Comunicatore GT e GT+ – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente dei comunicatori Trikdis GT e GT+: collegamento al bus dati, alla porta seriale o all'uscita della linea telefonica della centrale d'allarme, programmazione della centrale, configurazione in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2.



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

Indice

1. Panoramica

- 1.1 A cosa serve e come funziona
- 1.2 Versioni: GT e GT+
- 1.3 Centrali d'allarme compatibili
- 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 Connessione all'app Protegus 2
- 2.3 Connessione 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 DSC – bus dati (Keybus)
  - 3.3.2 DSC – Keybus e TIP/RING (solo GT+)
  - 3.3.3 Paradox – porta seriale
  - 3.3.4 Paradox SP/MG – Keybus e TIP/RING
  - 3.3.5 UTC Interlogix (Caddx) – bus dati
  - 3.3.6 Texecom – porta seriale
  - 3.3.7 InnerRange Inception
  - 3.3.8 InnerRange Integriti
  - 3.3.9 Honeywell Vista – bus dati
  - 3.3.10 Qualsiasi centrale – TIP/RING
- 3.4 Collegamento della zona chiave
- 3.5 Collegamento degli ingressi
- 3.6 Collegamento di un'uscita con relè
- 3.7 Collegamento dell'espansione iO-8
- 3.8 Accensione e prima verifica
- A TRIKDIS átjelző elindítása

4. Programmazione della centrale d'allarme

- 4.1 Collegamento al bus dati o seriale
  - 4.1.1 DSC
  - 4.1.2 Paradox
  - 4.1.3 Texecom
  - 4.1.4 UTC Interlogix (Caddx)
  - 4.1.5 InnerRange
  - 4.1.6 Honeywell Ademco Vista
- 4.2 Collegamento alla linea telefonica (TIP/RING)
  - 4.2.1 Programmazione del combinatore Honeywell Vista
  - 4.2.2 Il combinatore UTC Interlogix (Caddx) NX

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 tramite 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 Panel settings
6.4 CMS reporting
6.5 User reporting
6.6 Network settings
6.7 IN/OUT
6.8 RS485 modules
6.9 Event summary
6.10 Ripristino delle impostazioni di fabbrica

7. Programmazione a distanza

8. Verifica del funzionamento del comunicatore

9. Aggiornamento del firmware

10. Ricerca guasti e domande frequenti

11. Norme di sicurezza

Vedi anche

1. Panoramica

GT e GT+ sono i **comunicatori per rete mobile 4G** di Trikdis, che inoltrano gli eventi della centrale d'allarme alla centrale di vigilanza e all'app Protegus 2. Si possono collegare alla centrale in due modi: **direttamente**, al bus dati o alla porta seriale della centrale (con le centrali DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange e Honeywell), oppure al **combinatore telefonico di qualsiasi centrale** (TIP/RING) che invii gli eventi in formato Contact ID con toni DTMF. Il comunicatore trasmette alla centrale di vigilanza l'informazione completa dell'evento (codice, area, zona o utente). Con l'app Protegus 2 l'utente comanda il sistema a distanza e riceve notifiche sugli eventi; l'app funziona con tutte le centrali supportate dal comunicatore, indipendentemente dal produttore della centrale. La trasmissione alla centrale di vigilanza e Protegus 2 possono essere usati anche contemporaneamente. Questo manuale riguarda i comunicatori 4G GT e GT+; le differenze tra le due versioni sono riassunte nel paragrafo 1.2.

1.1 A cosa serve e come funziona

- **Trasmette alla centrale di vigilanza.** Invia gli eventi, tramite connessione IP, al ricevitore software o hardware Trikdis (protocollo TRK8) – che collabora con qualsiasi software di vigilanza –, a un ricevitore SIA DC-09 o a un ricevitore SUR-GARD (TL150). Verso un ricevitore SUR-GARD converte in codici SIA i codici Contact ID ricevuti dalla centrale; la tabella di conversione si trova nell'allegato della documentazione in inglese del produttore. Verifica la connessione con il ricevitore ogni 30 secondi (o all'intervallo impostato) con un messaggio PING; se il canale principale si interrompe, passa al canale di riserva. Con il canale parallelo gli eventi vanno contemporaneamente anche a due ricevitori. Se è attivo anche il servizio Protegus, l'evento viene ricevuto prima dalla centrale di vigilanza e solo dopo dall'app degli utenti.
- **Avvisa l'utente.** L'app Protegus 2 segnala gli eventi con notifiche push e con un segnale acustico dedicato; dall'app l'utente può inserire e disinserire e comandare i dispositivi collegati (illuminazione, cancello, ventilazione, riscaldamento, irrigazione ecc.). Nell'app i diritti dell'amministratore, dell'installatore e dell'utente sono diversi. Oltre a Protegus 2, le notifiche possono essere richieste anche via SMS e con chiamata telefonica.
- **Comanda direttamente la centrale.** Se collegato al bus dati o alla porta seriale, il comunicatore vede anche lo stato delle aree e delle zone della centrale, e l'utente inserisce e disinserisce da Protegus 2 con il proprio codice della tastiera – per questo non serve una zona chiave. Il GT+ può essere collegato alle centrali DSC contemporaneamente al bus dati (Keybus) e ai morsetti TIP/RING: il bus serve al comando e agli stati, mentre gli eventi vengono inviati con i codici Contact ID propri della centrale (paragrafo 3.3.2).
- **Ha ingressi e uscite propri.** Due morsetti I/O a doppia funzione possono essere usati come ingressi (IN) o come uscite comandabili (OUT). Le uscite possono essere comandate dall'app Protegus 2 e con comandi SMS. Con le espansioni iO-8 collegate al bus RS485 si possono aggiungere altri ingressi e uscite.
- **Configurazione.** Le impostazioni possono essere salvate in un file e caricate in altri comunicatori. Ci sono due livelli di accesso: quello dell'amministratore della centrale di vigilanza e quello dell'installatore. Il comunicatore può essere configurato anche a distanza, e anche il suo firmware può essere aggiornato a distanza.

La struttura del sistema è mostrata nella figura seguente: la centrale d'allarme si collega al comunicatore, il comunicatore raggiunge Internet tramite la rete mobile (LTE) e da lì il ricevitore della centrale di vigilanza (e il relativo software) e il server Protegus; l'utente vede il sistema nell'app Protegus 2 e tramite la rete mobile può

ricevere anche SMS e chiamate.

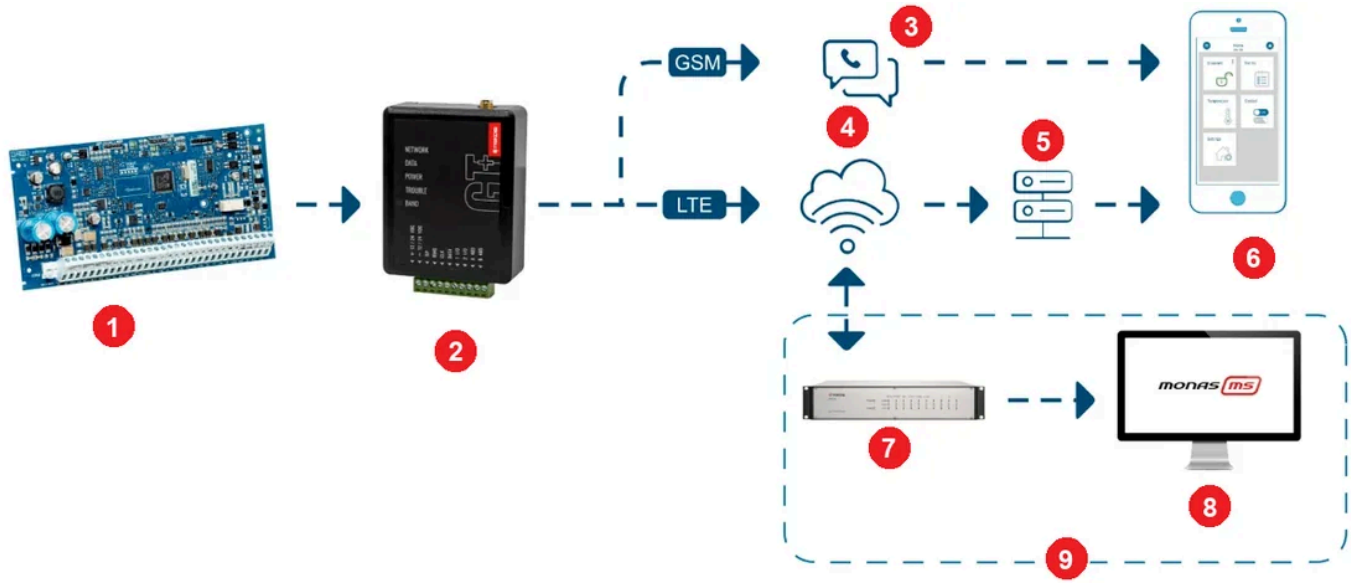


Figura 1. La posizione del comunicatore nel sistema: centrale d'allarme → GT / GT+ → rete mobile → Internet → ricevitore della centrale di vigilanza e server Protegus → app Protegus 2; SMS e chiamate direttamente tramite la rete mobile.

- 1 centrale d'allarme («Alarm panel»)
- 2 comunicatore LTE GT / GT+ («LTE communicator»)
- 3 chiamata e SMS («Call/SMS»)
- 4 Internet («Internet»)
- 5 server Protegus («Protegus server»)
- 6 telefono con l'app Protegus («Phone with Protegus software»)
- 7 ricevitore della centrale di vigilanza («Receiver»)
- 8 software di vigilanza («Monitoring software»)
- 9 la centrale di vigilanza dell'azienda di sicurezza («Monitoring station in security company») – nel riquadro tratteggiato

1.2 Versioni: GT e GT+

GT e GT+ sono lo stesso dispositivo in due versioni: collegamento, configurazione e funzionamento sono quasi identici, perciò li descriviamo in un unico manuale. Le differenze sono riassunte nella tabella seguente; dove il testo indica il dato del GT+, per il GT tieni conto di questa tabella.

	GT	**GT+**
Tensione di alimentazione	10–18 V DC	10–32 V DC
Sigla dei morsetti di alimentazione	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Collegamento di una centrale DSC	solo al bus dati (Keybus)	al bus dati, oppure al bus dati e ai morsetti TIP/RING insieme – così gli eventi vengono inviati con i codici Contact ID propri della centrale (ad es. incendio: E110) e non come allarme generico (E130)
Impostazione del collegamento alla linea telefonica (TIP/RING) in TrikdisConfig (**Panel settings → Communication protocol**)	**2. Dual tone**	**2. AUTO** (nell'elenco si può scegliere anche **3. MANUAL**)
Verifica con DSC collegata a bus + TIP/RING (capitolo 8)	–	l'allarme della zona incendio deve arrivare come E110

	GT	GT+
Tutto il resto: ingressi/uscite, bus RS485, modem, LED, dimensioni, protocolli, Protegus 2, comandi SMS	identico	identico

Entrambe le versioni sono prodotte con tre tipi di modem; per l'Europa è indicata la versione europea (EU). Il tipo di modem e la versione hardware si trovano nella barra di stato di TrikdisConfig (**Device**, **HW**) e sull'etichetta del dispositivo.

Modem	Rete e bande di frequenza
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (America Latina)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Centrali d'allarme compatibili

Le centrali seguenti possono essere collegate al comunicatore direttamente, tramite bus dati o porta seriale. La colonna «controllo diretto» indica se l'utente può inserire e disinserire da Protegus 2 con il proprio codice della tastiera senza altri collegamenti; dove ciò non è possibile, il comunicatore legge gli eventi dal bus, mentre per il comando serve una zona chiave (paragrafo 3.4).

Produttore	Modello	Collegamento	Controllo diretto
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	bus dati (Keybus); GT+: anche Keybus + TIP/RING	sì
DSC	PC5020	bus dati (Keybus)	no
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	porta seriale (cavo EX-CRP2.4), oppure Keybus + TIP/RING	sì
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	porta seriale (cavo EX-CRP2.4), oppure Keybus + TIP/RING	sì
Paradox	Digiplex EVO192, EVOHD, EVOHD+	porta seriale (cavo EX-CRP2.4)	sì
Paradox	Digiplex EVO48	porta seriale (cavo EX-CRP2.4)	no
Paradox	Spectra 1727, 1728, 1738; Esprit E55	porta seriale (cavo EX-CRP2.4)	no
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	bus dati	sì
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	porta seriale (cavo EX-CRP4)	sì
InnerRange	Inception, Integriti	porta seriale (con il cavo del produttore)	no
Honeywell	Ademco Vista-15, Vista-20, Vista-48	bus dati	sì

- Il firmware delle centrali **Paradox** a controllo diretto deve essere almeno **V.4**. Sulle centrali Paradox più recenti (SP+, MG+, EVOHD+) la porta seriale può essere bloccata di fabbrica; lo sblocco è descritto nel paragrafo 4.1.2. Le centrali Spectra SP / SP+ e Magellan MG / MG+ possono essere collegate, invece che alla porta seriale, anche al bus dati (Keybus) e ai morsetti TIP/RING insieme – per questo non serve lo sblocco a pagamento (paragrafo 3.3.4).
- Le centrali di **tutti gli altri produttori** si collegano tramite il loro combinatore telefonico (TIP/RING), se questo invia gli eventi in formato Contact ID con composizione DTMF; in questo caso per il comando serve una zona chiave.
- Quale comunicatore Trikdis e quale collegamento sono adatti alla tua centrale puoi verificarlo nel motore di ricerca della compatibilità.

1.4 Le parti del comunicatore

Il comunicatore ha il circuito stampato in un contenitore di plastica nero; il coperchio frontale si stacca a scatto e la morsettiera è estraibile. Nella figura seguente è mostrato il GT+; il GT è identico, solo la scritta sul contenitore è GT e la sigla dei morsetti di alimentazione è +12 VDC / −12 VDC.

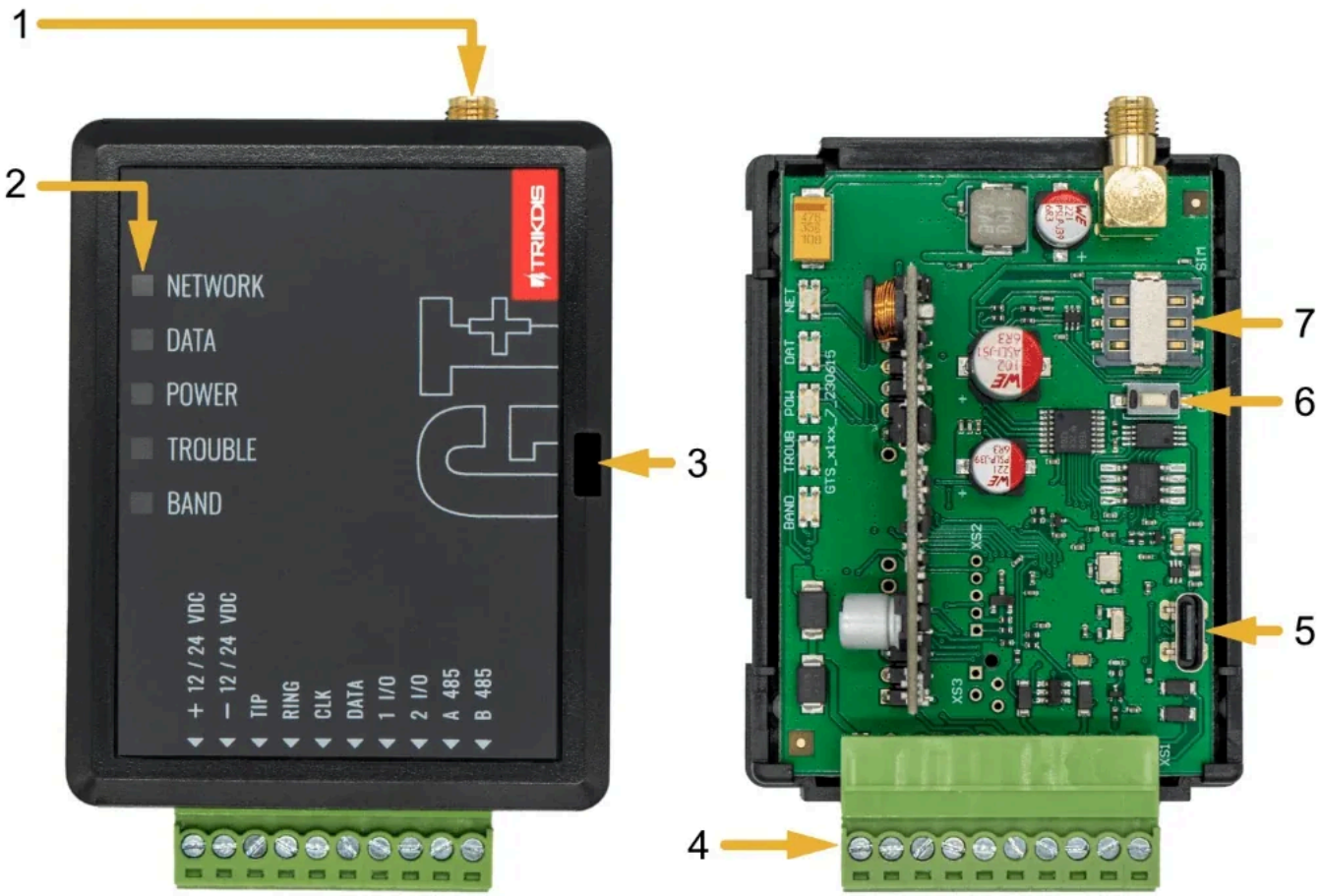


Figura 2. Le parti del comunicatore viste dal davanti (a sinistra) e con il contenitore aperto (a destra).

- 1 Connettore SMA dell'antenna mobile
- 2 Indicatori LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Fessura che aiuta a staccare il coperchio frontale
- 4 Morsettiera estraibile per i collegamenti esterni
- 5 Presa USB-C per la programmazione
- 6 Pulsante RESET
- 7 Alloggiamento della scheda nano-SIM

La morsettiera è estraibile: così il dispositivo può essere tolto dall'alimentazione o riavviato con un solo gesto, durante il collegamento è più comoda da maneggiare e per la programmazione via USB il dispositivo può essere portato al computer.

