisce per impostazione predefinita un impulso di 3 secondi; la durata dell'impulso o la modalità bistabile si possono modificare nelle impostazioni dell'app Protegus 2.

## 4.1 Programmazione del combinatore Honeywell Vista

Dalla tastiera entra in modalità di programmazione e imposta queste locazioni di programma:

| Locazione | Impostazione |
|---|---|
| `*41` | il numero di telefono del ricevitore della centrale di vigilanza: `1234` |
| `*43` | il codice impianto (account) della centrale |
| `*47` | Tone dial = `1`, e il numero di tentativi di chiamata |
| `*48` | `7` (predefinito) |
| `*49` | `5` (messaggio Split/Dual) |
| `*50` | il ritardo di invio dell'allarme intrusione – predefinito `2,0` (30 s); per l'invio immediato `0,0` |

Con la centrale **Honeywell Vista 48** imposta inoltre le seguenti locazioni di programma:

| Locazione | Valore | Locazione | Valore | Locazione | Valore |
|---|---|---|---|---|---|
| `*41` | 1234 (numero di telefono del ricevitore) | `*60` | 1 | `*69` | 1 |
| `*42` | 1234 | `*61` | 1 | `*70` | 1 |
| `*43` | 1234 (codice impianto) | `*62` | 1 | `*71` | 1 |
| `*44` | 1234 | `*63` | 1 | `*72` | 1 |
| `*45` | 1111 | `*64` | 1 | `*73` | 1 |
| `*47` | 1 | `*65` | 1 | `*74` | 1 |
| `*48` | 7 | `*66` | 1 | `*75` | 1 |
| `*50` | 1 | `*67` | 1 | `*76` | 1 |
| `*59` | 0 | `*68` | 1 | | |

Al termine della programmazione esci dalla modalità di programmazione con il comando `*99`.

## 4.2 Centrali di altri produttori

Nel manuale per l'installatore di ogni centrale cerca le stesse quattro impostazioni: abilitazione del comunicatore su linea telefonica, numero di telefono del ricevitore, modalità di composizione (DTMF) e formato di comunicazione (Contact ID). Se la centrale attende il tono di linea (dial tone) prima di comporre il numero, lo fornisce il G16T; se la chiamata comunque non parte, nella centrale disattiva il controllo del tono di linea („composizione senza tono di linea” o un'opzione simile).

Se a fine chiamata la centrale segnala un errore, anche se l'evento è arrivato, controlla l'impostazione **Wait acknowledgment from CMS** nella pagina **System settings** di TrikdisConfig: se è attiva, il comunicatore chiude la chiamata solo dopo la conferma del ricevitore della centrale di vigilanza (kiss-off). In un sistema senza centrale di vigilanza, solo con Protegus 2, lasciala disattivata (è lo stato di fabbrica), perché non c'è un ricevitore che dia la conferma.

# 5. Comando a distanza con l'app Protegus 2

Con l'app mobile e web Protegus 2 l'utente vede a distanza lo stato del sistema, riceve notifiche degli eventi, può inserire e disinserire il sistema e comandare le uscite del comunicatore.

## 5.1 Aggiunta del dispositivo

Prima di aggiungere il dispositivo verifica che:

1. La scheda SIM sia attiva e la connessione dati mobile funzioni; il suo codice PIN sia inserito nel dispositivo, oppure la richiesta del PIN sia disattivata.
2. Nella scheda **User reporting** → **PROTEGUS Cloud** di TrikdisConfig sia spuntato **Enable connection** e sia impostato il **Protegus Cloud access code** (dopo la creazione del sistema non si può più modificare).
3. Il LED **POWER** sia verde fisso, il LED **NETWORK** sia verde fisso e lampeggi giallo.

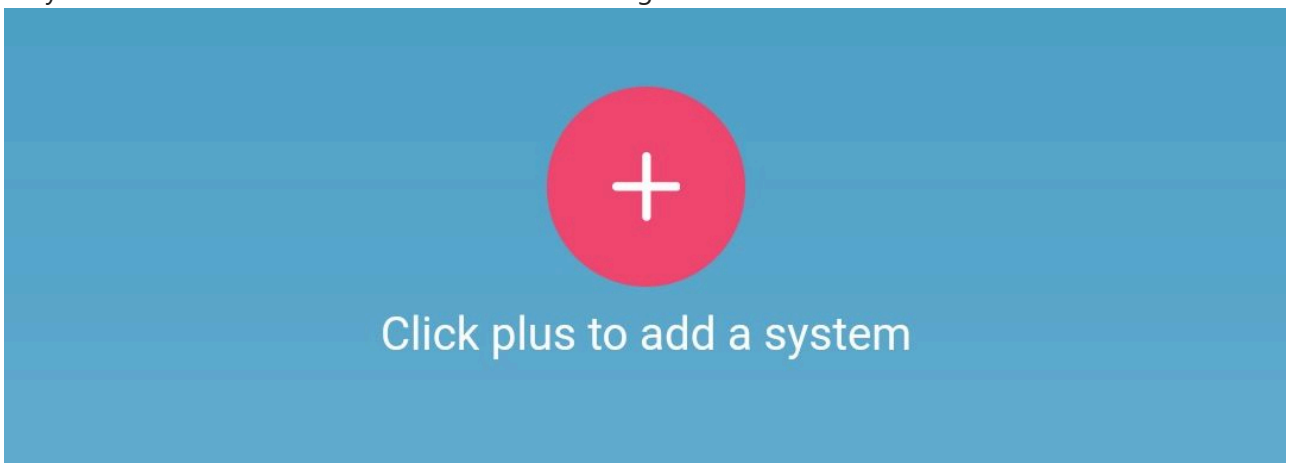
**Il LED DATA è il modo più semplice per verificare la connessione Internet.** Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

## A rendszer létrehozása a Protegus 2 alkalmazásban

1. Töltsd le a Protegus 2 alkalmazást a telefonodra vagy nyisd meg egy böngészőben



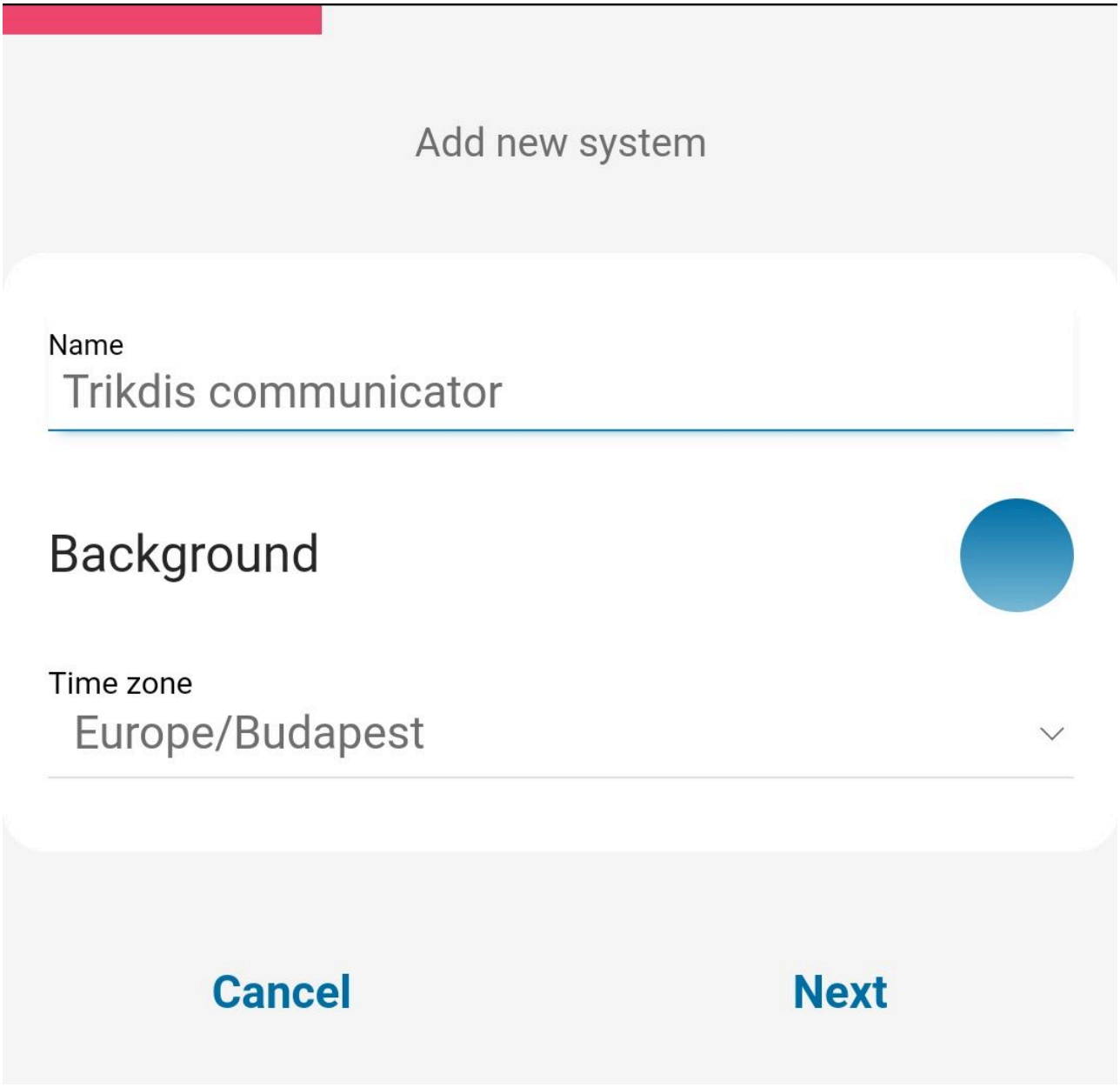
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



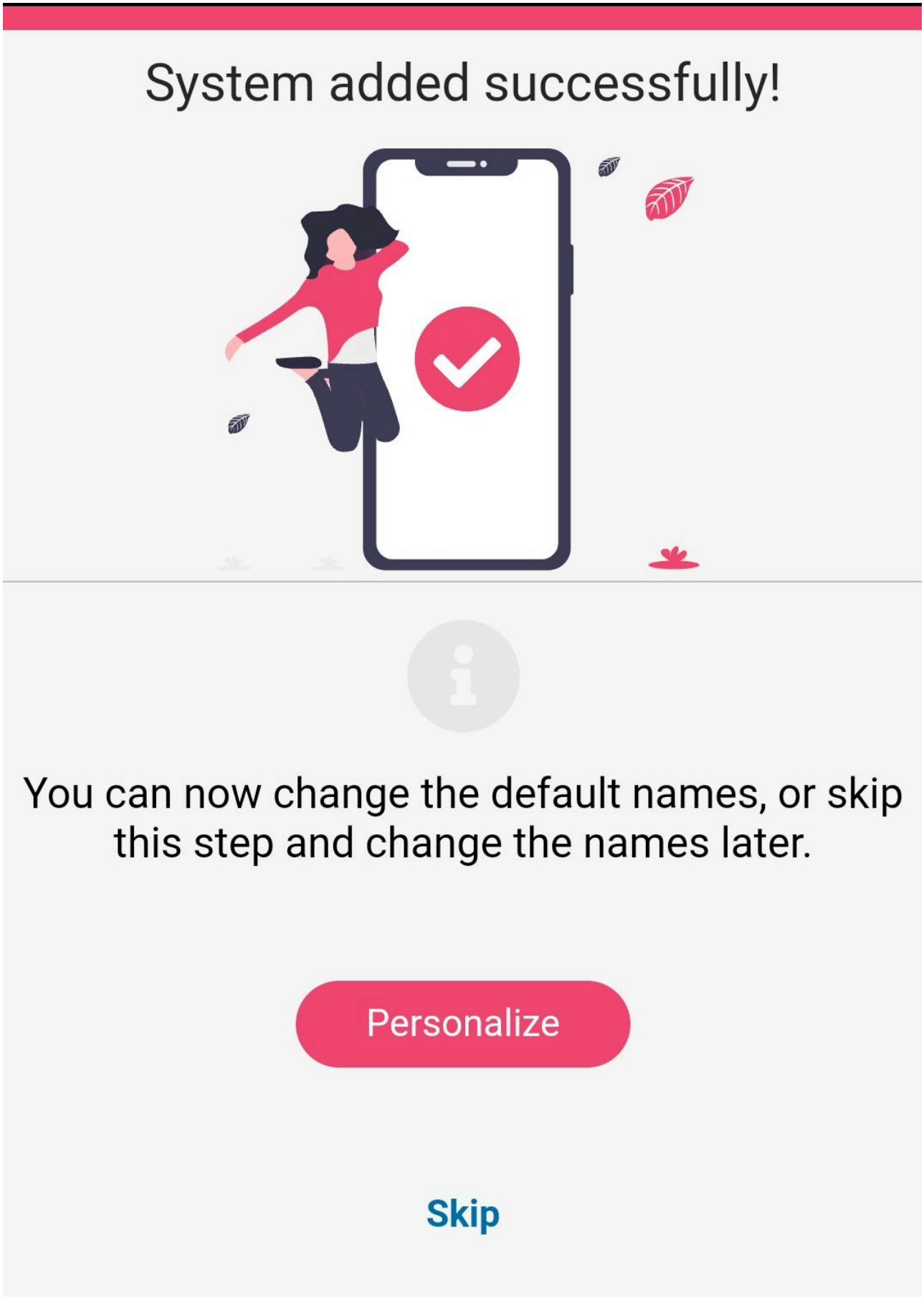

5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



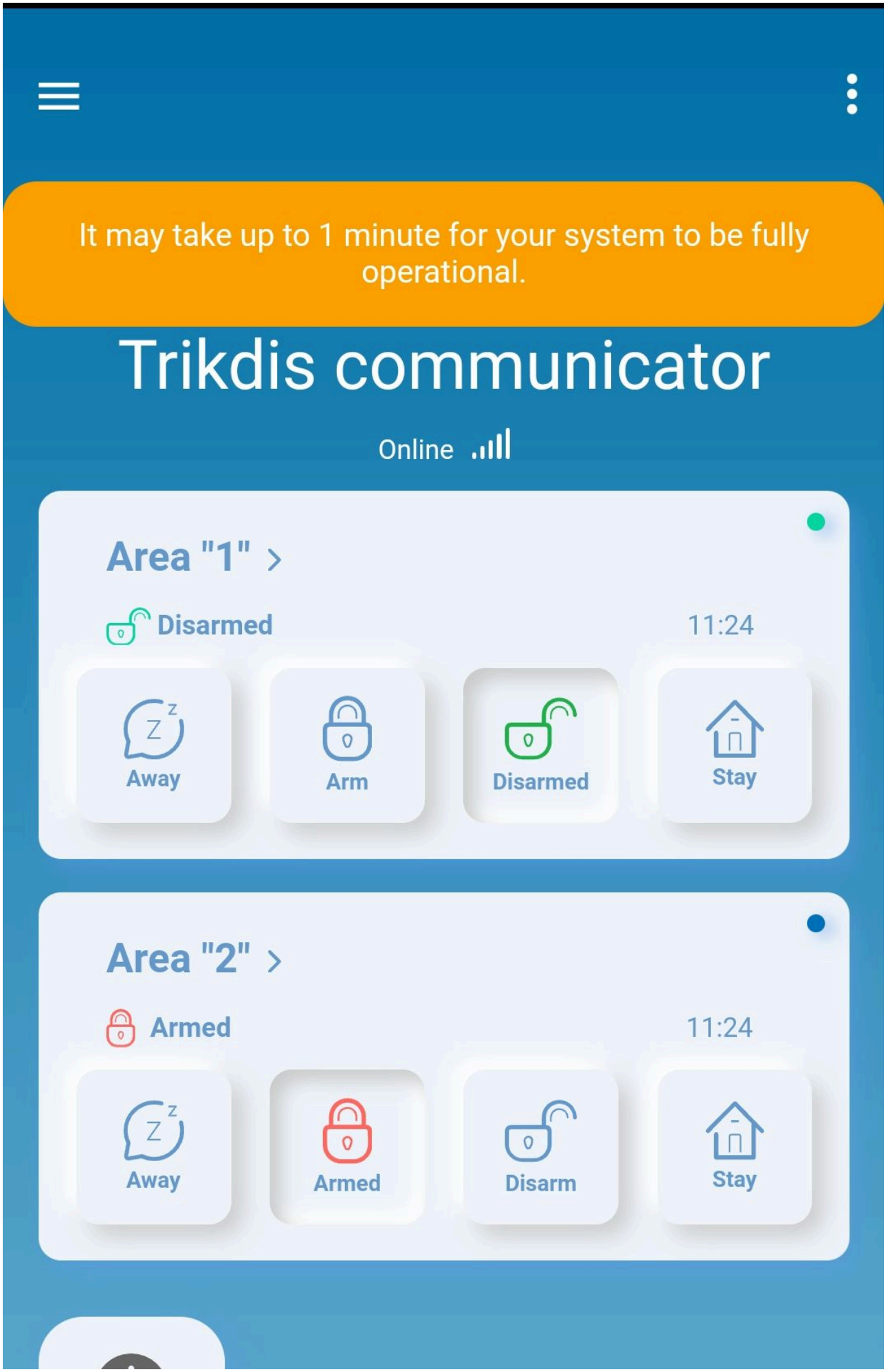

6. Add meg a rendszer nevét és válassz idozónát




7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.




8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


It may take up to 1 minute for your system to be fully operational.
Trikdis communicator
Online
Area "1" >
Disarmed
11:24
Away
Arm
Disarmed
Stay
Area "2" >
Armed
11:24
Away
Armed
Disarm
Stay




L'identificativo univoco del dispositivo (**IMEI**) si legge sulla scatola e sul retro del dispositivo, ed è mostrato anche nella barra di stato di TrikdisConfig.

## 5.2 Inserimento e disinserimento con un'uscita

Se vuoi inserire e disinserire la centrale d'allarme con l'uscita del comunicatore, tramite la zona a chiave della centrale, nell'app Protegus 2 indica per l'area quale uscita la controlla.

La zona della centrale a cui è collegata l'uscita del comunicatore deve essere programmata nella centrale come **zona a chiave**, e la centrale deve trasmettere gli eventi di inserimento e disinserimento – da questi Protegus 2 mostra lo stato dell'area.

L'impostazione si può fare alla creazione del sistema, quando aggiungi le aree, oppure in seguito nelle impostazioni del sistema, modificando l'area. Alla creazione del sistema ti guida la procedura guidata di Protegus 2: fai clic sul pulsante **Continue** (Continua), inserisci il nome dell'area (**Area name**) e abilita il controllo dell'uscita PGM dall'app Protegus 2 – con i passaggi seguenti:

1. Seleziona (o aggiungi) l'area che vuoi controllare. Il numero dell'area deve coincidere con quello che la centrale invia negli eventi (l'area 1 con l'1, la 2 con il 2).
2. Attiva l'opzione **Controllo con PGM** (Control with Protegus2) e nel campo **uscita** (Assigned Output) scegli l'uscita del comunicatore (PGM1, PGM2 …). Un'uscita può controllare una sola area.
3. Scegli la modalità di funzionamento: **a impulso** (Pulse) o **bistabile** (Level) – la stessa che hai impostato nella centrale per la zona a chiave. Di solito si usa quella a impulso; si può indicare anche la durata dell'impulso (predefinito 3 s).
4. Salva l'impostazione (**Save**). Con più aree ripeti per ciascuna, con la propria uscita: nella procedura guidata aggiungi un'altra area con il pulsante **Click to add an area** e imposti la sua uscita PGM allo stesso modo. Quando hai impostato tutte le aree, prosegui nella procedura guidata con il pulsante **Skip**.

Protegus 2 può mostrare correttamente lo stato delle aree solo se la centrale invia gli eventi di inserimento e disinserimento con il numero di area corretto. I dettagli e le insidie dell'inserimento tramite zona a chiave sono trattati in un articolo a parte: Inserimento da remoto tramite zona a chiave dall'app Protegus 2.

## 5.3 Inserimento e disinserimento dall'app

1. Apri il sistema nell'app Protegus 2. Nella schermata iniziale ogni area ha la propria scheda e il proprio lucchetto: il **lucchetto chiuso, rosso** indica un'area inserita, il **lucchetto aperto, verde** un'area disinserita.
2. Tocca il lucchetto dell'area e scegli l'operazione desiderata: inserimento o disinserimento.
3. Se l'app lo richiede, inserisci il codice PIN.

Il lucchetto assume lo stato effettivo in base all'evento ricevuto dalla centrale d'allarme; l'app conferma anche nell'elenco eventi e con una notifica se la centrale ha eseguito l'operazione.

### 5.4 Comando con messaggi SMS

Il comunicatore può essere controllato e programmato anche tramite messaggi SMS. Struttura del messaggio:

`PASSWORD spazio COMANDO spazio DATI` – ad esempio `123456 OUTPUT1 ON`

Con la password **amministratore** si possono usare tutti i comandi, con la password **installatore** i comandi INFO, RESET e OUTPUTx.

| Comando | Dati | Che cosa fa | Esempio |
|---|---|---|---|
| `INFO` | – | Richiede informazioni sul dispositivo: tipo, IMEI, numero di serie, versione firmware | `123456 INFO` |
| `RESET` | – | Riavvia il dispositivo | `123456 RESET` |
| `OUTPUTx` | `ON` | Attiva l'uscita x | `123456 OUTPUT1 ON` |
| `OUTPUTx` | `OFF` | Disattiva l'uscita x | `123456 OUTPUT1 OFF` |
| `OUTPUTx` | `PULSE=tttt` | Genera un impulso sull'uscita x; `tttt` = la durata dell'impulso in secondi, con quattro cifre | `123456 OUTPUT2 PULSE=0002` |
| `CONNECT` | `PROTEGUS=ON` / `PROTEGUS=OFF` | Abilita o disabilita la connessione a Protegus | `123456 CONNECT PROTEGUS=ON` |
| `CONNECT` | `IP=indirizzo:porta` | Indirizzo IP e porta del canale primario | `123456 CONNECT IP=192.120.120.255:8000` |
| `CONNECT` | `ENC=chiave` | La chiave di crittografia TRK | `123456 CONNECT ENC=123456` |
| `CONNECT` | `APN=nome` | L'APN della scheda SIM | `123456 CONNECT APN=internet` |
| `CONNECT` | `USER=nome` | Nome utente APN (se richiesto dall'operatore) | `123456 CONNECT USER=user` |
| `CONNECT` | `PASS=password` | Password APN (se richiesta dall'operatore) | `123456 CONNECT PASS=password` |

Puoi limitare da quali numeri di telefono il dispositivo accetta comandi: TrikdisConfig → pagina **User reporting** → **Control by SMS**. Se non è indicato nessun numero, esegue i comandi con password corretta provenienti da qualsiasi numero.

Nel G16T il comando `CONNECT` ha un ulteriore dato: `CP=1` disattiva, `CP=2` attiva l'interfaccia della linea telefonica del comunicatore. Esempio: `123456 CONNECT CP=2`.