1.5 Morsetti

Morsetto (GT)	Morsetto (GT+)	Funzione
+12 VDC	**+12 / 24 VDC**	Alimentazione, positivo: +10–18 V DC (GT), +10–32 V DC (GT+)
–12 VDC	**–12 / 24 VDC**	Alimentazione, 0 V
TIP	**TIP**	Morsetto TIP del combinatore telefonico della centrale d'allarme
RING	**RING**	Morsetto RING del combinatore telefonico della centrale d'allarme
CLK	**CLK**	Bus seriale o bus dati (clock) per il collegamento diretto della centrale
DATA	**DATA**	Bus seriale o bus dati (dati) per il collegamento diretto della centrale
1 I/O	**1 I/O**	Ingresso/uscita 1 (impostazione di fabbrica: ingresso, NO)
2 I/O	**2 I/O**	Ingresso/uscita 2 (impostazione di fabbrica: ingresso, NO)
A 485	**A 485**	Filo A del bus RS485
B 485	**B 485**	Filo B del bus RS485

Negli schemi di collegamento i morsetti di alimentazione sono indicati in modo uniforme come **+DC** e **–DC** (sul GT è il morsetto +12 VDC / −12 VDC, sul GT+ il morsetto +12 / 24 VDC / −12 / 24 VDC), mentre i morsetti RS485 come **A RS485** / **B RS485** (sul dispositivo A 485 / B 485). Le sigle della morsettiera sono riportate anche sul coperchio frontale.

1.6 Segnalazioni LED

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

NETWORK – connessione di rete

Segnalazione	Significato
spento	Nessuna connessione con la rete mobile
lampeggia in giallo	Connessione alla rete mobile in corso
verde fisso, lampeggia in giallo	Connesso alla rete mobile; il numero di lampeggi gialli è il **livello del segnale**: su 4G 3 lampeggi indicano un segnale adeguato

DATA – traffico dati

Segnalazione	Significato
spento	Nessun evento in attesa di invio
verde fisso	Ci sono eventi in memoria in attesa di invio
lampeggia in verde	Trasferimento dati tra il comunicatore e il computer (durante la programmazione)

Verifica rapida

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 adeguata
giallo fisso	Tensione di alimentazione non adeguata (al massimo 11,5 V)
verde fisso, lampeggia in giallo	Pronto per la programmazione (durante la programmazione)
giallo fisso (durante la programmazione)	Nessuna connessione con il computer

TROUBLE – guasto

Segnalazione	Significato
spento	Nessun guasto
1 lampeggio rosso	Nessuna scheda SIM
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)
6 lampeggi rossi	Nessuna connessione con il ricevitore della centrale di vigilanza
7 lampeggi rossi	Interrotta la connessione con la centrale d'allarme
8 lampeggi rossi	L'ICCID impostato non corrisponde all'ICCID della scheda SIM (paragrafo 6.6)
lampeggia in rosso (durante la programmazione)	Errore di memoria
rosso fisso (durante la programmazione)	Firmware danneggiato

BAND – tipo di rete

Lampeggi verdi	Rete
1	nessuna
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)

Lampeggi verdi	Rete
6	4G (LTE TDD, LTE FDD)

1.7 Dati tecnici

Parametro	Valore
Collegamento con la centrale d'allarme	bus seriale, bus dati (Keybus) o linea telefonica (TIP/RING, Contact ID, DTMF)
Ingressi/uscite	2 I/O a doppia funzione: come ingresso NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistenza di fine linea da 2,2 kΩ); come uscita a collettore aperto (OC), max. 0,15 A / 30 V DC. Espandibile con espansioni iO-8
Modem	EG915U-EU (Europa), EG915U-LA (America Latina) o BG95-M5 (LTE Cat M1) – le bande di frequenza sono elencate nella tabella del paragrafo 1.2
Tensione di alimentazione	GT: 10–18 V DC; GT+: 10–32 V DC
Assorbimento di corrente	al massimo 100 mA a riposo; al massimo 200 mA durante l'invio dei dati
Protocolli di trasmissione	TRK8, DC-09_2007, DC-09_2012, TL150
Cifratura	AES-128
Programmazione	TrikdisConfig (Windows) con cavo USB-C o a distanza
Ambiente di funzionamento	−10 … +50 °C, max. 80 % di umidità relativa (a +20 °C)
Dimensioni	92 × 62 × 26 mm
Peso	80 g

2. Messa in servizio rapida con TrikdisConfig

Tutte le impostazioni del comunicatore si fanno con il programma **TrikdisConfig**, che funziona su Windows – con cavo USB-C o a distanza. In questo capitolo descriviamo la strada più breve: configuri il dispositivo sulla scrivania, prima del collegamento, e poi sul posto basta collegarlo. Descriviamo quali impostazioni servono perché il comunicatore invii gli eventi alla centrale di vigilanza e perché il sistema possa essere comandato dall'app Protegus 2; la spiegazione dettagliata delle impostazioni si trova nel capitolo 6.

2.1 Preparativi

Cosa ti servirà

Cavo USB-C per la programmazione · cavo con almeno 4 conduttori tra il comunicatore e la centrale · per la porta seriale Paradox il cavo CRP2.4 · cacciavite piatto da 2,5 mm · antenna mobile con guadagno adeguato, se sul posto la copertura è debole · scheda SIM attiva (la richiesta del PIN può essere disattivata) · il manuale dell'installatore della centrale d'allarme.

Ordina separatamente gli accessori necessari presso il distributore.

1. Scarica e installa il software TrikdisConfig. Sul sito del produttore (www.trikdis.com) scrivi nel campo di ricerca: «TrikdisConfig».

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 contenitore del comunicatore con un cacciavite piatto: inserisci il cacciavite in alto, nella fessura accanto all'antenna, e fai leva verso l'esterno, poi in basso, nella fessura, verso il basso. La figura mostra anche la posizione della presa USB-C sul bordo del circuito stampato.

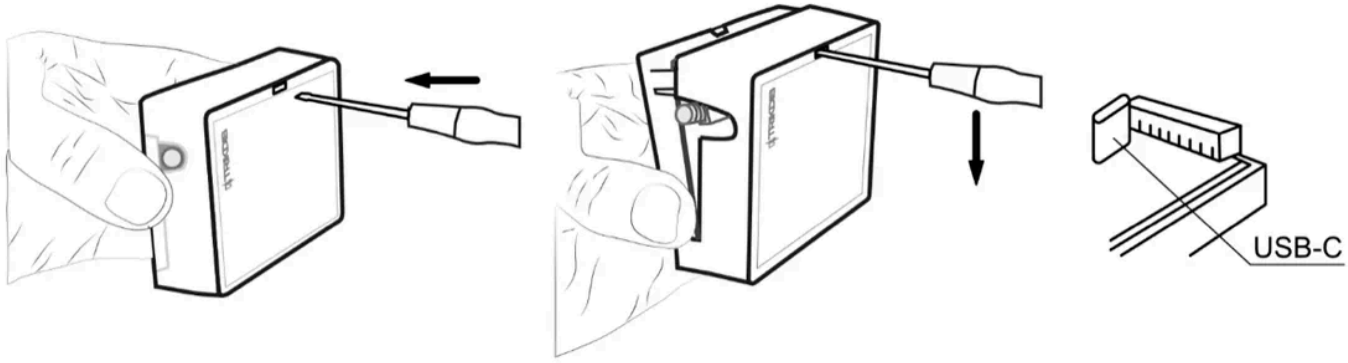


Figura 3. Come staccare il coperchio frontale con un cacciavite piatto; il dettaglio ingrandito mostra la posizione della presa USB-C.

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

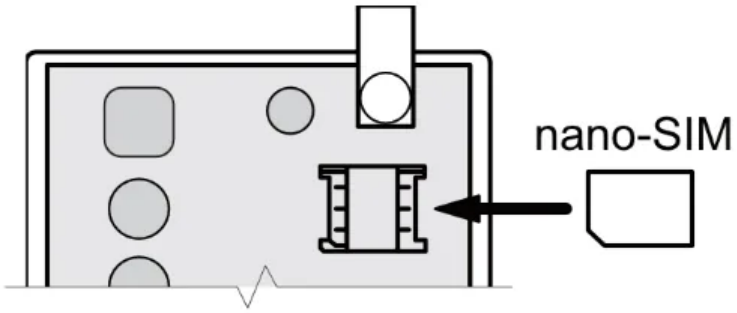


Figura 4. La posizione della scheda nano-SIM sul circuito stampato.

4. Collega il comunicatore al computer con un cavo USB-C.

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 a 6 cifre dell'amministratore (di fabbrica `123456`) o dell'installatore (di fabbrica

`654321`).

2.2 Connessione all'app Protegus 2

Per prima cosa, nella pagina **Panel settings** indica come il comunicatore si collega alla centrale.

Se lo colleghi all'uscita della linea telefonica (TIP/RING) della centrale: nel campo **Communication protocol** scegli il valore **AUTO** (sul GT il secondo elemento dell'elenco è **Dual tone** – lì scegli quello).

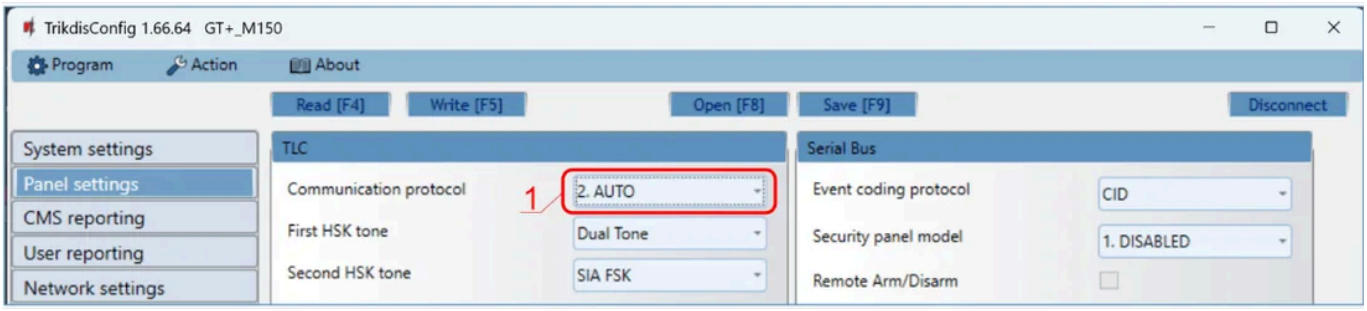


Figura 5. TrikdisConfig – Panel settings, gruppo TLC (nella figura l'impostazione del GT+).

- 1 **Communication protocol** – con collegamento TIP/RING **2. AUTO** (GT: **2. Dual tone**).

Se lo colleghi al bus dati o alla porta seriale della centrale: nel gruppo **Serial bus** imposta la centrale.



Figura 6. TrikdisConfig – Panel settings, gruppo Serial bus.

- 2 **Security panel model** – il modello della centrale collegata.
- 3 **Remote Arm/Disarm** – spunta questa opzione se gli utenti vogliono comandare la centrale da Protegus 2 con il proprio codice della tastiera. Compare solo con le centrali a controllo diretto.
- 4 **Security panel PC download password** – per il controllo diretto delle centrali Paradox e Texecom, la password PC o UDL impostata nella centrale; le due devono coincidere.

GT+, centrale DSC collegata al bus dati e ai morsetti TIP/RING insieme: il **Communication protocol** deve essere **AUTO**, il **Security panel model** il modello DSC, e spunta l'opzione **Remote Arm/Disarm** se la centrale deve essere comandata da Protegus 2 (paragrafo 3.3.2).

Per il controllo diretto bisogna configurare anche la centrale d'allarme – lo descrive il capitolo 4, dove trovi anche la procedura per impostare la password PC o UDL.

Poi, nella pagina **User reporting**, nella scheda **PROTEGUS Cloud**, abilita la connessione al cloud.

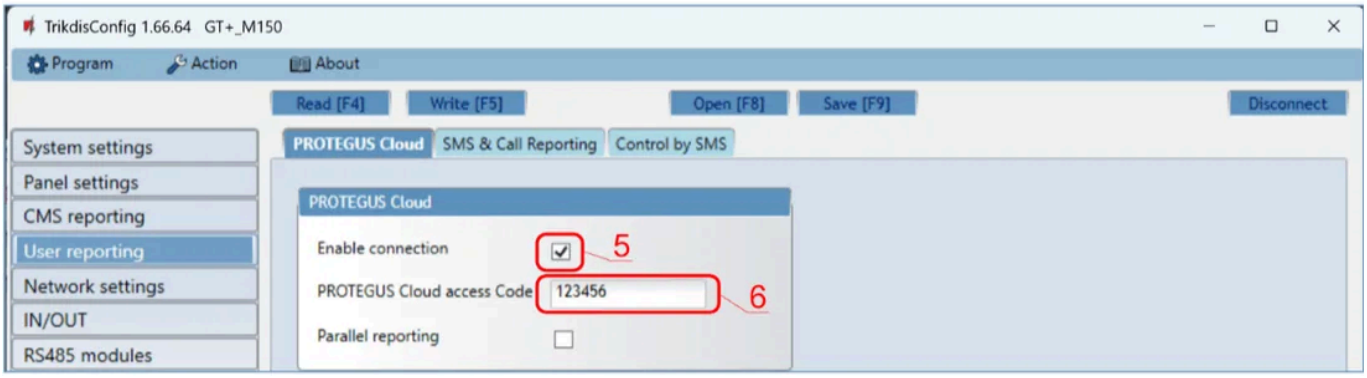


Figura 7. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- 5 **Enable connection** – spunta questa opzione: abilita la connessione con il cloud Protegus.
- 6 **PROTEGUS Cloud access Code** – il codice di accesso per Protegus 2 (di fabbrica `123456`). Cambialo se vuoi che l'utente debba inserirlo quando aggiunge il sistema all'app. Importante: se in seguito modifichi il codice in TrikdisConfig, devi aggiornarlo anche nell'app Protegus 2.

Infine, nella pagina **Network settings**, nella scheda **SIM1**, inserisci i dati della scheda.

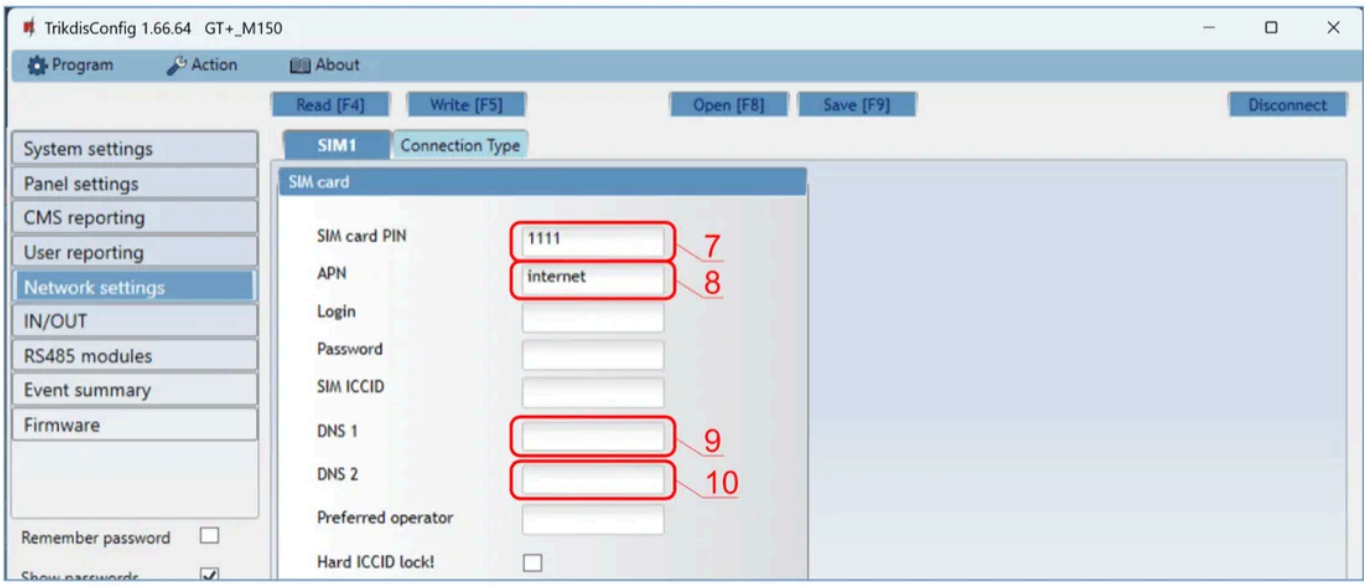


Figura 8. TrikdisConfig – Network settings, scheda SIM1.

- 7 **SIM card PIN** – il codice PIN della scheda (se la richiesta del PIN è disattivata, può restare il valore di fabbrica).
- 8 **APN** – il punto di accesso alla connessione dati dell'operatore (vedi sotto).
- 9 **DNS 1** – server dei nomi primario; di fabbrica è il DNS di Google. Indipendentemente dalle impostazioni IP, verifica che gli indirizzi DNS funzionino con il tuo operatore.
- 10 **DNS 2** – server dei nomi secondario (di fabbrica anch'esso di Google).

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

Per le schede dati IoT / M2M (machine-to-machine) 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 lo trovi 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 alla centrale di vigilanza, la configurazione è finita: premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB.

Con il collegamento alla linea telefonica (TIP/RING) non dimenticare di attivare e configurare il combinatore della centrale d'allarme, altrimenti la centrale non invia eventi; per il controllo diretto bisogna configurare anche le centrali Paradox, Texecom, Caddx, InnerRange e Honeywell. La configurazione della centrale è descritta nel capitolo 4.

2.3 Connessione alla centrale di vigilanza

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

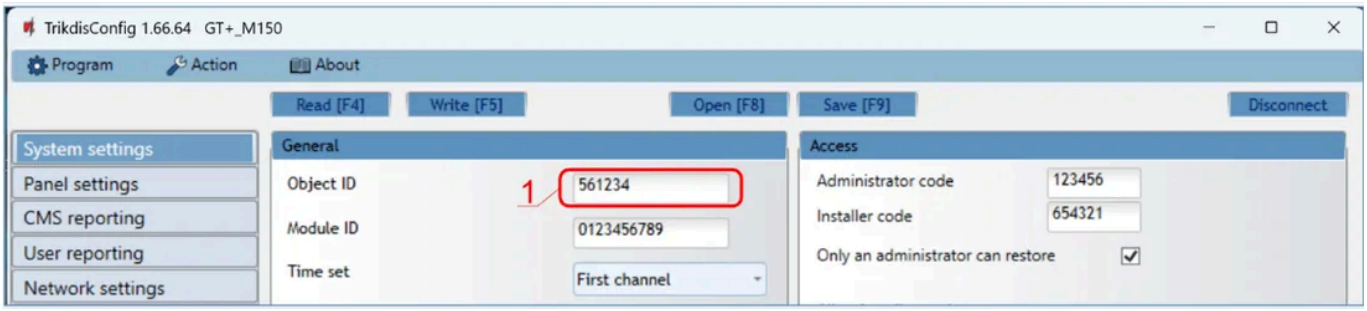


Figura 9. TrikdisConfig – pagina System settings, gruppo General.

- 1 **Object ID** – il codice impianto ricevuto dalla centrale di vigilanza (6 caratteri esadecimali, 0–9, A–F). `FFFE` e `FFFF` non possono essere usati.

Nella pagina **Panel settings** indica il collegamento della centrale, se non l'hai già fatto nel paragrafo 2.2: con collegamento TIP/RING il **Communication protocol** deve essere **AUTO** (GT: **Dual tone**); con collegamento al bus dati o seriale scegli nel campo **Security panel model** il modello della centrale collegata (le figure del paragrafo 2.2).

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

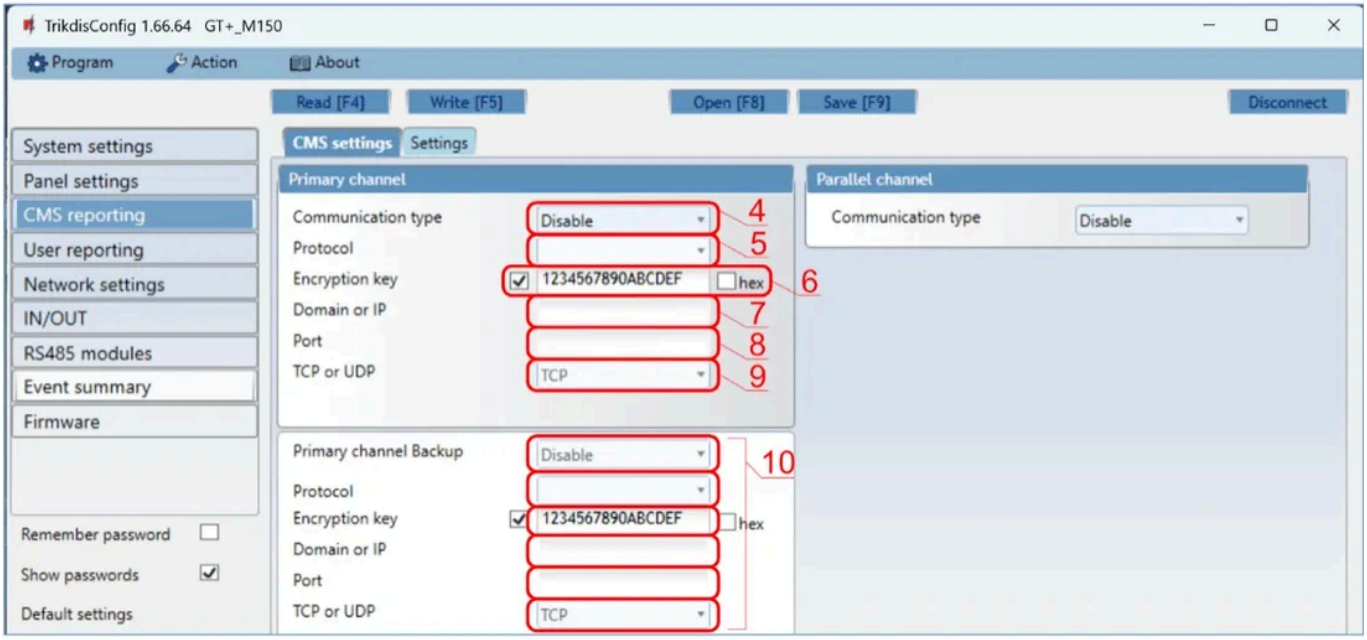


Figura 10. TrikdisConfig – CMS reporting, scheda CMS settings.

- 4 **Communication type** – scegli la connessione **IP**.
- 5 **Protocol** – **TRK8** per un ricevitore Trikdis, **DC-09_2007** o **DC-09_2012** per un ricevitore universale, **TL150** per un ricevitore SUR-GARD.
- 6 **Encryption key** – la chiave di cifratura impostata nel ricevitore.
- 7 **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- 8 **Port** – il numero di porta del ricevitore.
- 9 **TCP or UDP** – il protocollo di trasmissione; si adegua all'impostazione del ricevitore.
- 10 **Primary channel Backup** – canale di riserva in caso di guasto del canale principale; compilalo allo stesso modo, è consigliabile indicarlo.

Infine, nella pagina **Network settings**, nella scheda **SIM1**, inserisci i dati della scheda (**SIM card PIN**, **APN**, **DNS 1, DNS 2**), se non l'hai già fatto nel paragrafo 2.2.

Con il protocollo **DC-09** nella scheda **Settings** inserisci anche il numero di linea e di ricevitore (**Line No.**, **Receiver No.**, paragrafo 6.4). GT e GT+ trasmettono alla centrale di vigilanza solo tramite connessione IP, non hanno un canale di riserva via SMS.

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. Con il collegamento alla linea telefonica anche in questo caso bisogna attivare e configurare il combinatore della centrale d'allarme, 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 paragrafo 2.1) ed estrai la morsettiera.
2. Inserisci la scheda nano-SIM nell'alloggiamento, se non l'hai già fatto durante la messa in servizio.

3. Estrai il circuito stampato dalla base: apri il fermo accanto al connettore dell'antenna e solleva la scheda (vedi la figura).
4. Fissa la base con le viti nel punto scelto (nella figura i fori per le viti sono cerchiati).
5. Rimetti il circuito stampato nella base e reinserisci la morsettiera.
6. Avvita l'antenna mobile.
7. Rimetti il coperchio frontale.

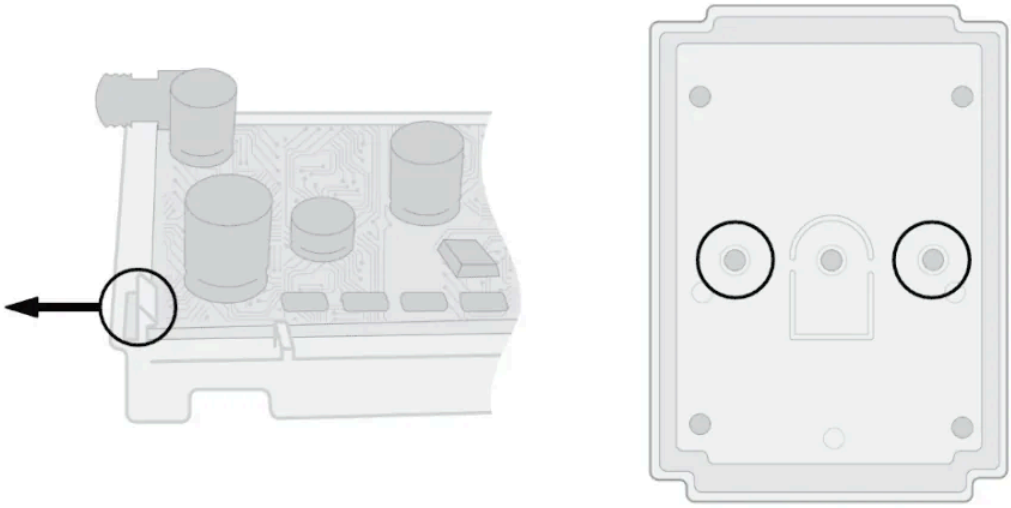


Figura 11. Estrazione del circuito stampato dalla base (a sinistra: il fermo e la direzione di estrazione) e i fori per le viti della base (a destra).

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, inserisci la scheda in un telefono cellulare e disattiva lì la richiesta del PIN.

3.2 Posizionamento e antenna

- Installa il comunicatore in un luogo **asciutto, al chiuso**, possibilmente vicino al contenitore della centrale d'allarme, perché il cablaggio sia corto.
- In un **contenitore metallico** il segnale mobile si attenua molto. Se il comunicatore va nel contenitore metallico della centrale, porta l'antenna fuori dal contenitore oppure usa un'antenna con cavo più lungo.
- Prima del fissaggio definitivo **verifica il livello del segnale**: il numero di lampeggi gialli del LED NETWORK su 4G deve essere almeno 3 (paragrafo 1.6). Se sono meno, cerca un posto migliore oppure passa a un'antenna più sensibile, posizionabile 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

Segui lo schema adatto alla tua centrale tra quelli seguenti. Negli schemi **+DC** e **–DC** sono i morsetti di alimentazione del comunicatore (GT: +12 VDC / −12 VDC, GT+: +12 / 24 VDC / −12 / 24 VDC), mentre **A RS485** / **B RS485** sono i morsetti A 485 / B 485. Il comunicatore riceve l'alimentazione dall'uscita di alimentazione ausiliaria (AUX) della centrale, così in caso di mancanza di rete la batteria della centrale alimenta anche il comunicatore. Negli schemi è rappresentato il GT+; il collegamento del GT è lo stesso.

3.3.1 DSC – bus dati (Keybus)

Collega il Keybus della centrale DSC al comunicatore con quattro fili: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

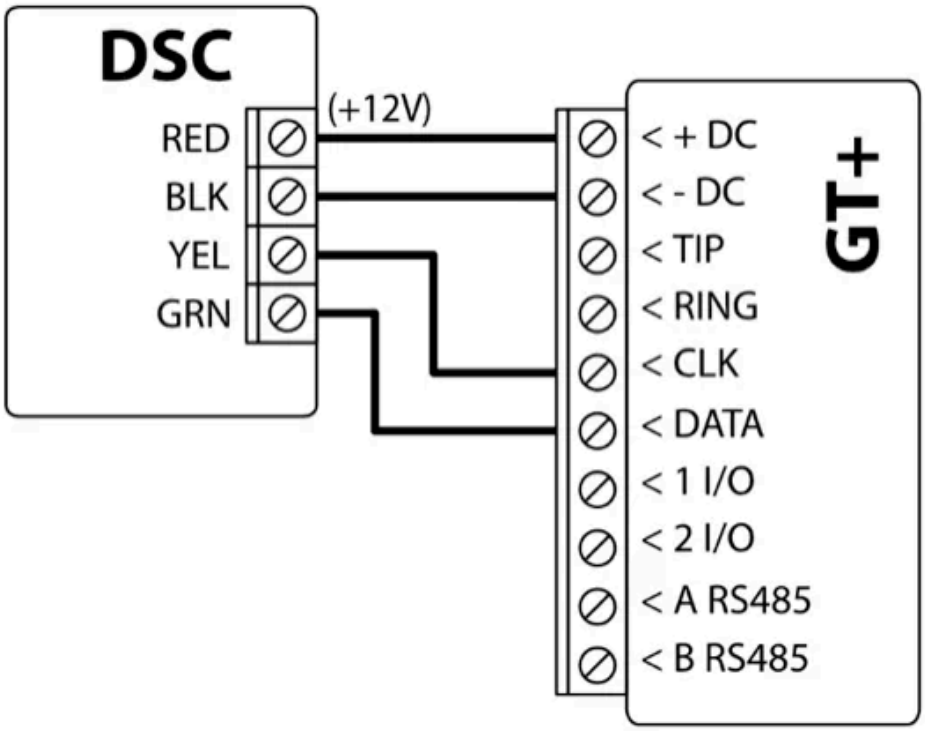


Figura 12. Collegamento di una centrale DSC al bus dati (Keybus, «Keypad bus»): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Se collegato solo al Keybus, il comunicatore riceve dalla centrale lo stato generico delle zone, ma non conosce il tipo di zona (incendio, intrusione, perdita d'acqua ecc.). Per questo trasmette ogni allarme **come allarme generico, con il codice Contact ID E130**, e alcune centrali di vigilanza lo gestiscono in modo diverso dal tipo di zona effettivamente attivato. Se vuoi inviare gli eventi con i codici Contact ID propri della centrale (ad esempio allarme incendio: E110), con il GT+ collega anche i morsetti TIP/RING (paragrafo 3.3.2).

3.3.2 DSC – Keybus e TIP/RING (solo GT+)

Il GT+ può essere collegato alla centrale DSC contemporaneamente al bus dati e all'uscita della linea telefonica: oltre ai fili del Keybus collega anche i morsetti **TIP** → **TIP** e **RING** → **RING** della centrale con quelli del comunicatore.

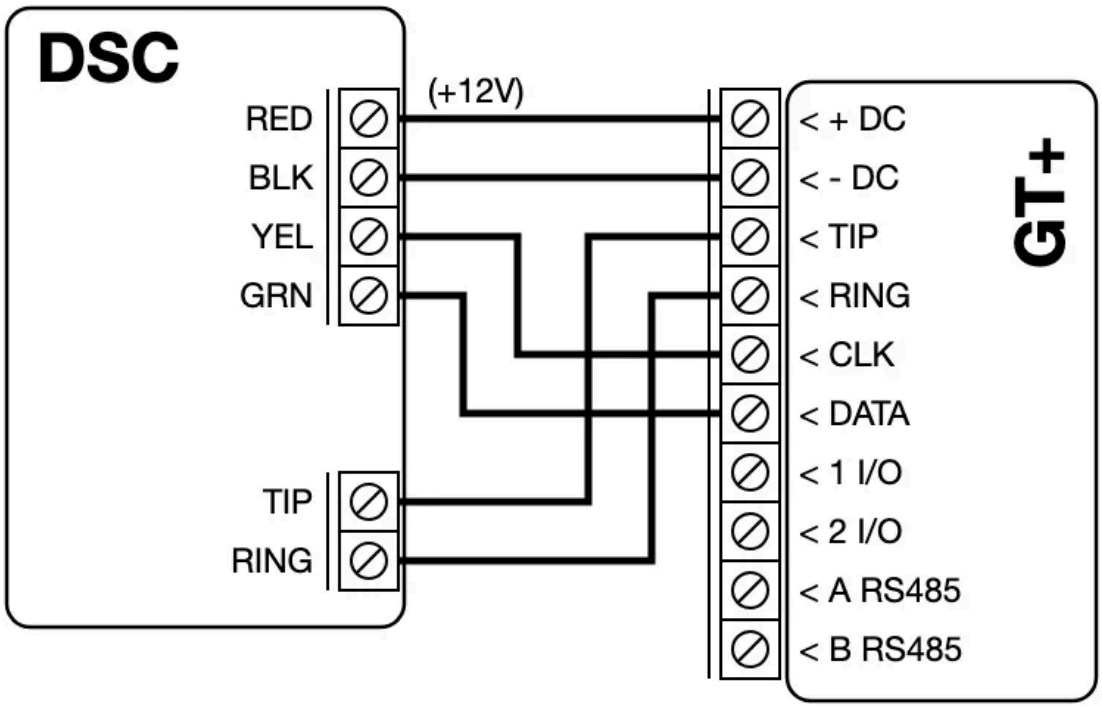


Figura 13. Collegamento di una centrale DSC al bus dati («Keypad bus») e ai morsetti TIP/RING insieme (GT+): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA, inoltre TIP → TIP, RING → RING.

In questo caso il Keybus serve al comando e agli stati (inserimento e disinserimento a distanza, stato delle aree e delle zone), mentre gli eventi vengono inviati dal combinatore telefonico della centrale sui morsetti TIP/RING, quindi con i codici Contact ID propri della centrale. Finché il collegamento TIP/RING funziona, il comunicatore non invia una seconda volta gli eventi provenienti dal Keybus.

Per questo collegamento imposta quanto segue nella pagina **Panel settings** di TrikdisConfig:

1. **Communication protocol**: **AUTO**.
2. **Security panel model**: il modello della centrale DSC.
3. **Remote Arm/Disarm**: spunta questa opzione se gli utenti vogliono comandare la centrale dall'app Protegus 2.

Bisogna programmare anche il combinatore telefonico della centrale DSC, perché invii gli eventi – lo descrive il paragrafo 4.1.1.

3.3.3 Paradox – porta seriale

Il comunicatore si collega alla porta seriale della centrale Paradox con il cavo **EX-CRP2.4**, da ordinare separatamente: **rosso** → **+DC**, **nero** → **−DC**, **giallo** → **CLK**, **verde** → **DATA**.

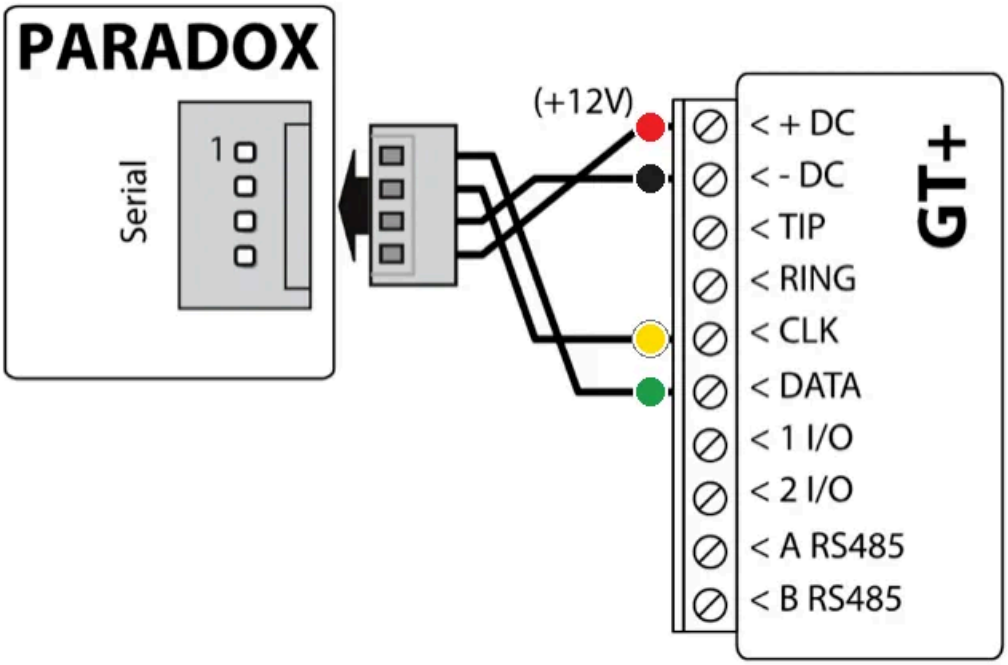


Figura 14. Collegamento di una centrale Paradox alla porta seriale con il cavo EX-CRP2.4 (da ordinare separatamente; «Use the EX-CRP2.4 cable (ordered separately)»): rosso → +DC, nero → −DC, giallo → CLK, verde → DATA.