## 6. TrikdisConfig – le impostazioni in dettaglio

Nella finestra di TrikdisConfig si vedono a sinistra l'elenco delle pagine (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), in alto la barra dei pulsanti (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), in basso la barra di stato. Questo capitolo esamina le impostazioni del G16T pagina per pagina.

### 6.1 La barra di stato

Dopo aver collegato e letto il dispositivo (**Read [F4]**), in fondo alla finestra compaiono i dati principali del dispositivo:

| Etichetta | Significato |
|---|---|
| **IMEI / Unique ID**, nei dispositivi Ethernet **MAC / Unique ID** | L'identificativo univoco del dispositivo: nei dispositivi con scheda SIM l'IMEI, nei dispositivi Ethernet l'indirizzo MAC. Lo stesso è riportato sulla scatola e sul retro del dispositivo. |
| **Status** | Lo stato di funzionamento attuale. |
| **Device** | Il tipo (la sigla) del dispositivo. Verifica che qui compaia il tipo del tuo dispositivo. |
| **SN** | Numero di serie. |
| **BL** | La versione del bootloader. |
| **FW** | La versione del firmware. |
| **HW** | La versione dell'hardware. |
| **State** | La modalità di connessione: USB o da remoto (remote). |
| **Administrator / Installer** | Il livello di accesso di chi esegue la programmazione (dopo l'inserimento della password). |

Dopo aver eseguito le impostazioni, le scrivi nel dispositivo con il pulsante **Write [F5]**; con i pulsanti **Open [F8]** e **Save [F9]** puoi salvare l'intero set di impostazioni su file e caricarlo in un altro dispositivo. **Save [F9]** salva le impostazioni in un file di configurazione, **Open [F8]** apre il file salvato; le impostazioni salvate si possono caricare in seguito anche in altri dispositivi, così puoi configurare più dispositivi rapidamente con le stesse impostazioni.




**Figura 23.** La barra di stato di TrikdisConfig con un G16T letto: identificativo, stato, tipo, numero di serie, versioni, modalità di connessione e livello di accesso.

Dopo **Read [F4]** il programma legge e mostra i valori impostati nel dispositivo; effettua le impostazioni necessarie seguendo le descrizioni delle pagine qui sotto.

## 6.2 System settings

La pagina è composta da due gruppi: nel gruppo **General** imposti il funzionamento di base del dispositivo, nel gruppo **Access** i livelli di accesso.

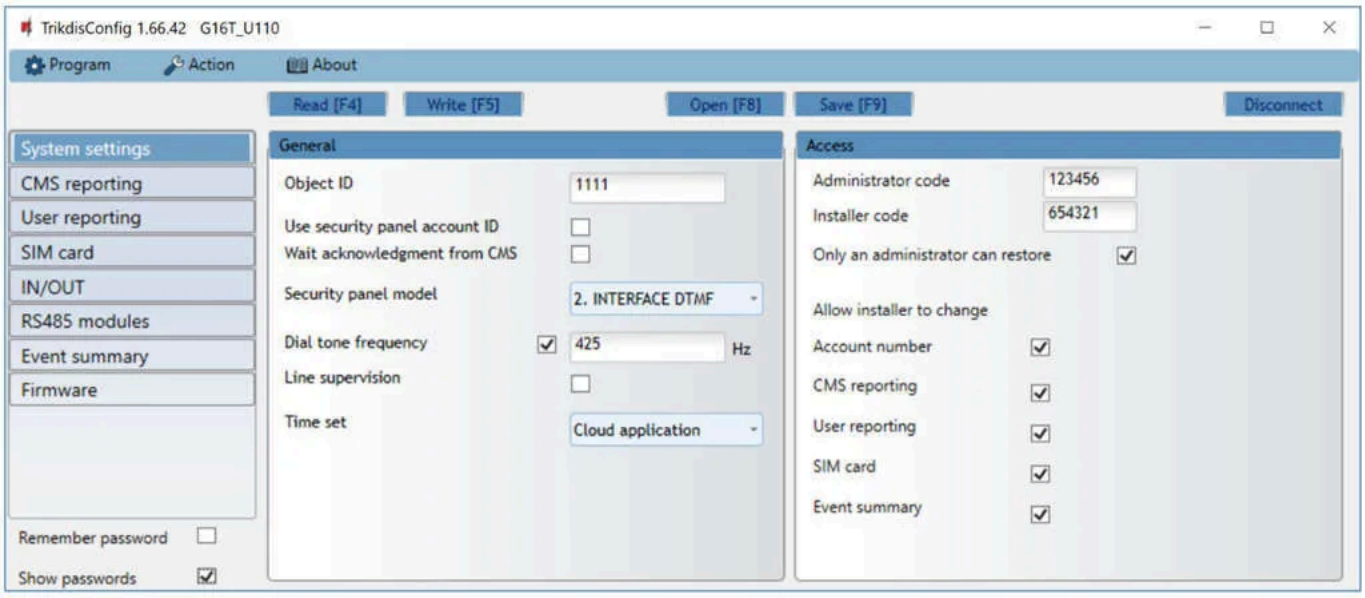



**Figura 24.** TrikdisConfig – pagina System settings: gruppi General e Access.

- **Object ID** – il codice impianto ricevuto dalla centrale di vigilanza (4 caratteri esadecimali: 0–9, A–F; `FFFE` e `FFFF` non si possono usare). Obbligatorio se il dispositivo trasmette anche a una centrale di vigilanza.
- **Use security panel account ID** – se spuntato, il comunicatore non usa il proprio Object ID, ma il codice che la centrale invia nel messaggio Contact ID. Utile se più aree trasmettono con codici separati.
- **Wait acknowledgment from CMS** – se spuntato, il comunicatore dopo ogni evento attende la conferma del ricevitore, e solo dopo invia alla centrale il segnale di chiusura (kiss-off). Se la conferma non arriva, la centrale invia di nuovo l'evento. In un sistema senza centrale di vigilanza, solo con Protegus 2, lascialo disattivato (stato di fabbrica).
- **Security panel model** – il tipo di interfaccia della linea telefonica (con questo abiliti o disabiliti l'interfaccia DTMF della linea telefonica del comunicatore); predefinito **2. INTERFACE DTMF**.
- **Dial tone frequency** – la frequenza del tono di linea che il G16T fornisce verso la centrale (predefinita 425 Hz, che è il tono di linea usato anche in Italia e nella maggior parte dei paesi europei).
- **Line supervision** – supervisione del cavo tra la centrale e il comunicatore; richiede anche il collegamento dei fili T-1 e R-1 (paragrafo 3.3.1).
- Sull'hardware 4 il tipo degli ingressi e il ruolo delle uscite si impostano nella pagina **IN/OUT** (punto 6.6). Sull'hardware 3 questi due campi sono qui: **Input IN1-IN2 type** – il tipo di ingresso dall'elenco (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL); **Output OUT1 mode** – la modalità di funzionamento dell'uscita dall'elenco.
- **Time set** – la fonte dell'orologio del dispositivo (predefinita **Cloud application**, il cloud Protegus).

Nel gruppo **Access** gestisci i livelli di accesso e le password.

Per le impostazioni del dispositivo esistono due livelli di accesso: **amministratore** e **installatore**.

- **Administrator code** – accesso a tutte le impostazioni (password di fabbrica: `123456`; la password è di 6 caratteri: cifre o lettere latine).
- **Installer code** – accesso limitabile (password di fabbrica: `654321`).
- **Only an administrator can restore** – con la spunta solo l'amministratore può avviare il ripristino delle impostazioni di fabbrica.
- **Allow installer to change** – qui puoi indicare quali gruppi di impostazioni può modificare l'installatore: **Account number** (codice impianto), **CMS reporting**, **User reporting**, **SIM card** (nei dispositivi su rete mobile) o **Ethernet settings** (nei dispositivi Ethernet), **Event summary**.

Non lasciare le password di fabbrica nel dispositivo!

Alla messa in servizio cambia almeno la password amministratore e annotala in un luogo sicuro. Una password dimenticata non si può cancellare nemmeno con il ripristino delle impostazioni di fabbrica, perché anche questo richiede la password: in tal caso solo il produttore o il distributore può ripristinarla, se gli fai avere il dispositivo. Fa eccezione il dispositivo con pulsante RESET fisico: tenendolo premuto per 10 secondi si ripristinano le impostazioni di fabbrica senza password.

## 6.3 CMS reporting

Il comunicatore invia gli eventi alla centrale di vigilanza tramite connessione dati mobile (IP) o via SMS. Gli eventi possono passare su più canali: il canale **primario** e quello **parallelo** funzionano contemporaneamente (verso due ricevitori), e a ciascuno appartiene un canale di **riserva**, che entra in funzione se il canale in questione si interrompe. La comunicazione è crittografata e protetta da password; per la ricezione e l'inoltro degli eventi al software della centrale di vigilanza serve un ricevitore Trikdis (ricevitore software IPcom – Windows o Linux –, RL14, RM14; per la ricezione SMS il ricevitore IP/SMS RL14, il ricevitore multicanale RM14 o il ricevitore SMS GM14) oppure un ricevitore universale che supporti il protocollo DC-09 / TL150. L'SMS è particolarmente utile come canale di riserva, perché funziona anche senza Internet mobile; come canale primario non lo consigliamo.