- filo rosso («R - red»)
- filo nero («B - black»)
- filo giallo («Y - yellow»)
- filo verde («G - green»)

Sulle centrali Paradox più recenti (SP+, MG+, EVOHD+) la porta seriale può essere bloccata di fabbrica; lo sblocco è descritto nel paragrafo 4.1.2. Con le centrali Spectra SP / SP+ e Magellan MG / MG+ si può usare, invece della porta seriale, anche il collegamento descritto nel paragrafo seguente.

3.3.4 Paradox SP/MG – Keybus e TIP/RING

Le centrali Paradox Spectra SP, SP+ e Magellan MG, MG+ possono essere collegate, invece che alla porta seriale, al loro bus dati (Keybus) e ai loro morsetti TIP/RING insieme: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK**, inoltre **TIP** → **TIP**, **RING** → **RING**. Questo collegamento usa il Keybus della centrale al posto della porta seriale, quindi non richiede lo sblocco a pagamento della porta seriale Paradox.

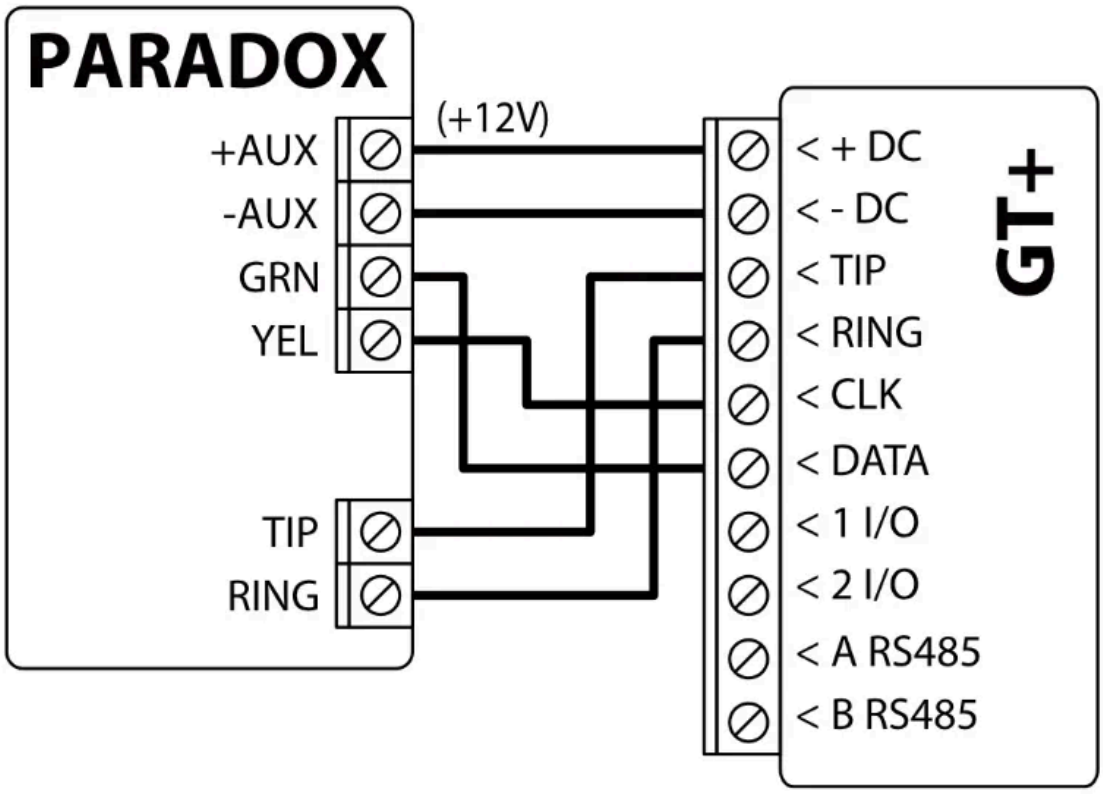


Figura 15. Collegamento di una centrale Paradox SP / SP+ / MG / MG+ al Keybus (bus dati, «Keypad bus») e ai morsetti TIP/RING insieme: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Per questo collegamento il firmware del comunicatore deve essere almeno **1.21** (l'aggiornamento è descritto nel capitolo 9).

Per questo collegamento imposta quanto segue nella pagina **Panel settings** di TrikdisConfig:

1. **Communication protocol**: **AUTO** (GT: **Dual tone**).
2. **Security panel model**: **7. Paradox SP+/MG+ series KeyBus**.
3. **Remote Arm/Disarm**: spunta questa opzione se gli utenti vogliono comandare la centrale dall'app Protegus 2 con il proprio codice della tastiera.
4. **Security panel PC download password**: per il controllo diretto inserisci la password PC impostata nella centrale; le due devono coincidere.



Figura 16. TrikdisConfig – Panel settings per il collegamento Keybus + TIP/RING: Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm spuntato, PC download password inserita.

Bisogna programmare anche la centrale Paradox, perché invii gli eventi alla centrale di vigilanza e possa essere comandata da Protegus 2 – lo descrive il paragrafo 4.1.2.

3.3.5 UTC Interlogix (Caddx) – bus dati

Collega il bus dati della centrale Caddx NetworX al comunicatore con tre fili: **POS** → **+DC**, **COM** → **–DC**, **DATA** → **DATA**. I morsetti TIP, RING e CLK non servono.

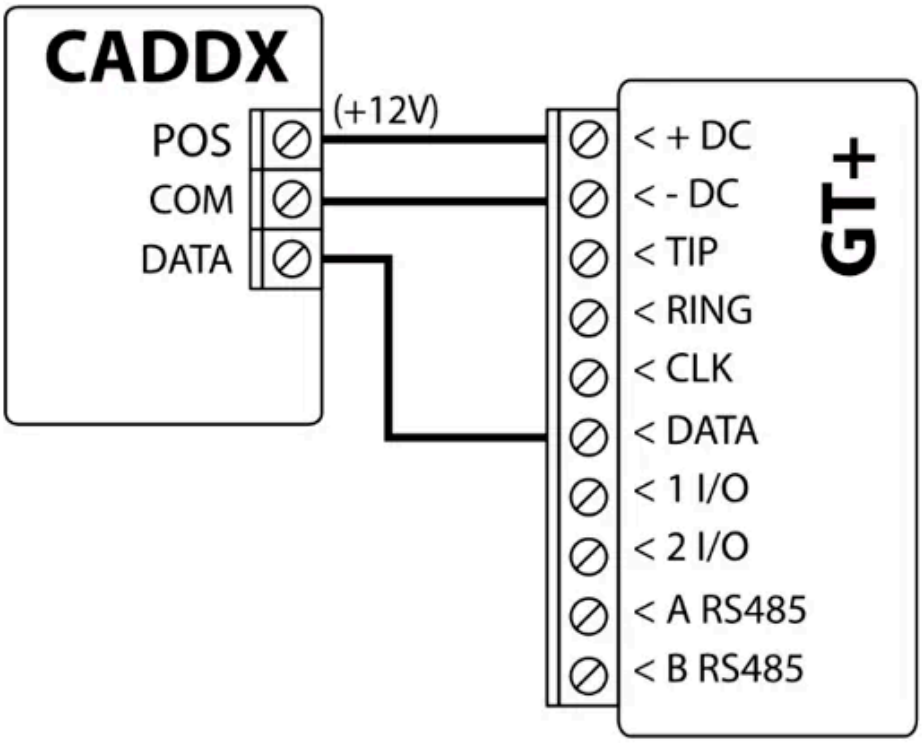


Figura 17. Collegamento di una centrale UTC Interlogix (Caddx) NetworX al bus dati («Keypad bus»): POS → +DC, COM → –DC, DATA → DATA.

3.3.6 Texecom – porta seriale

Il comunicatore si collega alla porta seriale della centrale Texecom Premier / Premier Elite con il cavo **EX-CRP4**, da ordinare separatamente: **rosso** → **+DC**, **nero** → **–DC**, **blu** → **CLK**, **bianco** → **DATA**.

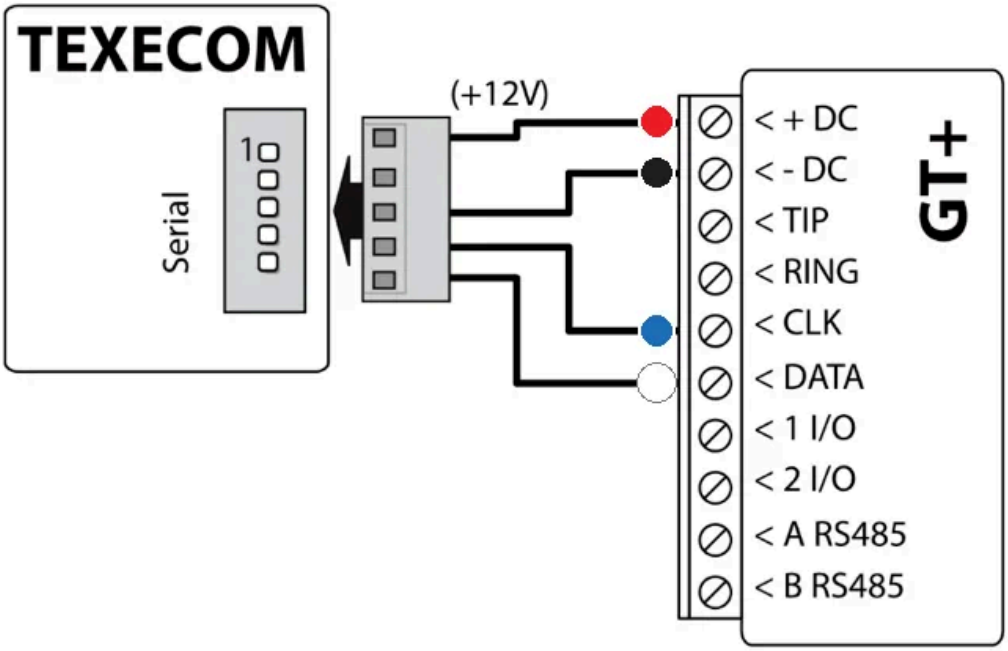


Figura 18. Collegamento di una centrale Texecom alla porta seriale con il cavo EX-CRP4 (da ordinare separatamente; «Use the EX-CRP4 cable (ordered separately)»): rosso → +DC, nero → −DC, blu → CLK, bianco → DATA.

- filo rosso («R - red»)
- filo nero («B - black»)
- filo blu («BL - blue»)
- filo bianco («W - white»)

3.3.7 InnerRange Inception

Il comunicatore riceve l'alimentazione dall'uscita di alimentazione della centrale Inception (**VOUT +** → **+DC**, **VOUT 0V** → **−DC**), mentre la connessione dati arriva dalla porta USB della centrale, con il cavo Inner Range **993030USB**: **nero** → **0V / −DC**, **verde** → **CLK**, **bianco** → **DATA**.

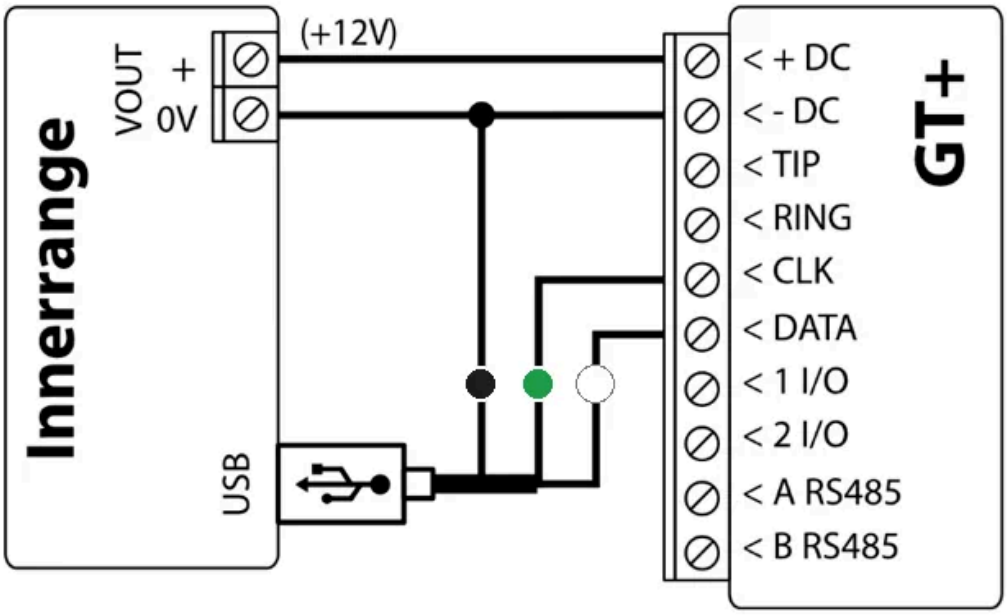


Figura 19. Collegamento di una InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; dalla porta USB con il cavo 993030USB («Cable, Inner Range part number 993030USB») nero → −DC, verde → CLK, bianco → DATA.

- filo nero («Black wire»)
- filo verde («Green wire»)
- filo bianco («White wire»)

3.3.8 InnerRange Integriti

Il comunicatore si collega alla porta seriale **Port 0** della centrale Integriti con il cavo Inner Range **INTG-996795**: **+DET (+13 V) → +DC**, **GND (5) → −DC**, **Rx (3) → CLK**, **Tx (2) → DATA**.

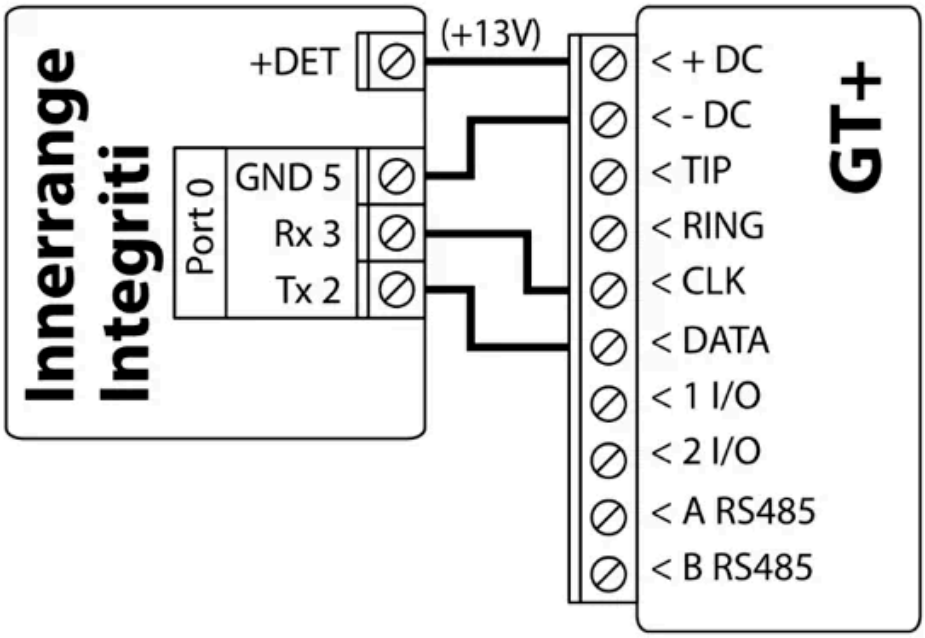


Figura 20. Collegamento di una InnerRange Integriti alla Port 0 con il cavo INTG-996795 («Cable, Inner Range part number INTG-996795»): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – bus dati

Collega il bus tastiere della centrale Honeywell Ademco Vista-15, Vista-20 e Vista-48 dai morsetti della centrale al comunicatore: **5** → **+DC** (+12 V), **4** → **–DC**, **7** → **CLK**, **6** → **DATA**.

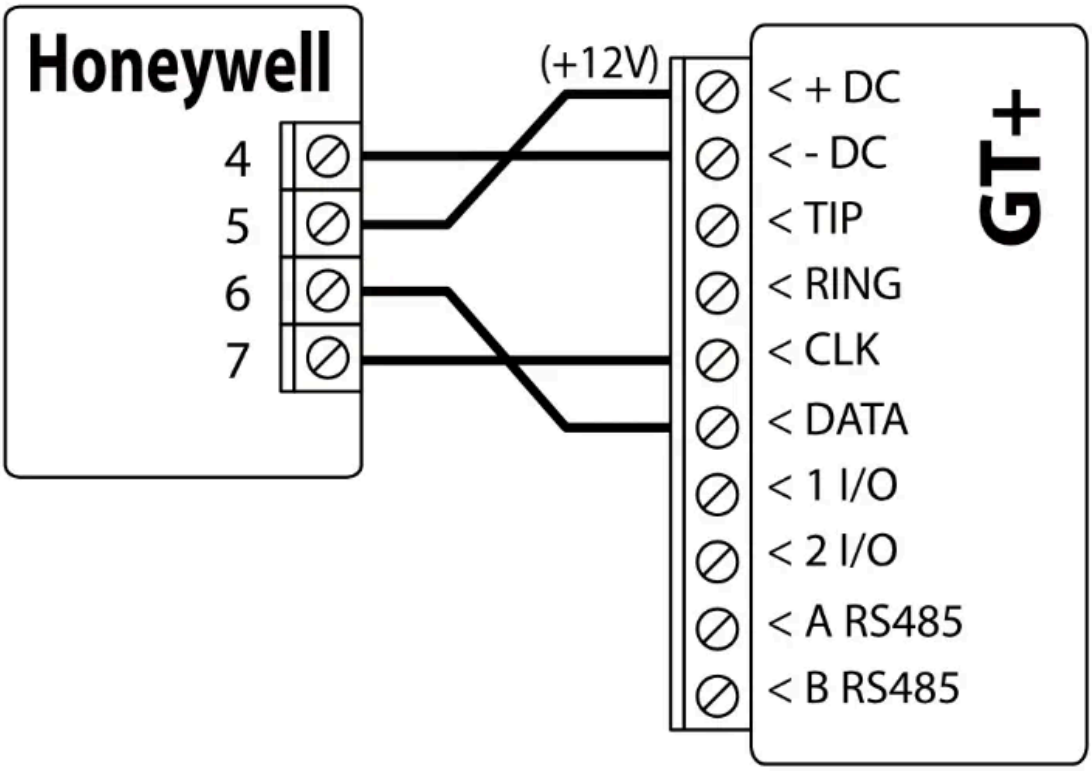


Figura 21. Collegamento di una centrale Honeywell Vista-15 / -20 / -48 al bus dati («Keypad bus»): morsetto 5 → +DC, 4 → –DC, 7 → CLK, 6 → DATA.

3.3.10 Qualsiasi centrale – TIP/RING

Qualsiasi altra centrale può essere collegata tramite il suo combinatore telefonico: l'alimentazione dall'uscita di alimentazione ausiliaria della centrale (**+AUX** → **+DC**, **–AUX** → **–DC**), l'uscita della linea telefonica ai morsetti **TIP** e **RING** del comunicatore (**TIP** → **TIP**, **RING** → **RING**). Il combinatore della centrale deve essere configurato (paragrafo 4.2).

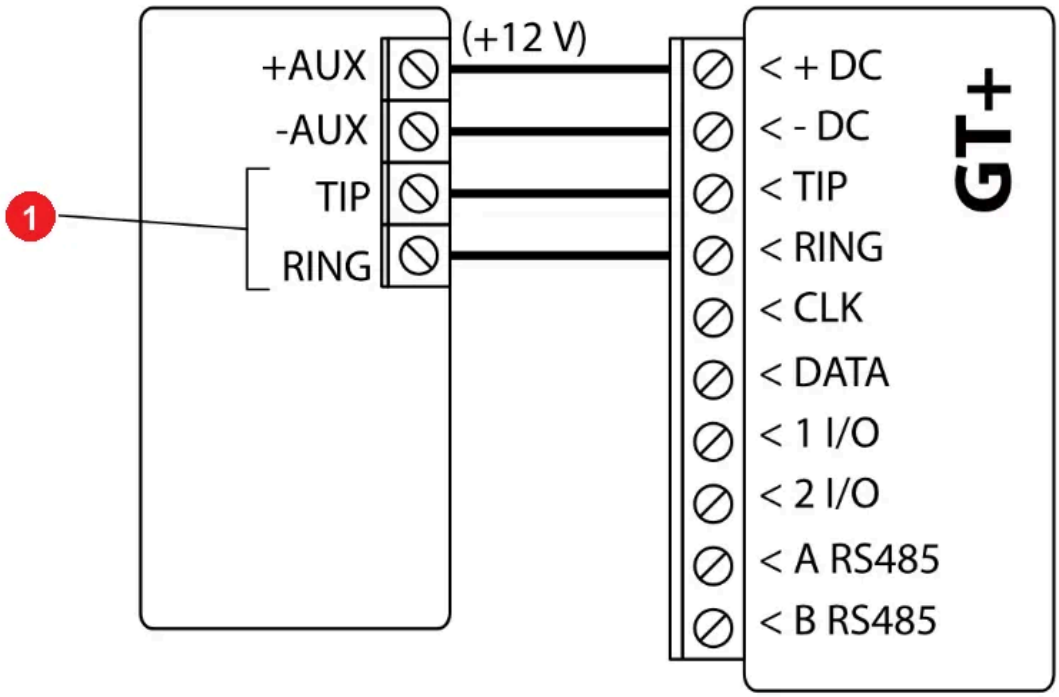


Figura 22. Collegamento al combinatore telefonico della centrale («Control panel»): +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

- 1 i morsetti del combinatore telefonico della centrale («Telephone line communicator terminals»)

3.4 Collegamento della zona chiave

Segui questo collegamento se vuoi inserire e disinserire la centrale dall'app Protegus 2 in modo che l'uscita del comunicatore (PGM) attivi la **zona chiave** della centrale. I due morsetti I/O a doppia funzione del comunicatore possono essere impostati come uscite (OUT, PGM), così le due uscite possono comandare due aree del sistema: collega la zona chiave dell'area 1 al morsetto **1 I/O**, quella dell'area 2 al morsetto **2 I/O**. Con questo collegamento, nella pagina **Panel settings** di TrikdisConfig togli la spunta da **Remote Arm/Disarm**, nella pagina **IN/OUT** imposta i morsetti sulla funzione **OUT** (paragrafo 6.7) e nell'app Protegus 2 assegna le uscite alle aree come descritto nel paragrafo 5.2.

Con il collegamento al bus dati o seriale la connessione dati tra la centrale e il comunicatore resta (il comunicatore legge gli eventi dal bus), mentre l'inserimento e il disinserimento avvengono tramite la zona chiave:

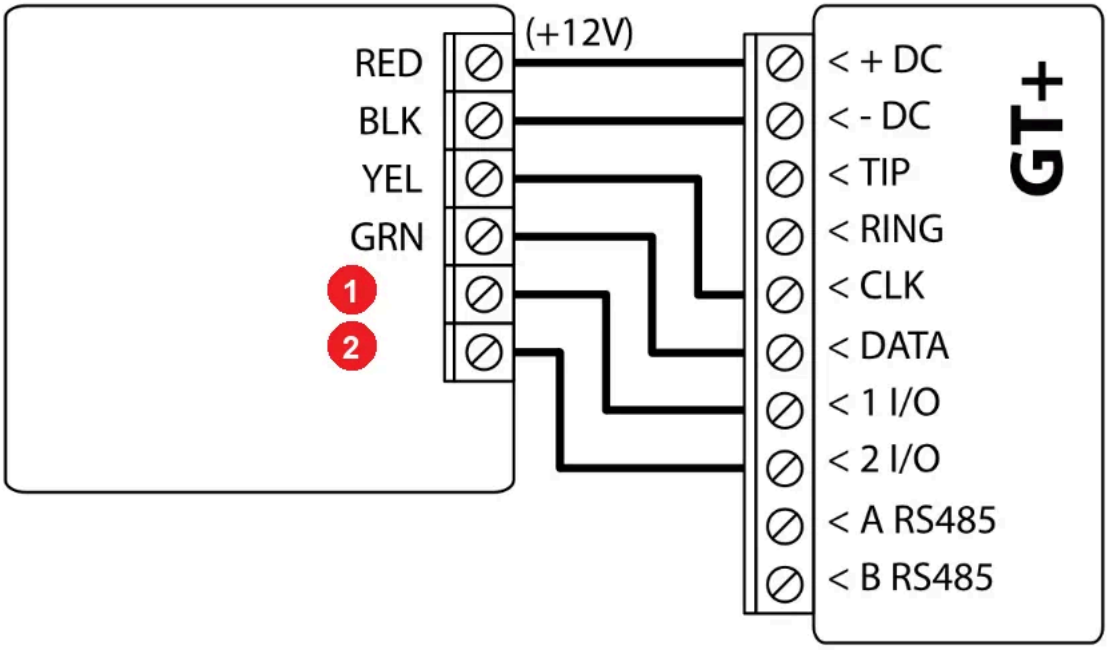


Figura 23. Inserimento e disinserimento con zona chiave («Zones (keyswitch)»), con collegamento al bus dati o seriale («Keypad bus or serial»): morsetto RED della centrale d'allarme («Control panel terminals») → +DC, BLK → −DC, YEL → CLK, GRN → DATA; la zona dell'area 1 → 1 I/O, quella dell'area 2 → 2 I/O.

- 1 la zona chiave dell'area 1 («1-st Area»)
- 2 la zona chiave dell'area 2 («2-nd Area»)

Con il collegamento alla linea telefonica (TIP/RING) la centrale invia gli eventi tramite il suo combinatore, mentre l'inserimento e il disinserimento avvengono allo stesso modo tramite la zona chiave:

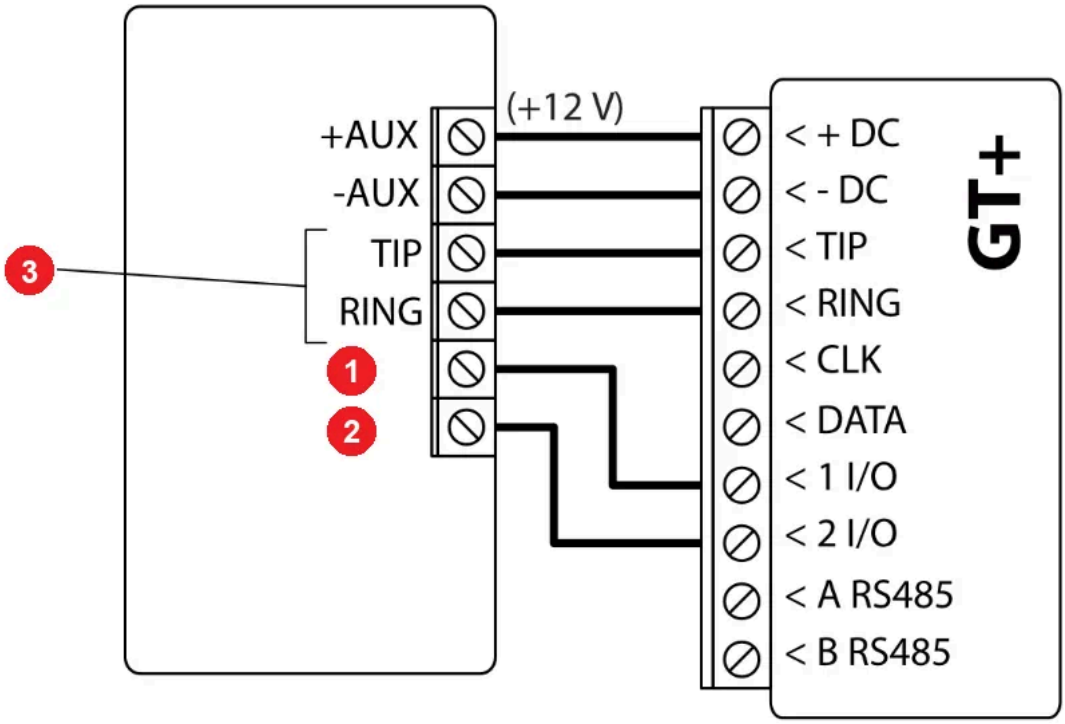


Figura 24. Inserimento e disinserimento con zona chiave («Zone (keyswitch)»), con collegamento alla linea telefonica: morsetto +AUX della centrale d'allarme («Control panel») → +DC, −AUX → −DC, TIP → TIP, RING → RING; la zona dell'area 1 → 1 I/O, quella dell'area 2 → 2 I/O.

- 1 la zona chiave dell'area 1 («1-st Area»)
- 2 la zona chiave dell'area 2 («2-nd Area»)
- 3 i morsetti del combinatore telefonico della centrale («Telephone line communicator terminals»)

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

3.5 Collegamento degli ingressi

I due morsetti I/O a doppia funzione del comunicatore possono essere usati come ingressi (IN) anche per ricevere altri sensori (ad es. interruttore antimanomissione, pulsante antipanico), indipendentemente dalla centrale d'allarme. All'ingresso si può collegare un circuito NO, NC, NO/EOL, NC/EOL, NO/DEOL o NC/DEOL; l'impostazione di fabbrica per entrambi i morsetti è ingresso, NO. Il tipo di ingresso si imposta nella pagina **IN/OUT** di TrikdisConfig, nel campo **Type**. L'ingresso va collegato tra l'I/O scelto e il morsetto **−DC** (COM), secondo il tipo scelto.

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	–

Tipo	Stato di riposo	Allarme	Sabotaggio
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 tra il punto COM e INx: NO, NC, NC/EOL, NO/EOL, inoltre con rilevamento della manomissione NO/DEOL e NC/DEOL, con resistenze di fine linea da 2,2 kΩ; i singoli stati (cortocircuito, interruzione, 2,2 kΩ, 3,3–5,5 kΩ) sono spiegati nella tabella del paragrafo 3.5.

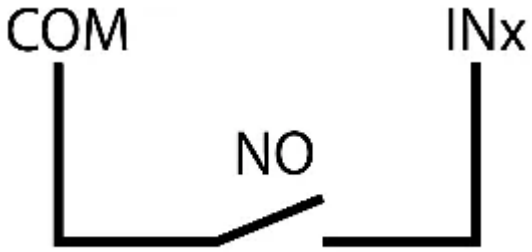


Figura 25. NO – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

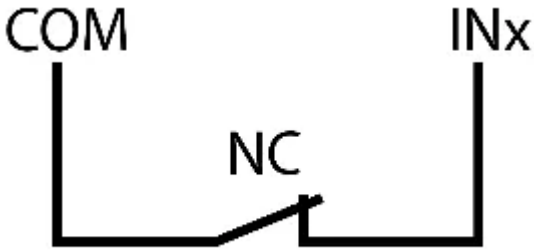


Figura 26. NC – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

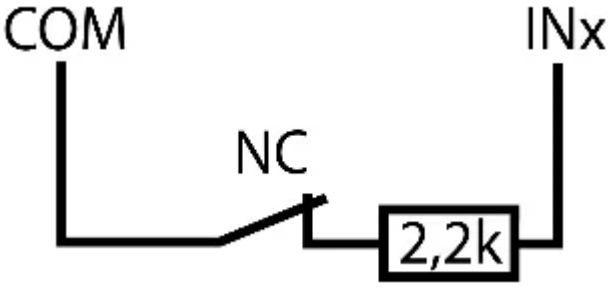


Figura 27. NC/EOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

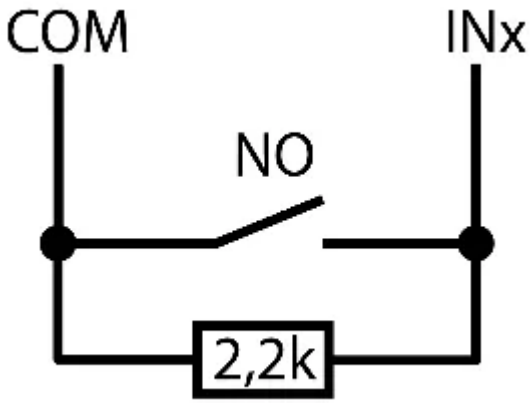


Figura 28. NO/EOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

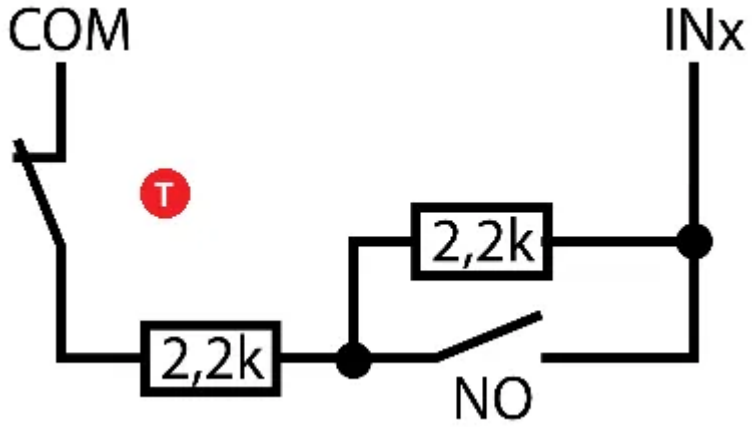


Figura 29. NO/DEOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

- T contatto antimanomissione («Tamper»), segnala l'apertura dell'involucro del sensore

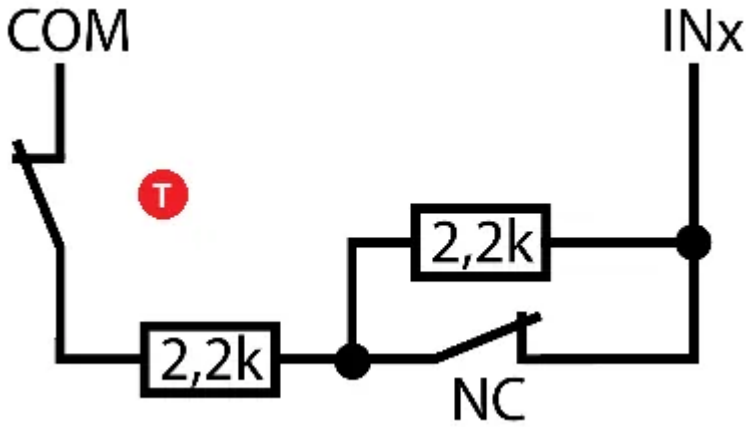


Figura 30. NC/DEOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

- T contatto antimanomissione («Tamper»), segnala l'apertura dell'involucro del sensore

Se servono più ingressi o uscite, collega al comunicatore un'espansione Trikdis **iO-8** (paragrafo 3.7); il suo collegamento è descritto anche nel manuale dell'iO-8.

3.6 Collegamento di un'uscita con relè

Come uscite, i morsetti I/O sono uscite a collettore aperto (OC): nello stato attivo portano al negativo il carico collegato, con al massimo 0,15 A, fino a 30 V DC. Con i contatti di un relè puoi accendere e spegnere diversi apparecchi elettrici: un'estremità della bobina del relè va su **+DC**, l'altra sul morsetto **x I/O**, e l'utilizzatore viene commutato dai contatti del relè (NC, C, NO). Il morsetto I/O usato deve essere impostato come uscita (**OUT**) nella pagina **IN/OUT** di TrikdisConfig.

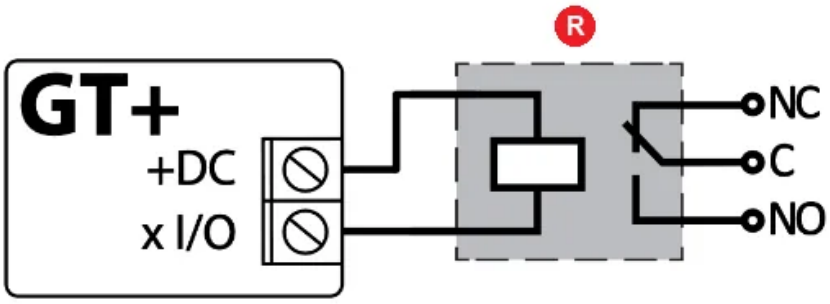


Figura 31. Collegamento di un relè all'uscita del comunicatore: la bobina va tra +DC e il morsetto x I/O, i contatti (NC, C, NO) commutano l'utilizzatore.