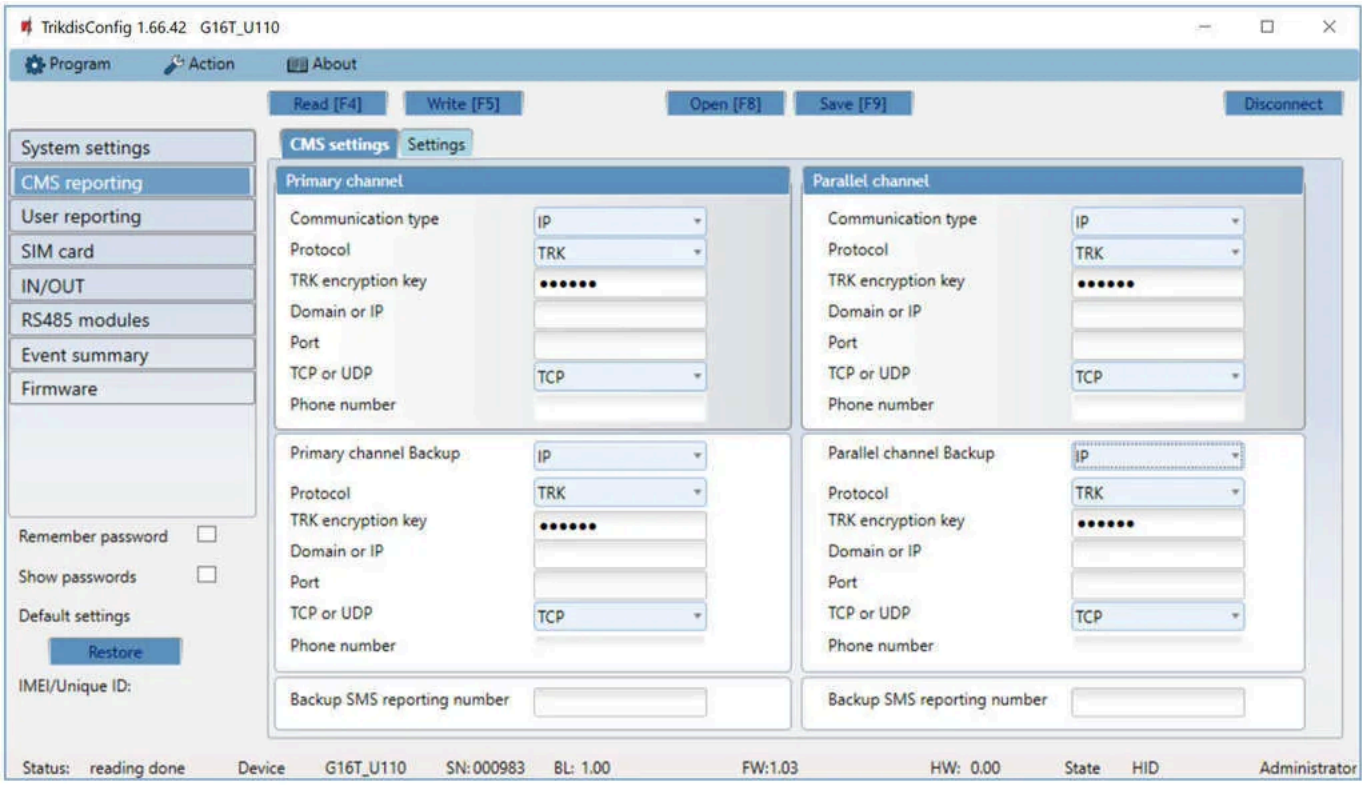



**Figura 25.** TrikdisConfig – CMS reporting, scheda CMS settings: canale primario, di riserva e parallelo.

### Primary channel – canale primario

- **Communication type** – IP o SMS.
- **Protocol** – TRK (ricevitori Trikdis), DC-09_2007 o DC-09_2012 (ricevitori universali), TL150 (SUR-GARD).
- **TRK encryption key** – chiave di crittografia di 6 cifre; deve essere la stessa nel comunicatore e nel ricevitore.
- **Domain or IP**, **Port** – l'indirizzo e la porta del ricevitore.
- **TCP or UDP** – il protocollo di trasmissione.

- **Phone number** – solo per la comunicazione via SMS: il numero di telefono del ricevitore SMS Trikdis con prefisso internazionale (ad es. `39xxxxxxxxx` per un numero italiano).

**Primary channel Backup – canale di riserva.** Subentra nella comunicazione se il canale primario non funziona; le sue impostazioni sono uguali a quelle sopra.

**Parallel channel – canale parallelo.** Oltre al primario invia contemporaneamente a un secondo ricevitore (ad esempio alla centrale di vigilanza locale e a quella centrale). Ha un proprio canale di riserva.

**Backup SMS reporting number – numero SMS di riserva.** Entra in funzione se l'invio non riesce né sul canale primario, né su quello parallelo, né su quello di riserva; è utile perché funziona anche senza connessione IP. È attivo solo se il canale primario e quello di riserva sono in modalità IP. Il dispositivo invia un SMS al ricevitore SMS della centrale di vigilanza dopo il primo avvio, e anche se la connessione TCP/IP o UDP/IP si interrompe sia sul canale primario sia sulla sua riserva. Inserisci il numero di telefono del ricevitore SMS Trikdis con prefisso internazionale (ad es. `39xxxxxxxxx` per un numero italiano).

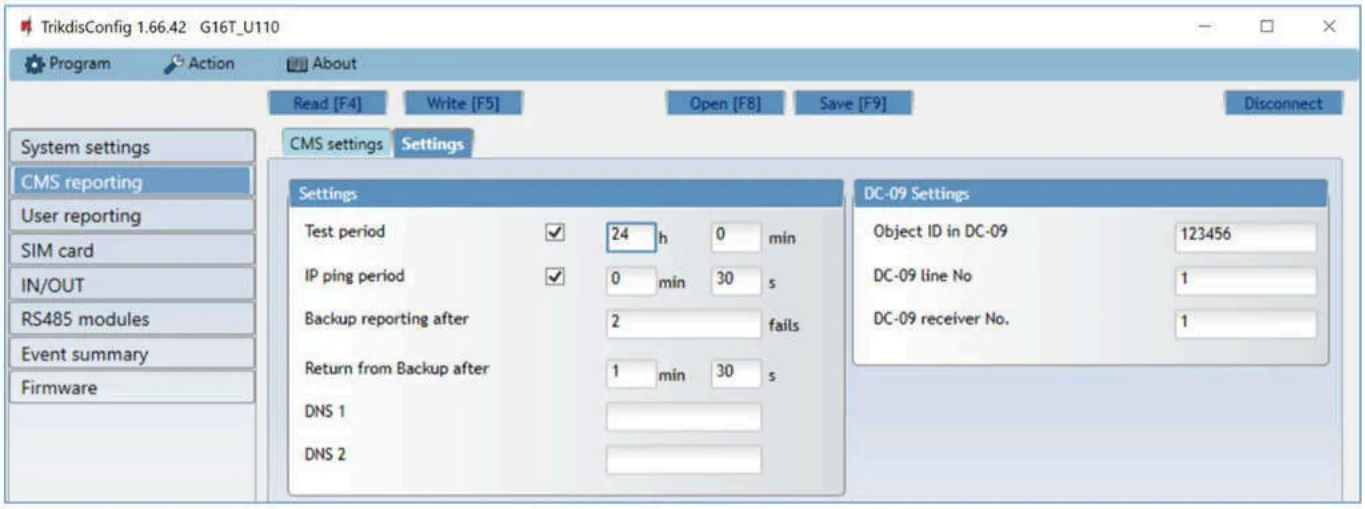



**Figura 26.** TrikdisConfig – CMS reporting, scheda Settings: rapporto di test, PING, temporizzazioni del canale di riserva, DNS e dati DC-09.

Nella scheda **Settings** imposti le temporizzazioni e i dati DC-09.

- **Test period** – l'intervallo del rapporto di test periodico (predefinito 24 ore). Il rapporto di test viene inviato come messaggio Contact ID alla centrale di vigilanza e a Protegus 2.
- **IP ping period** – l'intervallo del segnale di esistenza in vita (PING) sul canale IP (predefinito 30 s). Lo attivi con la spunta e imposti il tempo nelle caselle dei minuti (**min**) e dei secondi (**s**) del campo; è necessario per la supervisione del collegamento. Il ricevitore non inoltra i PING al software della centrale di vigilanza, per non sovraccaricarlo; il software riceve un messaggio solo se il ricevitore non riceve PING per il triplo del tempo impostato. Se ad esempio il periodo di PING è di 3 minuti, la perdita del collegamento viene segnalata dopo il 9° minuto.
- **Backup reporting after** – dopo questo numero di tentativi di invio falliti il dispositivo passa al canale di riserva (predefinito 2).
- **Return from Backup after** – dopo questo tempo torna al canale primario (predefinito 1 minuto 30 s).

Il PING mantiene attivo il collegamento tra il dispositivo e il ricevitore, e da esso dipendono anche l'accesso, il controllo e la programmazione da remoto. Per questo **non consigliamo un periodo di PING superiore a 5 minuti**.

**DC-09 Settings** (sul lato destro della scheda) – va compilato solo se invii su uno dei canali con protocollo DC-09_2007 o DC-09_2012; il gruppo compare quando nel campo **Protocol** di uno dei canali è selezionato DC-09_2007 o DC-09_2012:

- **Object ID in DC-09** – identificativo esadecimale di 3–16 caratteri, fornito dalla centrale di vigilanza.
- **DC-09 line No** – il numero della linea.
- **DC-09 receiver No.** – il numero del ricevitore.

In fondo alla scheda: **DNS 1, DNS 2** – server dei nomi (DNS, Domain Name System: fornisce l'indirizzo IP corrispondente al nome di dominio); servono se hai indicato il ricevitore con un nome di dominio e non con un indirizzo IP. Il valore predefinito è il DNS pubblico di Google.

## 6.4 User reporting

Nella scheda **PROTEGUS Cloud** abiliti il servizio Protegus. Con il servizio Protegus l'utente può monitorare e comandare a distanza il comunicatore e il sistema collegato; dettagli: www.protegus.app.

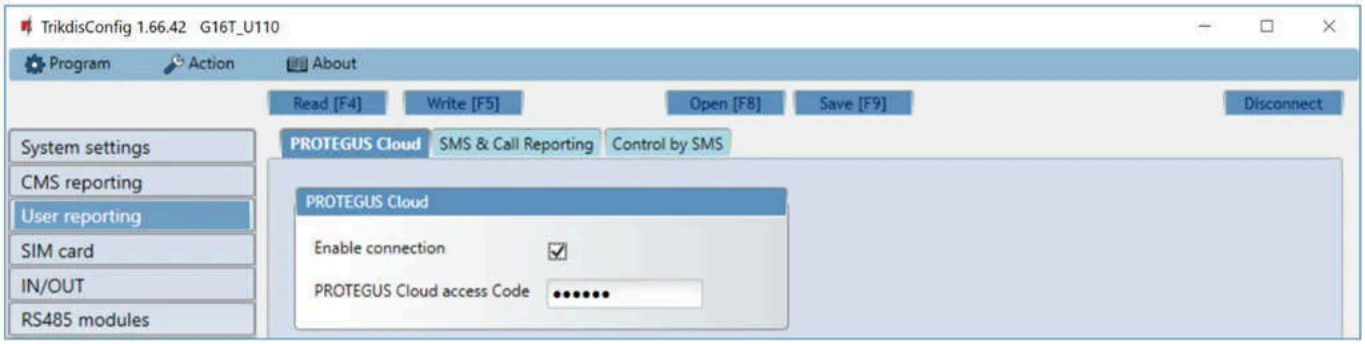



**Figura 27.** TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- **Enable connection** – abilita la connessione con il cloud Protegus e l'accesso remoto di TrikdisConfig.
- **Protegus Cloud access code** – codice di 6 cifre per la connessione Protegus (di fabbrica `123456`). Si può impostare solo prima della creazione del sistema in Protegus 2, in seguito non si può modificare.

Nella scheda **SMS & Call Reporting** l'utente può ricevere notifiche degli eventi anche via SMS o con una chiamata telefonica.

In caso di allarme, il dispositivo invia prima l'SMS a tutti i numeri di telefono inseriti, poi li chiama uno alla volta, da Tel 1 a Tel 4. Ogni numero viene chiamato una sola volta e squilla per 20 secondi; la chiamata è considerata riuscita se il numero squilla (basta anche che si risponda o si rifiuti). Il modem effettua la chiamata su 2G o VoLTE. Dove l'operatore ha spento il 2G e non ha approvato il modem per la VoLTE, l'SMS arriva ma il telefono non squilla. Non è un errore di configurazione. In questi casi usa gli SMS e l'app Protegus 2.