- R relè («Relay»)

Puoi comandare le uscite dall'app Protegus 2 o con un comando SMS (capitolo 5).

3.7 Collegamento dell'espansione iO-8

Se servono più ingressi o uscite, al bus RS485 del comunicatore si possono collegare al massimo quattro espansioni **iO-8**; ognuna aggiunge 8 I/O a doppia funzione. Collega i morsetti **A 485** e **B 485** con i morsetti **A (RS485)** e **B (RS485)** del modulo; sia il comunicatore sia l'espansione ricevono l'alimentazione dall'uscita di alimentazione ausiliaria della centrale (**+AUX** → **+DC**, **–AUX** → **–DC** su entrambi i dispositivi). L'espansione va aggiunta e configurata nella pagina **RS485 modules** di TrikdisConfig (paragrafo 6.8).

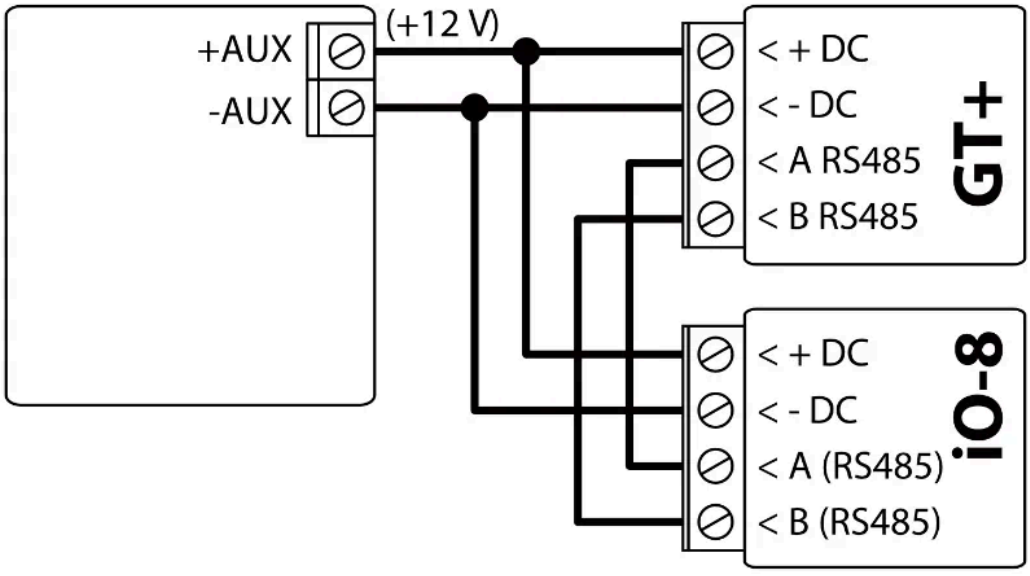


Figura 32. Collegamento dell'espansione iO-8 al bus RS485 del comunicatore; l'alimentazione dall'uscita AUX della centrale d'allarme («Control panel»), per entrambi i dispositivi.

3.8 Accensione e prima verifica

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 l'alimentazione della centrale d'allarme si avvia anche il comunicatore. Sul coperchio frontale devi vedere:

- **POWER** verde fisso – l'alimentazione è adeguata;
- **NETWORK** verde fisso e lampeggia in giallo – connesso alla rete; il numero di lampeggi gialli è il livello del segnale: su 4G 3 lampeggi sono adeguati; se ne conti meno, il segnale è debole: cerca un altro posto per il comunicatore o usa un'antenna più sensibile (paragrafo 3.2);
- **TROUBLE** spento.

Se TROUBLE lampeggia, il numero di lampeggi indica la causa (paragrafo 1.6); anche ogni altra segnalazione LED diversa da questa indica un guasto, la cui causa va cercata in base alle tabelle del paragrafo 1.6. Se nessun LED è acceso, controlla l'alimentazione e il collegamento.

4. Programmazione della centrale d'allarme

L'impostazione della centrale dipende da come l'hai collegata: al bus dati o alla porta seriale (paragrafo 4.1), oppure tramite il suo combinatore telefonico, ai morsetti TIP/RING (paragrafo 4.2). Con il GT+, per il collegamento DSC Keybus + TIP/RING servono entrambe le cose: le impostazioni del collegamento Keybus e la programmazione del combinatore della centrale (paragrafo 4.1.1).

4.1 Collegamento al bus dati o seriale

Qui descriviamo come impostare la centrale perché il comunicatore ne legga gli eventi e possa comandarla a distanza. Per il comando a distanza, nella pagina **Panel settings** di TrikdisConfig l'opzione **Remote Arm/Disarm** deve essere spuntata (paragrafo 2.2).

4.1.1 DSC

Le centrali **DSC PowerSeries** (l'elenco dei modelli supportati è al punto 1.2) non richiedono alcuna impostazione particolare: il comunicatore collegato al Keybus legge subito gli eventi e, dopo aver spuntato **Remote Arm/Disarm**, l'utente inserisce e disinserisce dall'app con il proprio codice utente. I dettagli del controllo diretto – stato delle zone, esclusione zone, riconoscimento automatico delle aree – sono trattati in un articolo a parte: Controllo diretto per le centrali d'allarme DSC PowerSeries.

Con le centrali **DSC PowerSeries NEO** il comunicatore non funziona: il produttore non consente dispositivi esterni sul bus NEO. Per NEO serve un comunicatore su linea telefonica (TIP/RING) – vedi DSC Power Series NEO e comunicatori Trikdis: compatibilità e soluzioni.

GT+, collegamento Keybus e TIP/RING (paragrafo 3.3.2): bisogna programmare il combinatore telefonico della centrale, perché invii gli eventi. La tabella seguente vale per la centrale DSC PowerSeries PC1616 (PC1832, PC1864). Sulla tastiera collegata alla centrale entra in programmazione: **[*][8][codice installatore]**, poi inserisci il numero della sezione.

Sezione	Valore
[301] Primo numero di telefono	Un numero qualsiasi più lungo di quattro cifre, **senza D** all'inizio (ad esempio `5555555`). La D significa attesa del tono di linea; senza di essa la centrale compone più velocemente. Il comunicatore risponde a tutte le chiamate
[310] Codice impianto del sistema	Il codice impianto a 4 cifre, seguito da `FF` (ad esempio `1234FF`). Al posto della cifra 0 usa la `A` esadecimale
[311] Codice impianto dell'area 1	Il codice impianto a 4 cifre; al posto dello 0 la `A` esadecimale
[350] Formato del combinatore	`03` (Contact ID) per il numero di telefono 1
[351]–[376] Direzioni di chiamata	Abilita per il numero di telefono 1 i gruppi di eventi necessari: Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Controlla a parte il gruppo Opening/Closing: su alcune centrali DSC è disattivato di fabbrica
[380] Opzione 1 del combinatore	Opzione 1 **ON** (combinatore abilitato); opzione 3 **OFF** (composizione DTMF)
[381] Opzione 2 del combinatore	Opzione 7 **OFF** (i codici di segnalazione Contact ID vengono generati automaticamente dalla centrale)
[320]–[349] Codici di segnalazione	Per gli eventi da trasmettere un valore qualsiasi, purché non sia `00`
[015] Opzione di sistema 3	Opzione 7 **OFF** (supervisione della linea telefonica, TLM, disattivata)

Disattiva la supervisione della linea telefonica (TLM): se resta attiva, la centrale può segnalare un guasto della linea telefonica. Il ritardo del guasto TLM si imposta nella sezione **[377]**.

I numeri di sezione sopra indicati valgono per le centrali PC1616, PC1832 e PC1864 (manuale di installazione v4.x). Con altri modelli DSC i numeri di sezione possono essere diversi – consulta il manuale di programmazione della centrale.

4.1.2 Paradox

Le centrali **Paradox** vanno programmate solo per il controllo diretto; per la lettura degli eventi non serve impostare nulla. Il firmware della centrale deve essere almeno **V.4**.

Sulle centrali Paradox più recenti (ad esempio le serie SP+, MG+ ed EVOHD+) la porta seriale può essere **bloccata di fabbrica**: il comunicatore non riceve dati finché non sblocchi la porta. La procedura di sblocco: Sblocco della porta seriale bloccata sulle centrali d'allarme Paradox.

Per il controllo va impostata la **password PC** della centrale (PC password), e la stessa va inserita anche nel campo **System settings** → **Security panel PC download password** di TrikdisConfig – le due devono coincidere.

1. Entra nella programmazione installatore della centrale dalla tastiera.
2. Apri la sezione della password PC: per le serie **MAGELLAN e SPECTRA** la sezione **911**, per la serie **DIGIPLEX EVO** la sezione **3012**.
3. Inserisci una password di **4 caratteri**. La password non può essere 0000 e **non deve iniziare con zero**.
4. Esci dalla programmazione e **riavvia la centrale** – la modifica della password PC diventa effettiva dopo il riavvio. Poi inserisci la stessa password in TrikdisConfig.

Errori tipici e soluzioni

- Il **codice utente assegnato all'area non può essere il codice master**: assegna all'utente un altro codice, e con quello l'inserimento / disinserimento da Protegus 2 funzionerà.
- **Dopo qualsiasi modifica dei codici utente riavvia il comunicatore** (togliendo l'alimentazione o con il comando SMS `RESET`): legge i codici all'avvio e non vede le modifiche successive.

Sui comunicatori GT e GT+ il campo **Security panel PC download password** si trova nella pagina **Panel settings** di TrikdisConfig, nel gruppo **Serial bus** (paragrafi 2.2 e 6.3).

Collegamento Keybus e TIP/RING (SP / SP+ / MG / MG+, paragrafo 3.3.4): la centrale va inoltre programmata in modo che invii gli eventi alla centrale di vigilanza e possa essere comandata da Protegus 2:

Sezione	Valore	Sezione	Valore
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

4.1.3 Texecom

Le centrali **Texecom Premier / Premier Elite** vanno programmate sia per la lettura degli eventi sia per il controllo: va impostata la password di 4 caratteri della centrale chiamata **UDL passcode**, e la stessa va inserita nel campo **System settings** → **Security panel PC download password** di TrikdisConfig – le due devono coincidere.

Con il software Wintex di Texecom: l'UDL passcode si trova nella scheda **Options** della finestra **Communication Options**.

Dalla tastiera:

1. Digita il codice installatore di 4 cifre e premi il tasto **[Menu]** per entrare nel menu di programmazione.
2. Subito dopo premi il tasto **[9]**.
3. Premi i tasti **[7][6]**, poi il tasto **[2]**, e inserisci l'UDL passcode di 4 cifre.
4. Premi il tasto **[Yes]**, poi esci dalla programmazione con il tasto **[Menu]**.

Sui comunicatori GT e GT+ il campo **Security panel PC download password** si trova nella pagina **Panel settings** di TrikdisConfig, nel gruppo **Serial bus**; l'UDL passcode deve coincidere con questo.

4.1.4 UTC Interlogix (Caddx)

Il firmware della centrale **UTC Interlogix (Caddx) NetworX** deve essere almeno **V2**. Sulla tastiera della centrale va impostato quanto segue:

1. Premi i tasti **[*][8]** e inserisci il codice installatore (di fabbrica **9713**).
2. Inserisci il **numero di dispositivo** assegnato al comunicatore (device address; di fabbrica **0**).
3. Programma una dopo l'altra le righe della tabella seguente: inserisci la locazione (location), il numero del segmento, poi l'impostazione. Con il tasto **[*]** puoi tornare al campo precedente. `12345678` significa che tutti gli otto interruttori del segmento sono attivati (sul display sono visibili tutte le cifre).

Locazione (location)	Segmento	Impostazione
23	3	12345678
37 (non strettamente necessario)	3	12345678
37 (non strettamente necessario)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Dopo aver programmato tutte le righe, premi due volte il tasto **[Exit]** per uscire dalla programmazione.

4.1.5 InnerRange

Il firmware della centrale **InnerRange Inception** deve essere almeno **2.3.0.3507-r0**, e la centrale necessita di una connessione Internet. La configurazione si esegue dall'interfaccia web della centrale:

1. Apri nel browser l'indirizzo `https://skytunnel.com.au/inception/NUMERODISERIE`, dove NUMERODISERIE è il numero di serie riportato sulla scatola della centrale. Accedi con l'account installatore.
2. Apri la pagina **Configuration → General → Alarm Reporting**.
3. Nel gruppo **3rd Party Device Configuration**: - spunta l'opzione **Enable 3rd Party Device Reporting**; - nel campo **3rd Party Device Type** scegli il valore **Trikdis**; - nel campo **Serial Port** scegli il valore **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Salva le impostazioni ed esci dall'interfaccia.

Il firmware della centrale **InnerRange Integriti** deve essere almeno **19.1.0.36608**, il suo software di programmazione (Integriti Professional) almeno **19.1.0.15396**. La configurazione si esegue nel software di programmazione della centrale:

1. Per la porta seriale (**TTL Port-0**) a cui è collegato il comunicatore, scegli il protocollo di comunicazione **Trikdis**.
2. Il formato dati deve essere **Contact ID**.
3. Impostazione della porta: **19200, 8, N, 1**.
4. Salva le impostazioni ed esci dal programma.

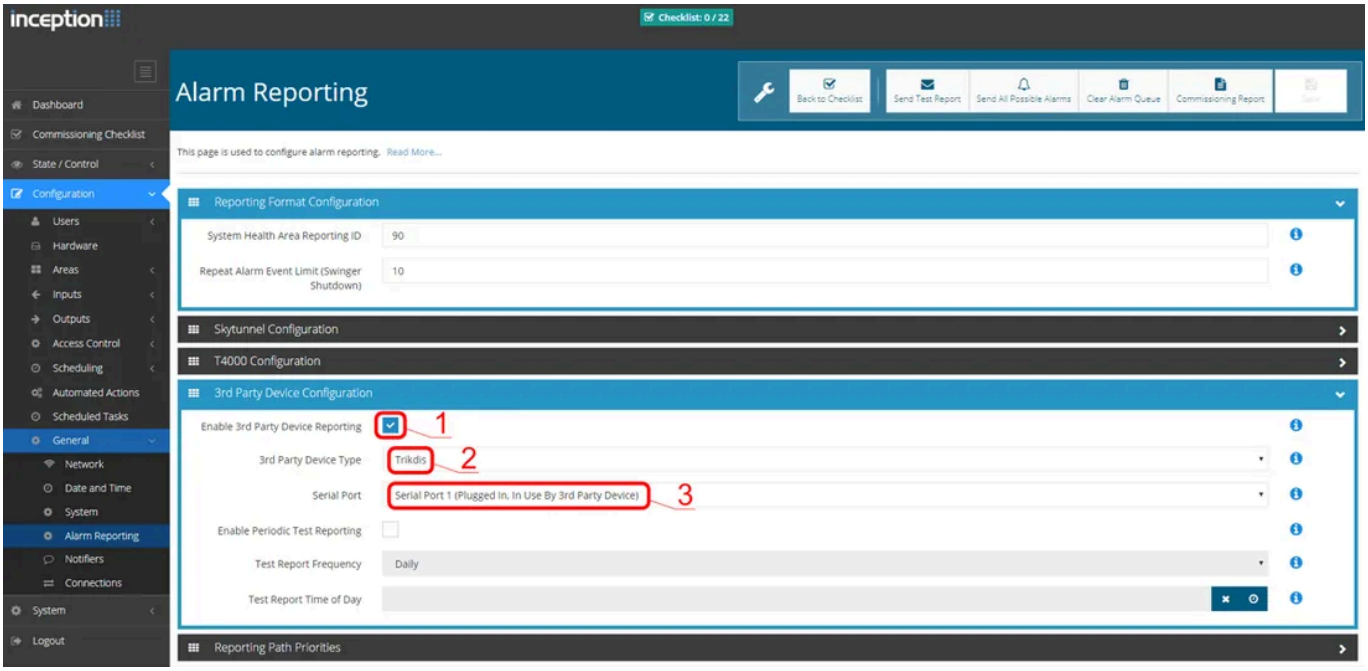


Figura 33. InnerRange Inception – Configuration → General → Alarm Reporting, gruppo 3rd Party Device Configuration: Enable 3rd Party Device Reporting spuntato, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

Il firmware delle centrali **Honeywell Ademco Vista-20** e **Vista-48** deve essere almeno **V5.3**. La configurazione si esegue dalla tastiera della centrale.

Accesso alla programmazione – in due modi:

- digita il codice installatore (di fabbrica **4112**), poi i tasti **[8][0][0]**; oppure
- alimenta la centrale ed **entro 50 secondi** premi contemporaneamente i tasti **[*]** e **[#]** (funziona solo se in precedenza si è usciti dalla programmazione con i tasti [*][9][8]).

Impostazioni:

1. Attiva l'invio degli eventi Contact ID sull'uscita radio a lunga portata (LRR): premi i tasti **[*][2][9][1][#]**.
2. Per il controllo da remoto abilita l'uso del **2° indirizzo AUI** (2nd AUI address): premi i tasti **[*][1][8][9][1][1][#]**.

Uscita dalla programmazione: premi i tasti **[*][9][9]**.

4.2 Collegamento alla linea telefonica (TIP/RING)

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.

Anche le centrali DSC, Paradox, Caddx, Texecom, InnerRange e Honeywell possono essere collegate al comunicatore tramite la loro uscita della linea telefonica (paragrafo 3.3.10) – in questo caso anche per queste bisogna configurare il combinatore, e il controllo diretto non è disponibile.

4.2.1 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`.

4.2.2 Il combinatore UTC Interlogix (Caddx) NX

Programmazione della centrale Interlogix NX-4V2 (NX-6V2, NX-8V2), se il comunicatore è collegato ai morsetti TIP/RING della centrale. Sulla tastiera inserisci in sequenza quanto segue:

Locazione (location)	Tasti	Nota
	`*89713`	Ingresso in programmazione (`9713` è il codice installatore di fabbrica)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Tutti i LED di zona accesi (segmento 1)
Location 4	`12345678*`	Tutti i LED di zona accesi (segmento 2)
Location 4	`12345678*#`	
Location 23	`23#`	Tutti i LED di zona accesi (segmento 3)
Location 23	`**`	Tutti i LED di zona accesi (segmento 3)
Location 23	`12345678*#`	Tutti i LED di zona accesi (segmento 3)
Location 37	`37#`	Tutti i LED di zona accesi (segmento 3)
Location 37	`**`	Tutti i LED di zona accesi (segmento 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT` `EXIT`	Uscita dalla programmazione

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 sugli eventi, può inserire e disinserire e comandare le uscite del comunicatore. L'app si scarica per Android e iOS (Google Play, App Store), oppure si può usare dal browser: web.protegus.app. Accedi con il tuo nome utente e la tua password, oppure registra un nuovo account.

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** (paragrafo 6.5).
3. Il LED **POWER** sia verde fisso.
4. Il LED **NETWORK** sia verde fisso e lampeggi in giallo (il dispositivo è in rete).

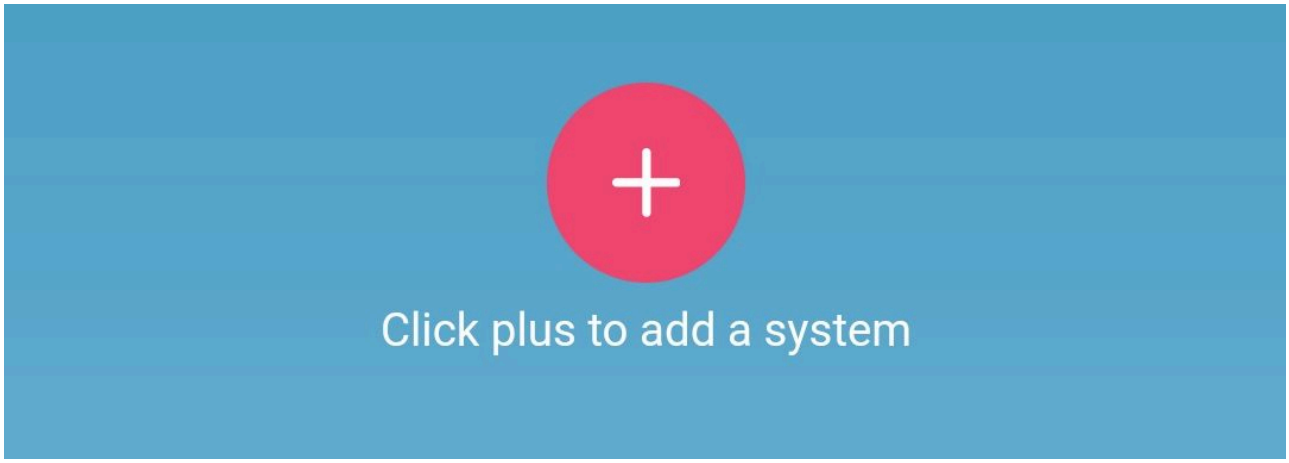
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è 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



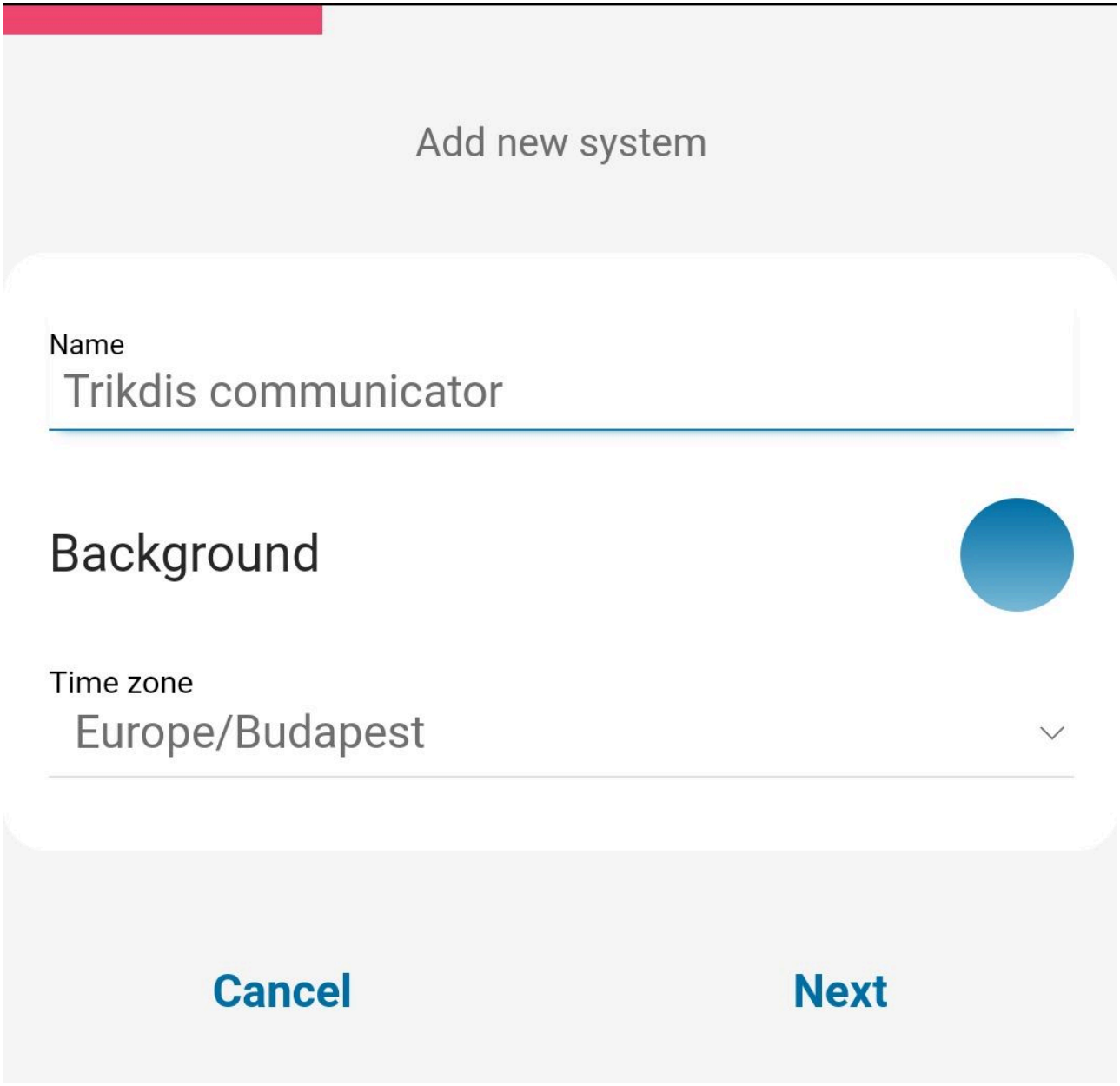
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



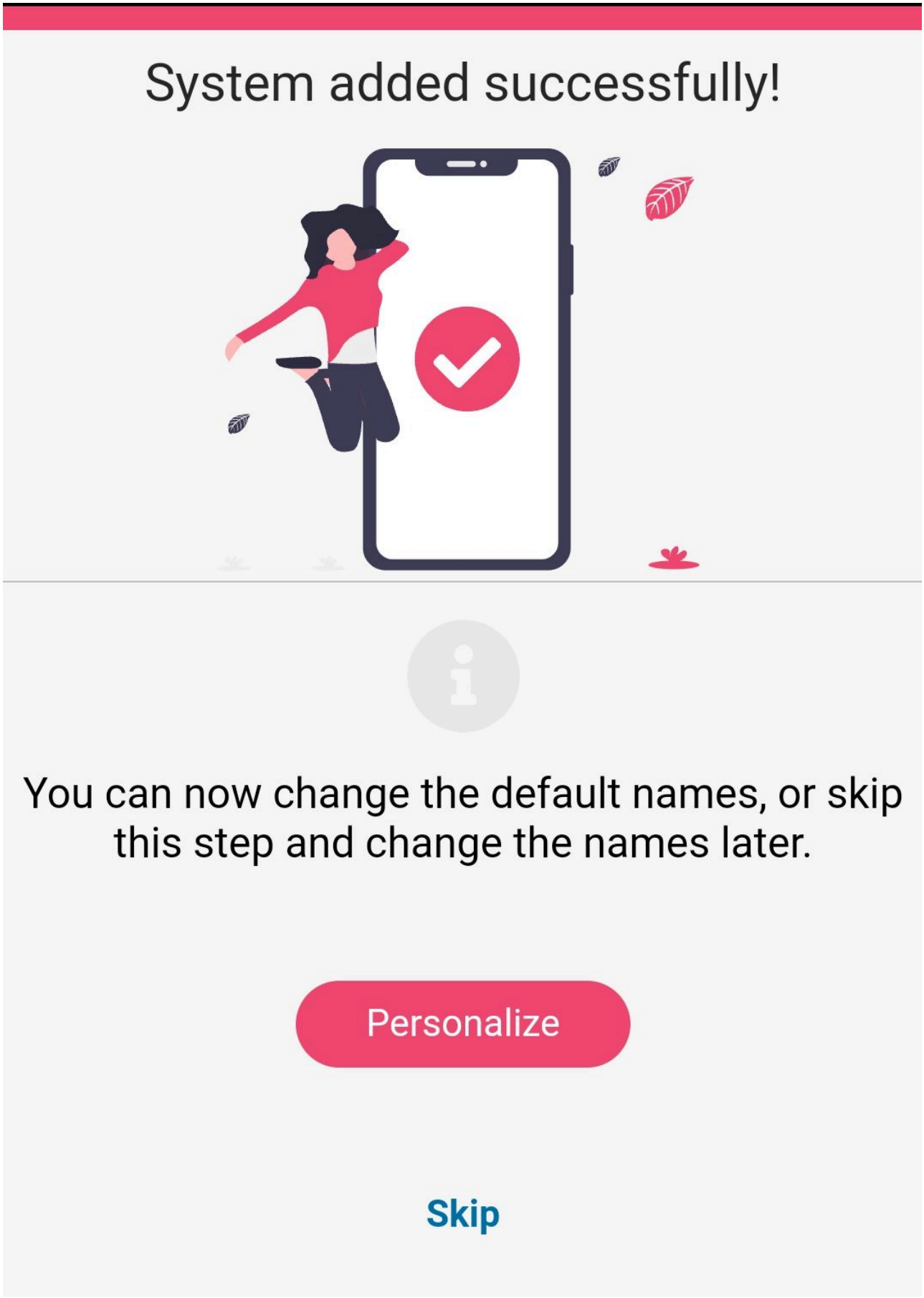
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



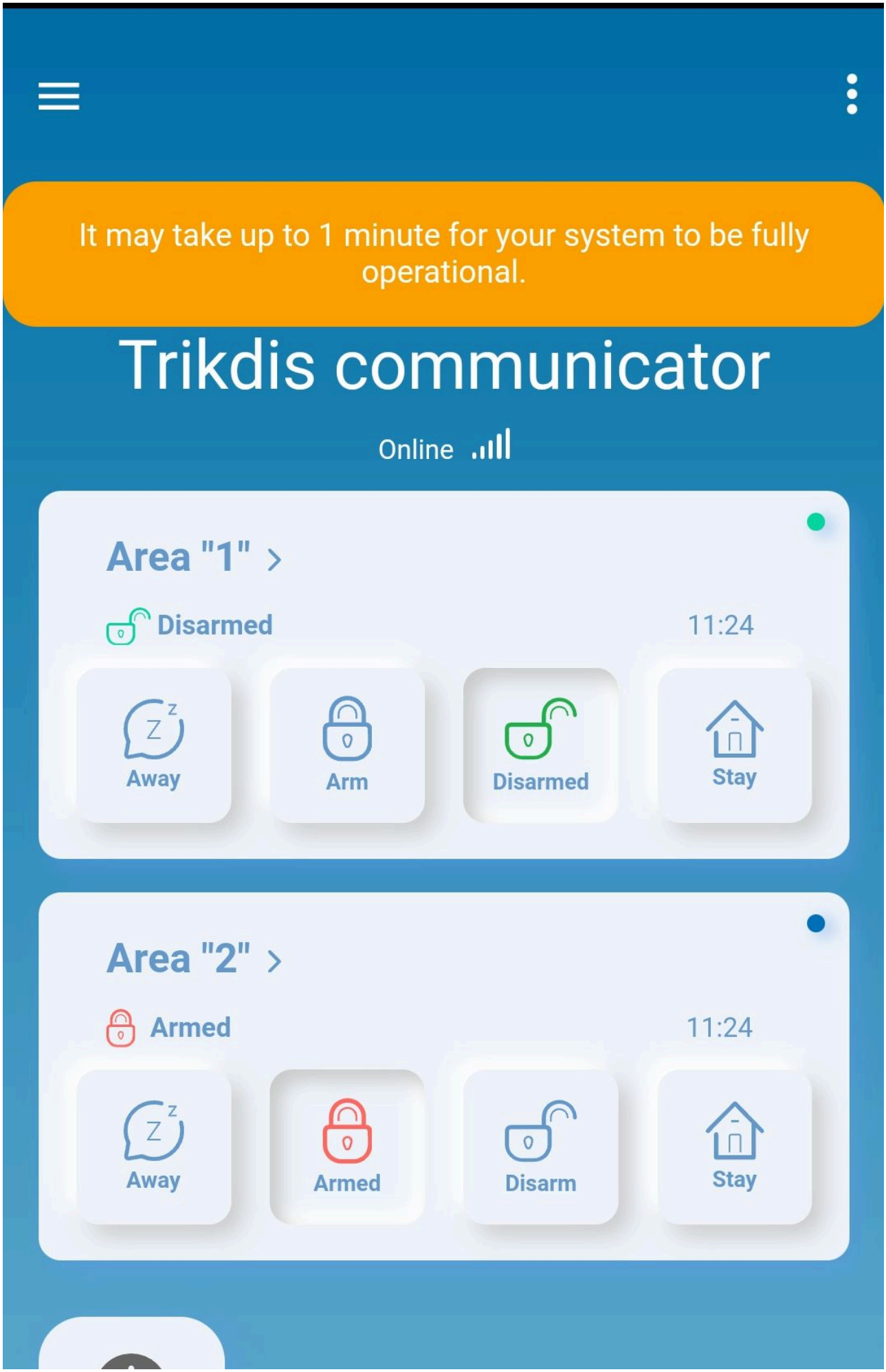
6. Add meg a rendszer nevét és válassz idozónát



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

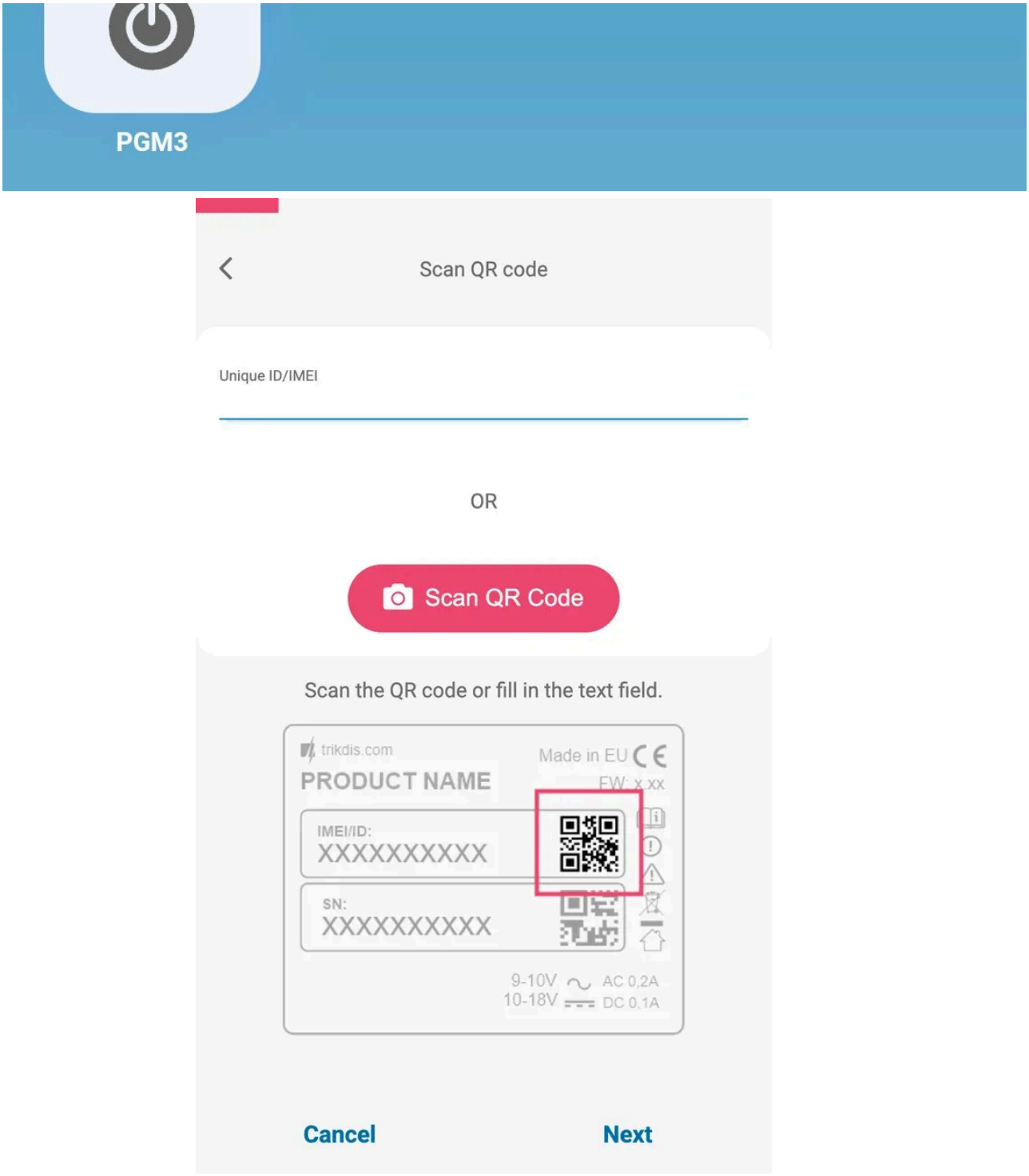


Figura 34. Protegus 2 – aggiunta di un nuovo sistema: inserimento dell'IMEI / Unique ID o lettura del codice QR dell'etichetta, poi Next.