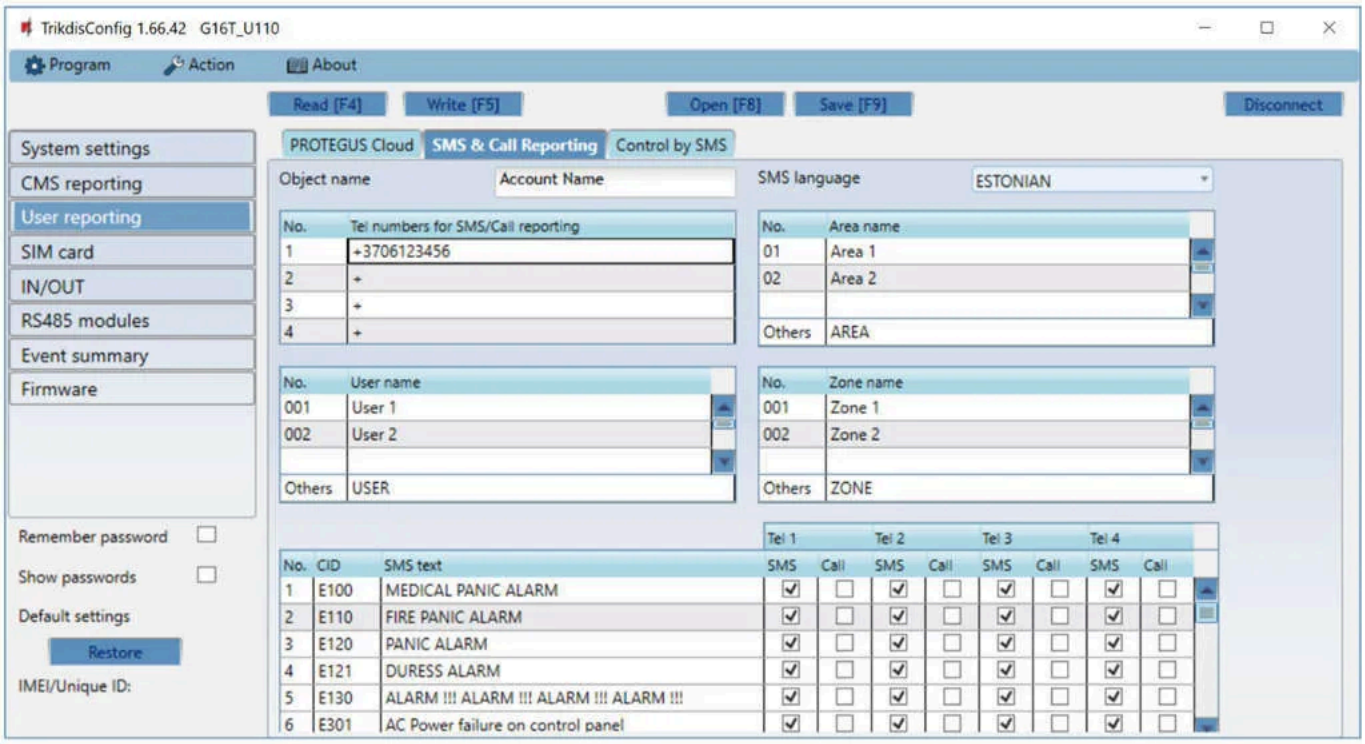



**Figura 28.** TrikdisConfig – User reporting, scheda SMS & Call Reporting.

- **Object name** – il nome del sistema; compare in ogni SMS.
- **SMS language** – la lingua degli SMS (per i caratteri accentati della lingua).
- **Tel numbers for SMS/Call reporting** – fino a 4 numeri di telefono con prefisso internazionale (ad es. per un numero italiano `+39…`, `0039…` o `39…`).
- **Area name, User name, Zone name** – i nomi delle aree, degli utenti e delle zone; il dispositivo li usa nel testo degli SMS. Nella tabella corrispondente scrivi il numero dell'area, dell'utente o della zona, e accanto il suo nome.
- **CID event table** – per ogni evento si può impostare quale numero riceve l'SMS o la chiamata; anche il testo del messaggio e il codice Contact ID si possono modificare, e si può aggiungere un nuovo evento.

Nella scheda **Control by SMS** imposti la ricezione dei comandi SMS (i comandi sono descritti al punto 5.4).

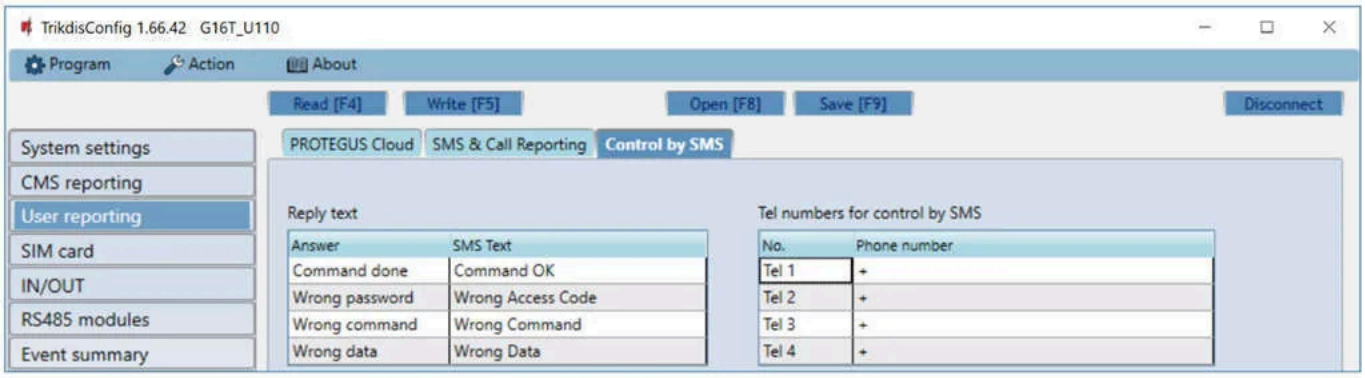



**Figura 29.** TrikdisConfig – User reporting, scheda Control by SMS.

- **Reply text** – il testo dei quattro messaggi di risposta al comando SMS: comando eseguito (Command done), password errata (Wrong password), comando errato (Wrong command), dato errato (Wrong data). I testi di risposta sono modificabili.
- **Tel numbers for control by SMS** – fino a 4 numeri; il dispositivo accetta comandi solo da questi numeri. Se è vuoto, accetta il comando con la password corretta da qualsiasi numero. Anche in questo caso la sicurezza è data dal fatto che nel comando è obbligatoria la password dell'amministratore o

dell'installatore.

## 6.5 SIM card

Senza i dati della scheda SIM il dispositivo non si connette alla rete dati.

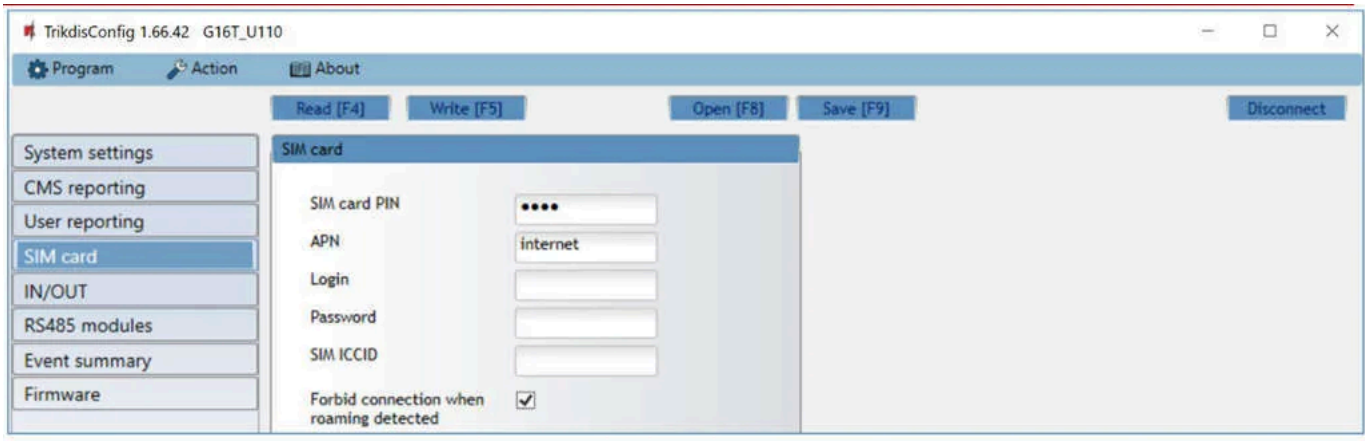



**Figura 30.** TrikdisConfig – pagina SIM card.

- **SIM card PIN** – il codice PIN della scheda. Puoi disattivare la richiesta del PIN mettendo la scheda in un telefono cellulare e disabilitandola lì. Se la richiesta del PIN è disattivata, il campo può restare con il valore di fabbrica.
- **APN** – il punto di accesso dell'operatore; gli APN noti degli operatori sono elencati nell'articolo sugli APN (per una scheda IoT / M2M l'operatore fornisce un APN separato, vedi il punto 2.2). L'APN è necessario per la connessione a Internet del dispositivo; se non hai altre informazioni, prova l'APN `internet`, che è generico e funziona nella rete di molti operatori.
- **Login, Password** – nome utente e password dell'APN, se l'operatore li richiede.
- **Forbid connection when roaming detected** – utile vicino al confine di stato: impedisce che il dispositivo si connetta alla rete del paese vicino.

Prima dell'uso assicurati che la scheda SIM sia attiva e che, per la comunicazione IP, il servizio dati mobile sia abilitato.

## 6.6 IN/OUT

Qui imposti il ruolo dei tre morsetti I/O a doppia funzione del comunicatore: **Disabled** (non usato), **IN** (ingresso) o **OUT** (uscita). Per un ingresso bisogna indicare anche il tipo (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Sull'hardware 3 queste impostazioni sono nella pagina **System settings** (punto 6.2).

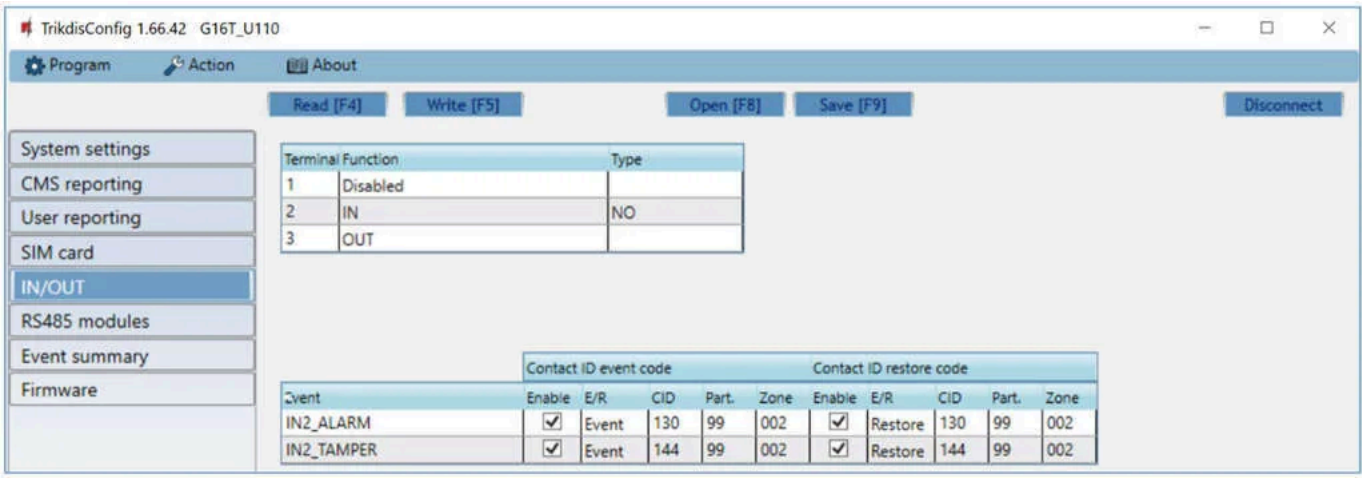



**Figura 31.** TrikdisConfig – pagina IN/OUT: funzione dei morsetti I/O ed eventi degli ingressi.

Quando il rilevatore collegato all'ingresso viene violato, il comunicatore invia un proprio evento (**INx_ALARM**, Contact ID 130), e quando viene violato il circuito tamper invia un evento di manomissione (**INx_TAMPER**, 144) alla centrale di vigilanza e a Protegus 2; nella tabella compaiono gli eventi di ogni morsetto impostato come ingresso. Le colonne della tabella:

- **Enable** – abilita l'invio del messaggio.
- **E/R** – il tipo di evento: Event (allarme) o Restore (ripristino).
- **CID** – il codice Contact ID.
- **Part.** – il numero dell'area nel messaggio.
- **Zone** – il numero della zona nel messaggio.

## 6.7 RS485 modules

Con le espansioni della serie iO si possono aggiungere al comunicatore ulteriori ingressi, uscite e un bus seriale per sensori di temperatura. Le espansioni iO-8 (e le altre espansioni della serie iO) e i moduli W485 / E485 collegati al bus RS485 vanno aggiunti nella scheda **Modules list**.

Sul G16T con modem 2G (G16T_G410) questa pagina non si può usare: la versione 2G non ha il bus RS485.

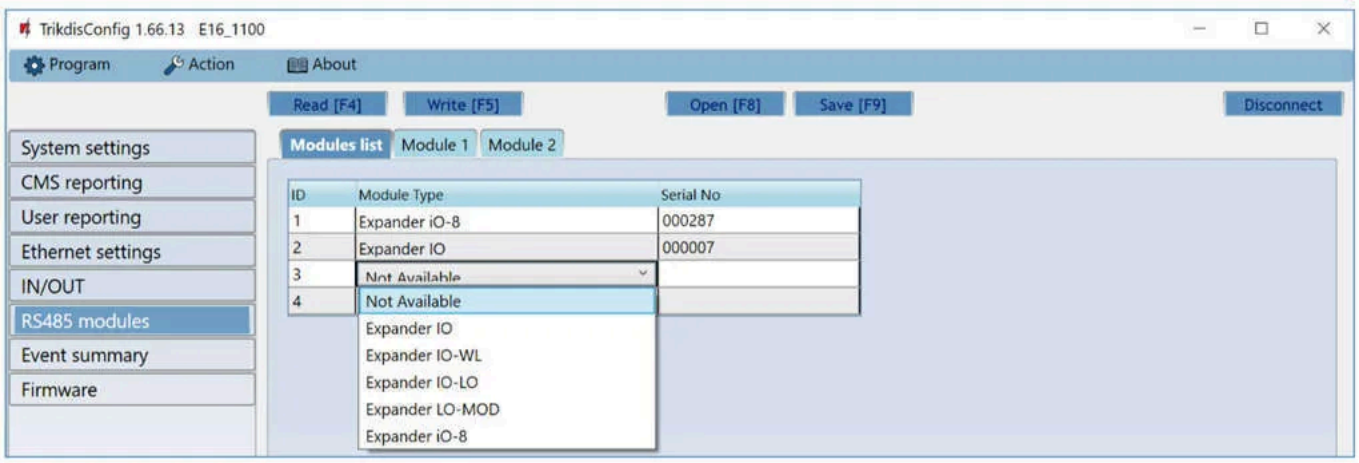



**Figura 32.** TrikdisConfig – RS485 modules, scheda Modules list.

- **Module Type** – il tipo del modulo collegato, dall'elenco (iO-8 e altre espansioni della serie iO, W485, E485).
- **Serial No** – il numero di serie di 6 cifre del modulo (sul modulo e sulla sua scatola, SN).

Dopo aver scelto il modulo e inserito il numero di serie premi il pulsante **Write [F5]**, scollega il cavo USB e attendi un minuto, finché il comunicatore registra il modulo. Poi ricollega il cavo, leggi il dispositivo (**Read [F4]**), e nella pagina RS485 modules compare la scheda numerata propria del modulo.

**Espansione iO-8** – 8 I/O a doppia funzione; al comunicatore si possono collegare al massimo 4 moduli.

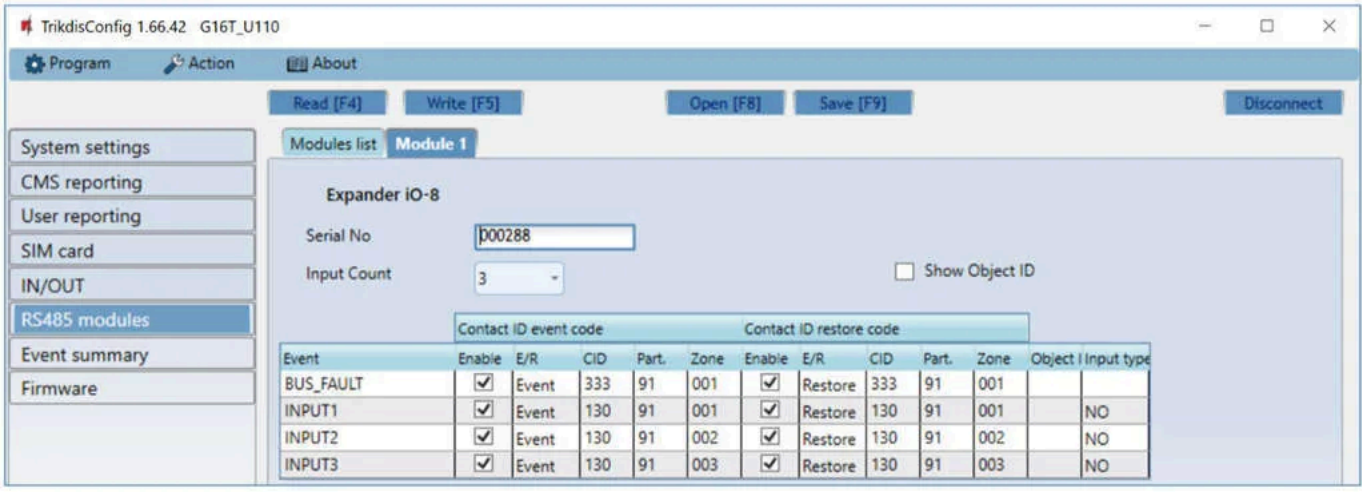



**Figura 33.** TrikdisConfig – RS485 modules, scheda del modulo iO-8.

- **Input Count** – quanti morsetti devono essere ingressi; gli altri saranno uscite. Il tipo di ingresso (**Input type**: NO o NC) si imposta nella tabella. Il ruolo delle uscite (inserimento / disinserimento o comando di un dispositivo) si imposta nell'app Protegus 2.
- Nella tabella puoi assegnare un codice Contact ID al guasto del bus (**BUS_FAULT**, Contact ID 333) e agli eventi di violazione e ripristino degli ingressi (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**); alla violazione dell'ingresso il comunicatore invia un evento con il codice impostato al ricevitore della centrale di vigilanza e a Protegus 2. Per impostazione predefinita il modulo 1 trasmette con l'area 91, il modulo 4 con l'area 94. Spuntando **Show Object ID** si può indicare per gli ingressi anche un codice impianto diverso da quello del comunicatore.
- Se l'utente deve ricevere un SMS o una chiamata anche per la violazione degli ingressi dell'espansione, aggiungi il codice evento Contact ID assegnato all'ingresso anche nella tabella della scheda **User reporting → SMS & Call Reporting**.

**Espansione iO** – 1 ingresso, 1 uscita relè (contatti del relè) e un bus seriale 1-Wire per sensori di temperatura. L'uscita relè si può comandare anche secondo condizioni logiche (SE … ALLORA).

- **Input IN1 type** – il tipo di ingresso (NO o NC).
- **Max °C (T1)** – se la temperatura è più alta di questo valore, il dispositivo invia un evento; per questo l'evento deve essere abilitato nella tabella.
- **Min °C (T2)** – se la temperatura è più bassa di questo valore, il dispositivo invia un evento; per questo l'evento deve essere abilitato nella tabella.
- Nella tabella puoi assegnare all'ingresso un codice Contact ID di evento e di ripristino allo stesso modo dell'espansione iO-8; alla violazione dell'ingresso il comunicatore invia un evento con il codice impostato al ricevitore della centrale di vigilanza e a Protegus 2.

**Modulo WiFi W485** (nell'elenco W17u/W485) – i dati della rete WiFi e le impostazioni di rete.

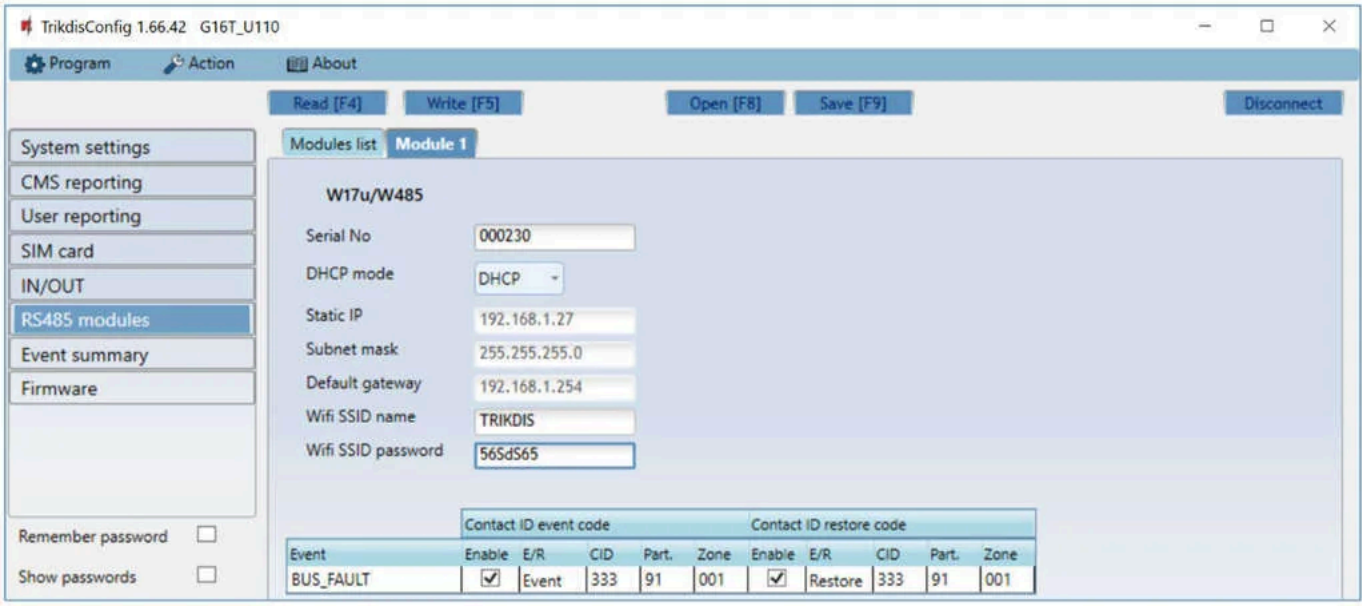



**Figura 34.** TrikdisConfig – RS485 modules, scheda del modulo W485.

- **DHCP mode** – impostazione di rete automatica o manuale.
- **Static IP**, **Subnet mask**, **Default gateway** – per l'impostazione manuale.
- **Wifi SSID name**, **Wifi SSID password** – il nome e la password della rete WiFi.
- Nella tabella puoi assegnare un codice Contact ID ai guasti del bus RS485 (interruzione e ripristino della connessione tra il modulo e il G16T); l'evento viene ricevuto sia dalla centrale di vigilanza sia da Protegus 2.

**Modulo Ethernet E485** – le stesse impostazioni di rete senza WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**), e allo stesso modo puoi assegnare un codice Contact ID ai guasti del bus RS485 (interruzione e ripristino della connessione tra il modulo e il G16T); l'evento viene ricevuto sia dalla centrale di vigilanza sia da Protegus 2.

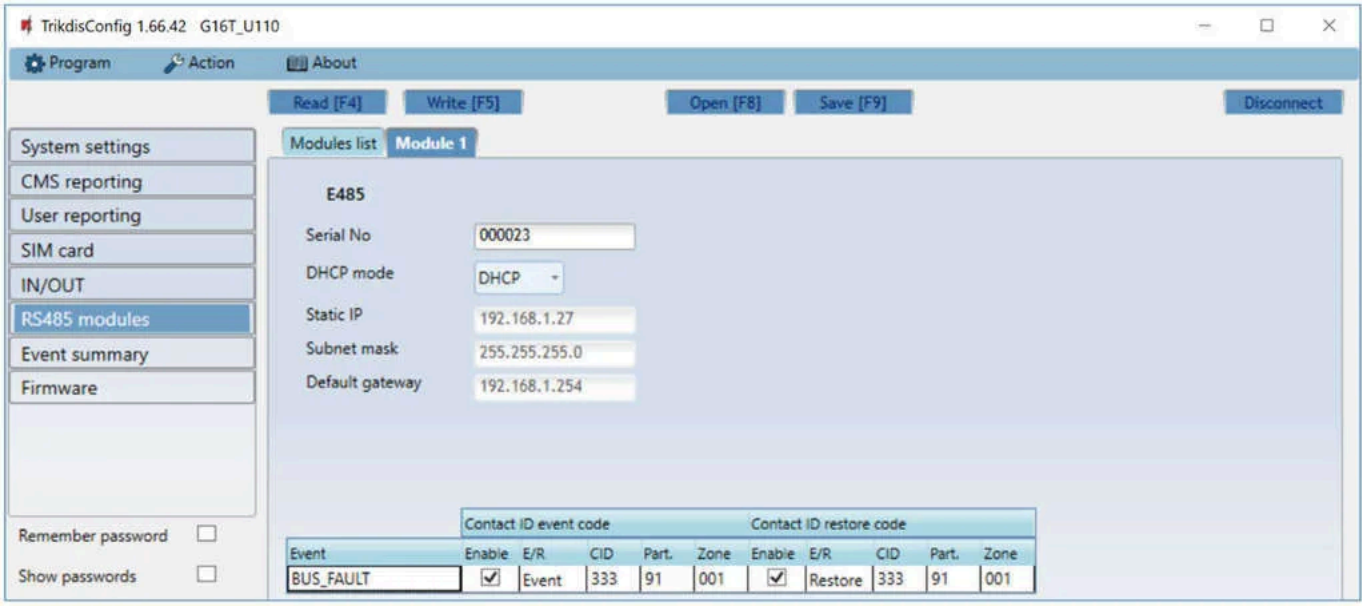



**Figura 35.** TrikdisConfig – RS485 modules, scheda del modulo E485.

Per il funzionamento del W485 e dell'E485 deve essere impostata la connessione del G16T con la centrale di vigilanza e/o con Protegus (punti 2.2 e 2.3), e normalmente nel G16T deve esserci anche una scheda SIM (se necessario, può funzionare anche senza SIM: Trikdis ha aggiunto questa possibilità in seguito, su richiesta).

## 6.8 Event summary

In questa pagina puoi attivare o disattivare i **messaggi interni propri** del dispositivo e modificarne il codice Contact ID, il numero di area e di zona. Un messaggio disattivato qui non viene inviato dal dispositivo su nessun canale. Di fabbrica i messaggi partono con l'area 99 e la zona 999.

| Messaggio | Contact ID | Quando viene generato |
|---|---|---|
| **COMMUNICATION** | 350 | La comunicazione tra il comunicatore e la centrale d'allarme si è interrotta (disattivato di fabbrica). Il comunicatore collegato al bus o alla porta seriale lo rileva direttamente; il comunicatore su linea telefonica solo con **Line supervision** attivata. |
| **POWER** | 302 | Tensione di alimentazione non adeguata (bassa); il ripristino è un messaggio a parte. |
| **REMOTE_STARTED** | 411 | È iniziata una programmazione da remoto con TrikdisConfig. |
| **REMOTE_FINISHED** | 412 | La programmazione da remoto è terminata. |
| **START** | 700 | Il dispositivo si è connesso alla rete (avvio). |
| **TEST** | 602 | Rapporto di test periodico. |
| **PING** | 760 | Il messaggio di esistenza in vita PING. Non compare nell'elenco di tutti i dispositivi: sulla schermata della versione hardware precedente sì, nella pagina Event summary delle versioni più recenti questa riga non c'è. L'intervallo si imposta nel campo **CMS reporting → Settings → IP ping period**. |

- **Enable** – abilita l'invio del messaggio alla centrale di vigilanza e a Protegus 2.
- **E/R** – il tipo di messaggio: Event (evento) o Restore (ripristino) – la riga indica il verificarsi dell'evento oppure il suo ripristino.
- **Part.** – il numero di area che il dispositivo invia per l'evento interno e per il ripristino.
- **Zone** – il numero di zona che il dispositivo invia per l'evento interno e per il ripristino.
- Il codice **CID**, l'**area** e la **zona** si possono modificare per qualsiasi evento; dove esiste un ripristino (Restore), il suo codice si può impostare separatamente.

Gli eventi degli ingressi propri (**INx_ALARM**, **INx_TAMPER**) si impostano nella pagina **IN/OUT**, gli eventi dei moduli di espansione (**BUS_FAULT**, **INPUTx**) nella pagina **RS485 modules**, nella scheda del modulo. L'abilitazione e l'intervallo del rapporto di test si impostano nel campo **CMS reporting → Settings → Test period**.

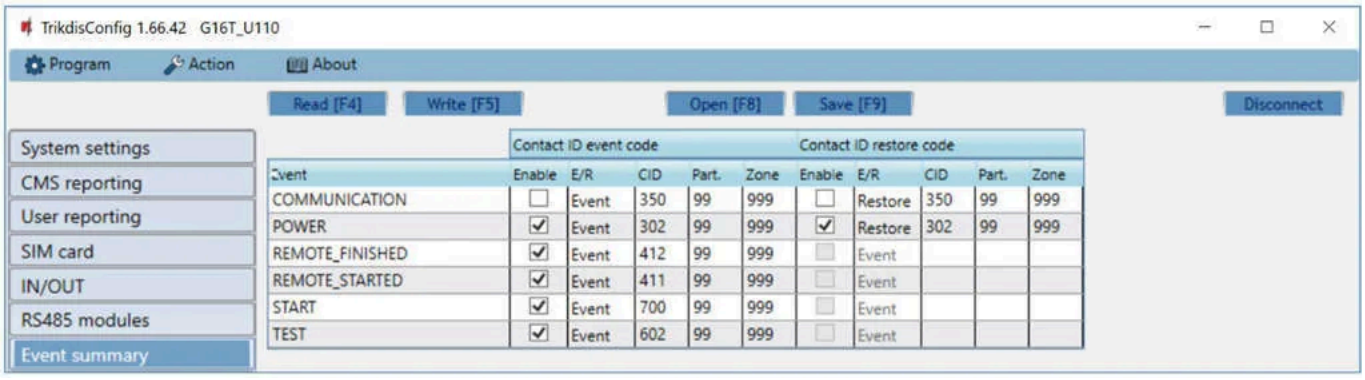



**Figura 36.** TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo.

### 6.9 Ripristino delle impostazioni di fabbrica

Per ripristinare le impostazioni di fabbrica fai clic sul pulsante **Restore** nel gruppo **Default settings**, nella parte in basso a sinistra della finestra di TrikdisConfig. Il ripristino cancella tutte le impostazioni – anche le password –, quindi conviene prima salvare le impostazioni su file (**Save [F9]**).

Con la password dell'installatore è possibile solo se l'amministratore non l'ha disabilitato nella pagina **System settings → Access**.

## 7. Programmazione a distanza

TrikdisConfig raggiunge i dispositivi Trikdis non solo tramite cavo USB, ma anche **da remoto, attraverso il cloud Protegus**. In questo modo puoi modificare le impostazioni di un dispositivo già installato senza recarti sul posto.

**Per l'accesso da remoto servono:**

1. Il dispositivo deve essere acceso e avere la connessione di rete (i LED **POWER** e **NETWORK** sono accesi verdi; nei dispositivi su rete mobile il NETWORK lampeggia anche giallo). Nei dispositivi su rete mobile la scheda SIM inserita deve essere attiva e il suo codice PIN deve essere impostato nel dispositivo, oppure la richiesta del PIN deve essere disattivata; nei dispositivi Ethernet il cavo di rete (LAN) deve essere collegato e il dispositivo deve raggiungere Internet.
2. Nella pagina **User reporting → PROTEGUS Cloud** di TrikdisConfig deve essere spuntato **Enable connection** (impostalo via USB, alla prima messa in servizio).
3. Devi conoscere l'**identificativo univoco** del dispositivo (IMEI o MAC – riportato sulla scatola e sul retro del dispositivo) e la password amministratore o installatore.

**Passaggi:**

1. Avvia il software TrikdisConfig.
2. Nella sezione **Remote access**, nel campo **Unique ID**, inserisci l'identificativo univoco del dispositivo (IMEI o MAC).
3. Se vuoi, dai un nome al sistema nel campo **System name** – il programma lo ricorda e la volta successiva puoi sceglierlo dall'elenco a discesa.
4. Premi il pulsante **Configure**.
5. Nella finestra che si apre fai clic sul pulsante **Read [F4]** (lettura) e inserisci la password. Con la spunta **Remember password** il programma la ricorda per questa sessione.
6. Esegui le modifiche, poi inviale al dispositivo con il pulsante **Write [F5]** (scrittura).

Il programma salva i sistemi programmati in precedenza da remoto e dotati di nome; puoi elencarli con la freccia accanto al campo **System name**. Per eliminarne uno seleziona l'identificativo nell'elenco, premi il tasto **Delete** e conferma.

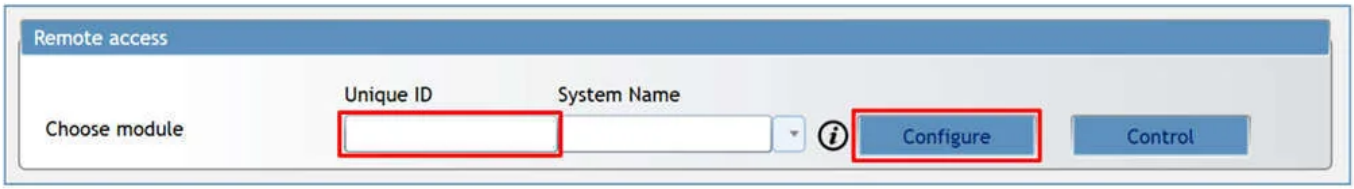



**Figura 37.** TrikdisConfig – Remote access: l'identificativo del dispositivo, il nome del sistema e il pulsante Configure.

L'abilitazione del cloud Protegus è descritta al punto 6.4.

## 8. Verifica del funzionamento del comunicatore

Dopo la programmazione e il cablaggio verifica sempre l'intera catena: centrale d'allarme → comunicatore → centrale di vigilanza e/o Protegus 2.

Prima controlla che ci sia alimentazione (il LED **POWER** è acceso verde) e che ci sia la connessione di rete (il LED **NETWORK** è acceso verde).

1. **Genera un evento.** Inserisci e poi disinserisci il sistema dalla tastiera, oppure, con il sistema inserito, viola una zona per generare un allarme.
2. **Verifica la ricezione.** Controlla che l'evento sia comparso nel software della centrale di vigilanza e/o nell'elenco eventi dell'app Protegus 2 – con il numero di area e di zona corretto.
3. **Ingressi.** Viola il sensore collegato a un ingresso proprio del comunicatore e verifica l'evento corrispondente.
4. **Uscite.** Attiva l'uscita dall'app Protegus 2 e verifica che il dispositivo collegato (relè, zona a chiave) entri effettivamente in funzione.
5. **Inserimento da remoto.** Se la centrale è controllabile da remoto, inseriscila e disinseriscila anche dall'app Protegus 2.

## 9. Aggiornamento del firmware

Ha bármikor az USB bedugásakor a program azt jelzi, hogy új firmware verzió jelent meg a Trikdis eszközhöz, fogadd el a frissítést és telepítsd!

Puoi aggiornare il firmware anche da solo – a una versione più recente e, se necessario, anche a una precedente. Dopo l'aggiornamento tutte le impostazioni del dispositivo restano invariate.

1. Avvia il software TrikdisConfig e collega il dispositivo con il cavo USB, oppure accedi alla sua programmazione da remoto.
2. Se c'è un firmware più recente, il programma ne propone il download – accetta.
3. Scegli la pagina **Firmware** e fai clic sul pulsante **Open firmware**. Seleziona il file del firmware.
4. Premi il pulsante **Update [F12]**, attendi la fine dell'aggiornamento, poi nella finestra che compare fai clic su **OK**. Nel frattempo non scollegare il cavo e non interrompere la connessione.

I file del firmware si trovano nella cartella di installazione di TrikdisConfig, all'interno della sottocartella **Firmwares**, nella cartella con il nome del dispositivo. Se questa cartella non c'è, o non esiste un aggiornamento per il dispositivo, oppure va aggiornato il software TrikdisConfig stesso. I file più recenti si possono scaricare anche dal sito del produttore, dalla pagina del dispositivo, come utente registrato.

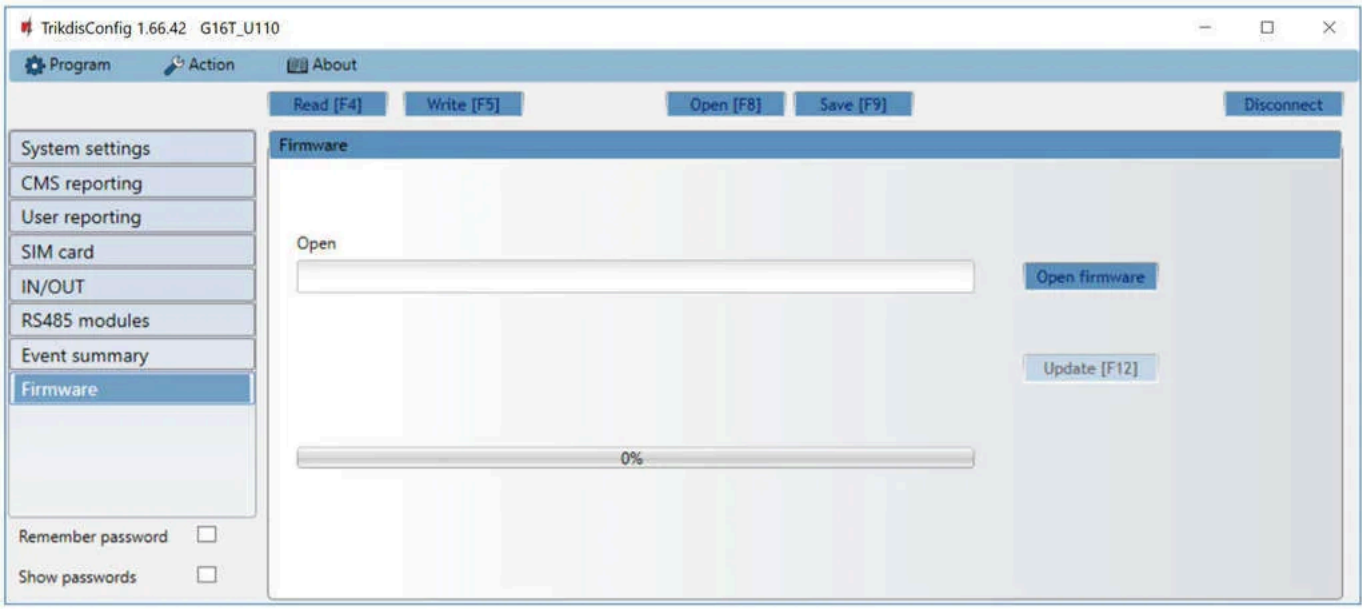



**Figura 38.** TrikdisConfig – pagina Firmware: Open firmware e Update [F12].

Per l'aggiornamento serve una connessione a Internet. Un antivirus, un firewall o impostazioni di rete restrittive possono impedire il download automatico del firmware; in questo caso scarica il file manualmente e aprilo nella scheda Firmware.

## 10. Risoluzione dei problemi e domande frequenti

Le domande e i guasti più frequenti, partendo dalle segnalazioni LED. Se la risposta rimanda al capitolo dettagliato, lì trovi la posizione esatta dell'impostazione.

### Il LED NETWORK è spento – nessuna rete

1. Guarda i lampeggi del LED **TROUBLE**: 1 = nessuna SIM, 2 = PIN errato, 3 = manca l'APN, 4 = non riesce a connettersi alla rete GSM, 5 = non riesce a connettersi alla rete dati.
2. Verifica che la scheda SIM sia attiva, abbia il servizio dati e sia inserita correttamente nell'alloggiamento.
3. Se sulla scheda è attiva la richiesta del PIN, inserisci il PIN nella pagina **SIM card**, oppure disattiva la richiesta del PIN usando un telefono.
4. Controlla l'antenna: è avvitata, non è in una scatola metallica, il livello del segnale è adeguato (punti 1.6 e 3.2).

### C'è rete, ma la centrale di vigilanza non riceve eventi

**Il LED DATA è il modo più semplice per verificare la connessione Internet.** Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

1. 6 lampeggi del LED **TROUBLE** indicano che non c'è connessione con il ricevitore: controlla l'indirizzo, la porta, l'impostazione TCP/UDP e la chiave di crittografia del ricevitore (**CMS reporting**).

2. Se il ricevitore è indicato con un nome di dominio, controlla l'impostazione DNS (**CMS reporting → Settings**).
3. Verifica che il piano dati della scheda SIM non blocchi la porta necessaria (alcune schede M2M consentono solo indirizzi determinati).

### La centrale non invia gli eventi al comunicatore

1. Il combinatore della centrale deve essere attivo, in modalità DTMF, con formato Contact ID e con il numero di telefono impostato (capitolo 4).
2. Controlla il collegamento TIP/RING; 7 lampeggi del LED **TROUBLE** indicano la mancanza di collegamento con la centrale (se collegato con supervisione della linea).
3. Se la centrale attende il tono di linea e non avvia la chiamata, disattiva in essa il controllo del tono di linea.
4. Se la centrale segnala un „errore di comunicazione" anche se l'evento è arrivato, controlla l'impostazione **Wait acknowledgment from CMS** (punto 6.2).

### Protegus 2 non vede il dispositivo

1. Nella scheda **User reporting → PROTEGUS Cloud** deve essere spuntato **Enable connection**.
2. Alla creazione del sistema bisogna inserire il **Protegus Cloud access code** impostato nel dispositivo; dopo la creazione del sistema non si può più modificare nel dispositivo.
3. Inserisci l'IMEI esattamente, prendendolo dalla scatola o dal retro.
4. Il servizio dati della scheda SIM e l'APN devono essere a posto (il LED NETWORK è verde e il LED DATA si spegne dopo un evento).

### Non riesco ad accedere a distanza con TrikdisConfig

1. Il dispositivo deve essere online (LED NETWORK verde) e la connessione Protegus deve essere abilitata.
2. **CMS reporting → Settings → IP ping period** non deve superare i 5 minuti: il PING mantiene la connessione necessaria per l'accesso remoto.
3. Controlla la password dell'amministratore o dell'installatore.

### Ho dimenticato la password

Una password dimenticata non si può recuperare né cancellare con il ripristino delle impostazioni di fabbrica, perché anche il ripristino richiede la password. In questo caso solo il produttore o il distributore può ripristinarla: il dispositivo va fatto pervenire a loro. Annota quindi le password impostate in un luogo sicuro.

### Perché non vedo la pagina RS485 modules, o perché l'iO-8 non funziona?

Il G16T con modem 2G (G16T_G410) non ha il bus RS485; iO-8, W485 ed E485 si possono collegare solo alla versione 4G (G16T_E120). Per i moduli W485 ed E485 normalmente nel G16T deve esserci anche una scheda SIM; se necessario, può funzionare anche senza SIM (una funzione aggiunta da Trikdis in seguito, su richiesta).

### Ho un dispositivo 2G – fino a quando funzionerà?

La dismissione delle reti 2G procede con tempi diversi a seconda dell'operatore; per un funzionamento a lungo termine consigliamo la versione 4G, che ha anche la riserva 2G. La versione 4G, inoltre, si può espandere anche tramite il bus RS485.

### Quanto traffico dati usa il dispositivo?

I messaggi di evento e i PING sono molto piccoli; il traffico dipende soprattutto dal periodo di PING e dalla frequenza dei rapporti di test. In un tipico sistema domestico il traffico mensile resta di solito sotto i 10 MB. Il valore esatto dipende dalle impostazioni e dall'unità di tariffazione dell'operatore, quindi con una scheda a traffico limitato conviene controllare il traffico del primo mese.

## 11. Norme di sicurezza

**Figyelem!**

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- Solo un installatore qualificato può installare ed effettuare la manutenzione delle apparecchiature di sicurezza.
- Prima dell'installazione leggi il manuale; ignorare le istruzioni può causare un funzionamento errato o un guasto.
- Prima del collegamento, prima di ogni connessione elettrica e prima dell'assistenza, scollega l'apparecchiatura dall'alimentazione.
- I guasti derivanti da installazione o uso non corretti, nonché le modifiche e le riparazioni non autorizzate dal produttore, fanno decadere la garanzia.
- Rispetta le norme locali sui rifiuti: non gettare il dispositivo guasto o le sue parti nei rifiuti domestici.

## Vedi anche

- Inserimento a distanza con zona a chiave dall'app Protegus 2 – dettagli e insidie dell'inserimento tramite zona a chiave.
- Arriva la versione hardware 4 dei comunicatori GSM G16 e G16T – che cosa è cambiato rispetto alla versione precedente.
- Le novità del comunicatore G16T v3 – l'annuncio del prodotto.
- Documentazione in inglese: docs.trikdis.com.

I manuali di docs.trikdis.com sono in inglese.

## Prodotti correlati

**Trikdis G16T 4G GSM comunicatore intelligente (TIP-RING)**

**Trikdis G16T 2G GSM comunicatore intelligente (TIP-RING)**

**Trikdis iO8 modulo di espansione cablato**

## Diritti d'autore

Questo manuale è stato realizzato da trikdis.hu e mobilamb.eu. Il testo, la struttura, le nostre illustrazioni e le integrazioni sono di nostra proprietà intellettuale e sono protetti dal diritto d'autore. Senza il nostro consenso non può essere copiato, distribuito né pubblicato su un altro sito web, né in tutto né in parte. Puoi scaricarlo e stamparlo liberamente per installare e usare il prodotto.

I nomi e i loghi Trikdis e Protegus sono marchi di UAB Trikdis.

Versione sempre aggiornata di questo manuale: https://trikdis.it/manuale-g16t