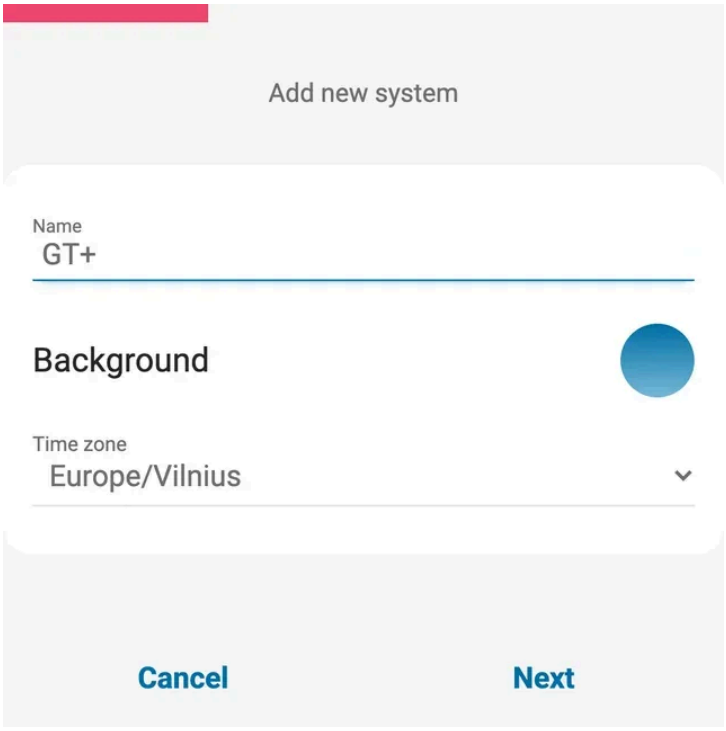


Figura 35. Protegus 2 – inserimento del nome del sistema (Name), poi Next.

L'identificativo univoco del dispositivo (**IMEI / Unique ID**) si legge sull'etichetta del dispositivo e sull'adesivo della confezione, ed è mostrato anche nella barra di stato di TrikdisConfig. Se nel dispositivo il **PROTEGUS Cloud access Code** non è quello di fabbrica, l'app lo chiede durante l'aggiunta.

5.2 Inserimento e disinserimento tramite 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.



Figura 36. Protegus 2 – la pagina «Il sistema non viene comandato a distanza» durante la creazione del sistema: con il pulsante Continue passi all'impostazione dell'area e dell'uscita PGM.

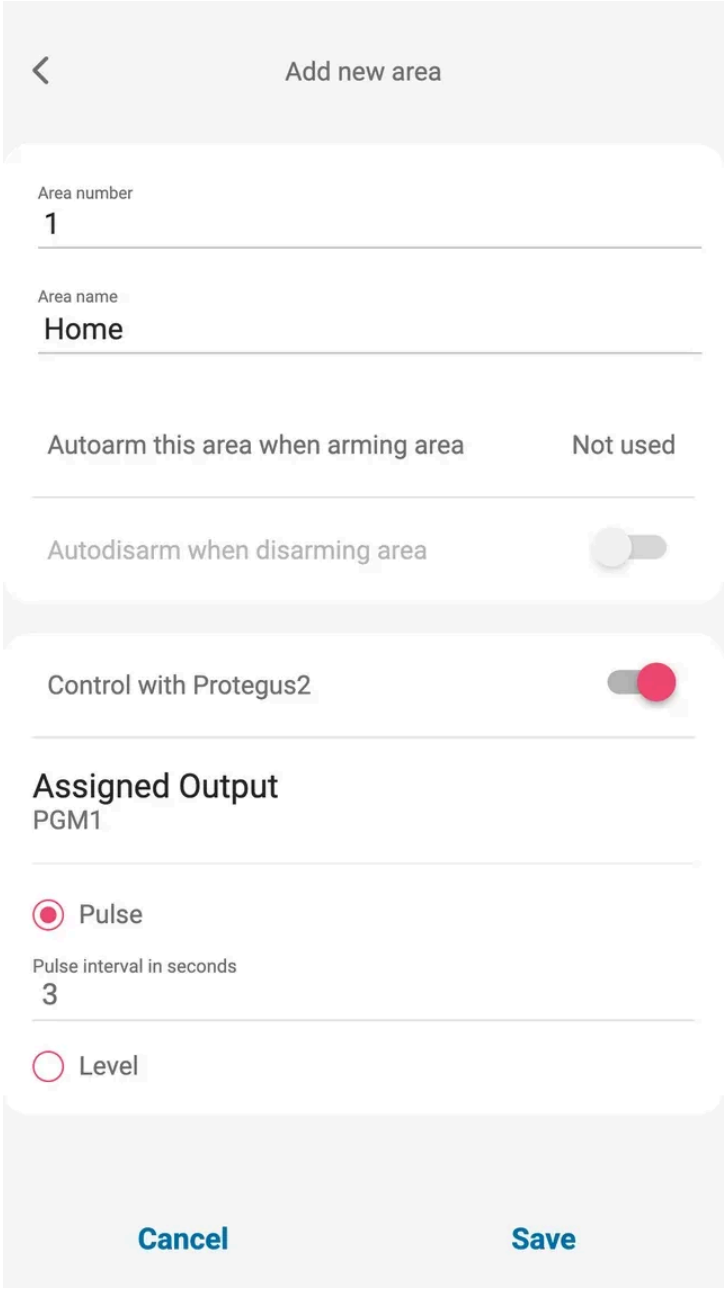


Figura 37. Protegus 2 – aggiunta di un'area (Add new area): Area number, Area name, Control with Protegus2 attivato, Assigned Output PGM1, Pulse (3 s) o Level, poi Save.

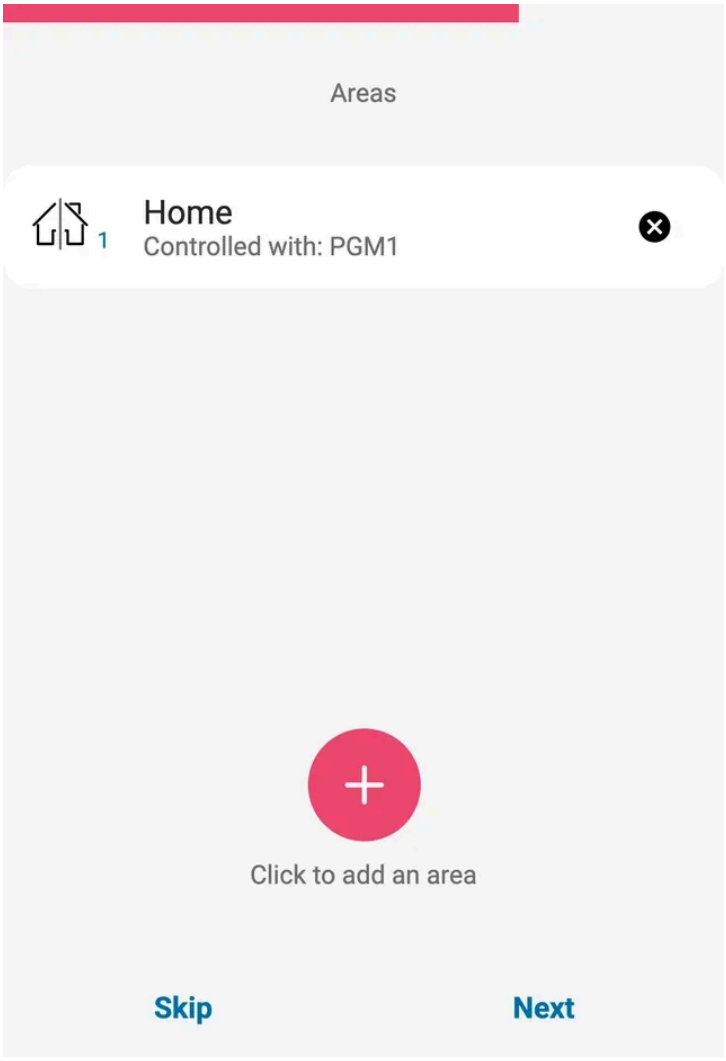


Figura 38. Protegus 2 – l'elenco delle aree (Areas): l'area Home è comandata da PGM1; un'altra area si aggiunge con il pulsante Click to add an area, la procedura guidata si chiude con il pulsante Skip.

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.

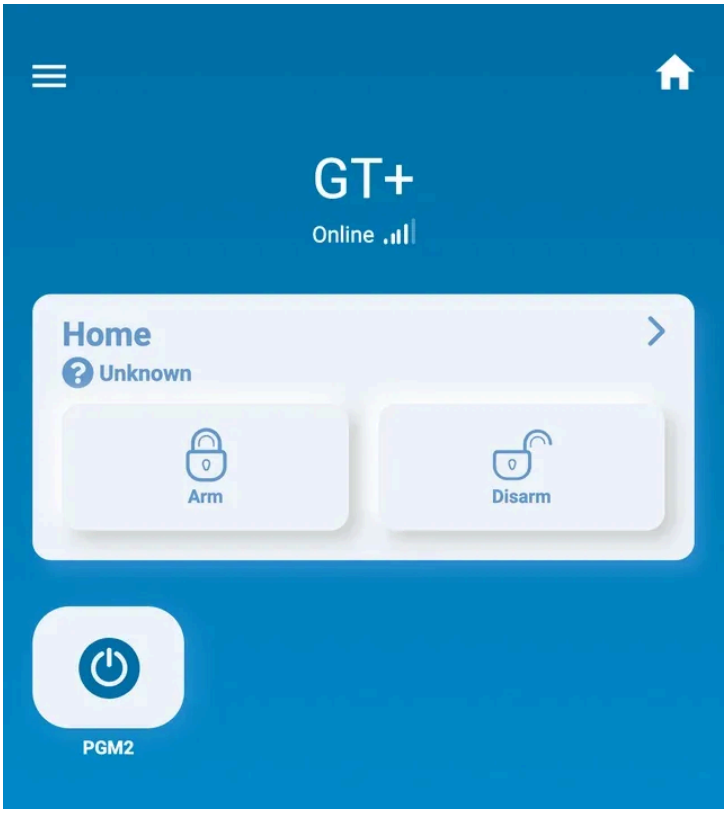


Figura 39. Protegus 2 – la schermata iniziale del sistema: lo stato dell'area, i pulsanti Arm e Disarm, sotto l'uscita PGM comandabile.

5.4 Comando con messaggi SMS

Il comunicatore può essere comandato anche con comandi SMS. La struttura del messaggio: `Password Comando Dati` (separati da spazi). Come password puoi usare il codice **amministratore** (di fabbrica `123456`) per i comandi `INFO`, `RESET` e `OUTPUTx`, e il codice **installatore** (di fabbrica `654321`) per i comandi `INFO` e `OUTPUTx`.

Comando	Dati	Cosa fa	Esempio
`INFO`	–	Richiede informazioni sul dispositivo. La risposta: il tipo di dispositivo, il numero IMEI, il numero di serie e la versione del firmware.	`123456 INFO`
`RESET`	–	Riavvia il dispositivo (solo con il codice amministratore).	`123456 RESET`
`OUTPUTx`	`ON`	Attiva l'uscita x (x = 1 o 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Disattiva l'uscita x.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Attiva l'uscita in modalità impulsiva per il tempo indicato; `tttt` è la durata dell'impulso in secondi, con quattro cifre.	`123456 OUTPUT2 PULSE=0002`

L'uscita può essere comandata solo se nella pagina **IN/OUT** di TrikdisConfig il morsetto I/O in questione è impostato come uscita (**OUT**). Puoi limitare i numeri di telefono da cui il dispositivo accetta comandi nella scheda **User reporting** → **Control by SMS** (paragrafo 6.5).

6. TrikdisConfig – le impostazioni in dettaglio

Sul lato sinistro della finestra di TrikdisConfig si vede l'elenco delle pagine (System settings, Panel settings, CMS reporting, User reporting, Network settings, 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 pagina per pagina le impostazioni del GT e del GT+; dove le due versioni differiscono, lo indichiamo a parte.

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 40. La barra di stato di TrikdisConfig con un GT+ letto: identificativo, stato, tipo (Device: GT+_M150), numero di serie, versioni, modalità di connessione e livello di accesso.

Nel campo **Device** deve comparire la sigla GT per il GT e GT+ per il GT+ (nella figura GT+_M150; il suffisso lettera-numero indica la versione hardware). Dopo **Read [F4]** il programma legge e mostra i valori impostati nel dispositivo; esegui le impostazioni necessarie secondo le descrizioni delle pagine riportate di seguito.

6.2 System settings

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

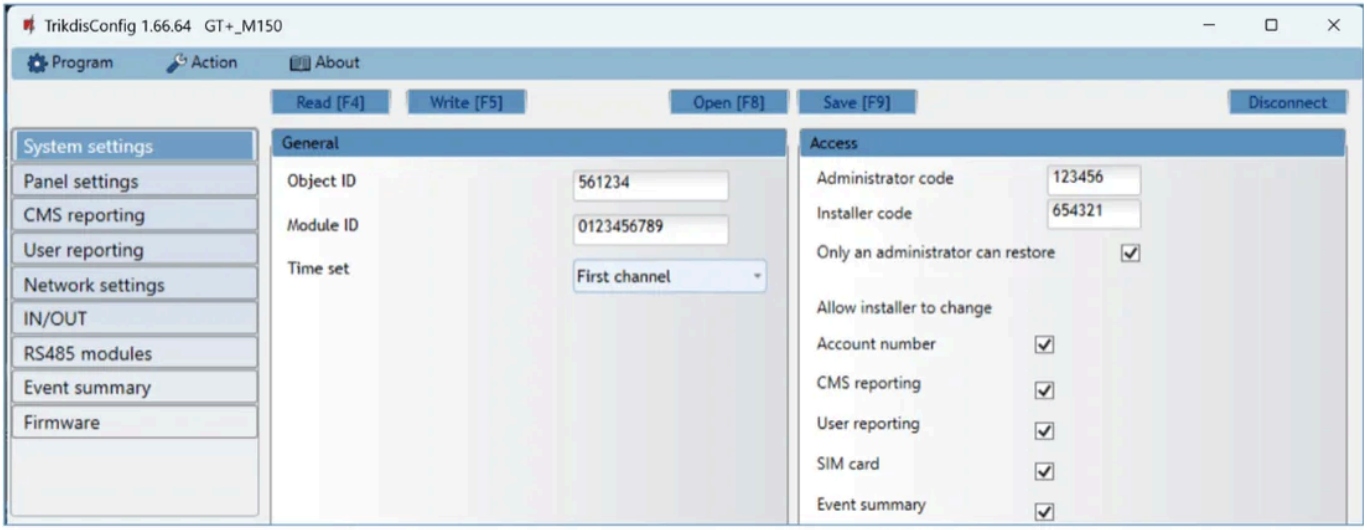


Figura 41. TrikdisConfig – pagina System settings: gruppi General e Access.

- **Object ID** – il codice impianto ricevuto dalla centrale di vigilanza (6 caratteri esadecimali: 0–9, A–F; `FFFE` e `FFFF` non possono essere usati). Obbligatorio se il dispositivo trasmette anche alla centrale di vigilanza.
- **Module ID** – il numero identificativo del modulo.
- **Time set** – il server da cui il dispositivo sincronizza il proprio orologio.

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 Panel settings

In questa pagina indichi come il comunicatore si collega alla centrale d'allarme: il gruppo **TLC** contiene le impostazioni del collegamento alla linea telefonica (TIP/RING), il gruppo **Serial bus** quelle del collegamento al bus dati o seriale. Qui si trovano anche le impostazioni comuni che riguardano la gestione degli eventi della centrale.

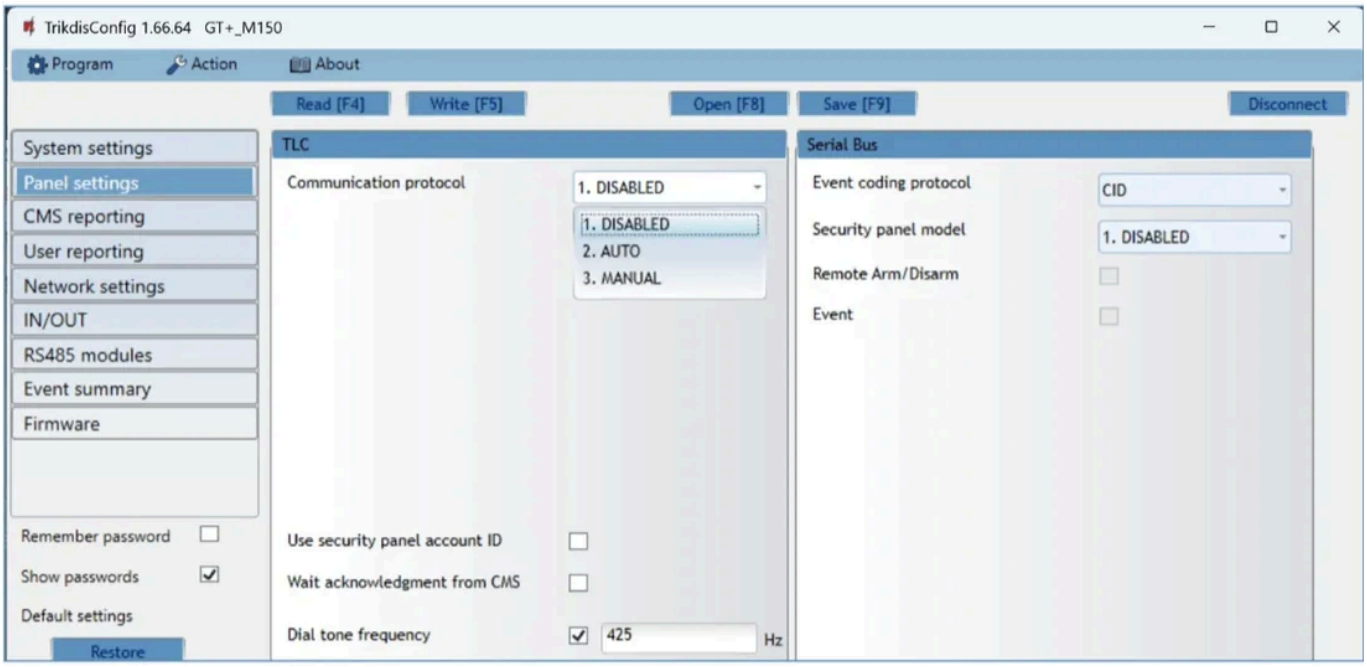


Figura 42. TrikdisConfig – Panel settings sul GT+: l'elenco Communication protocol del gruppo TLC (1. DISABLED, 2. AUTO, 3. MANUAL), sotto il gruppo Serial bus e le impostazioni comuni.

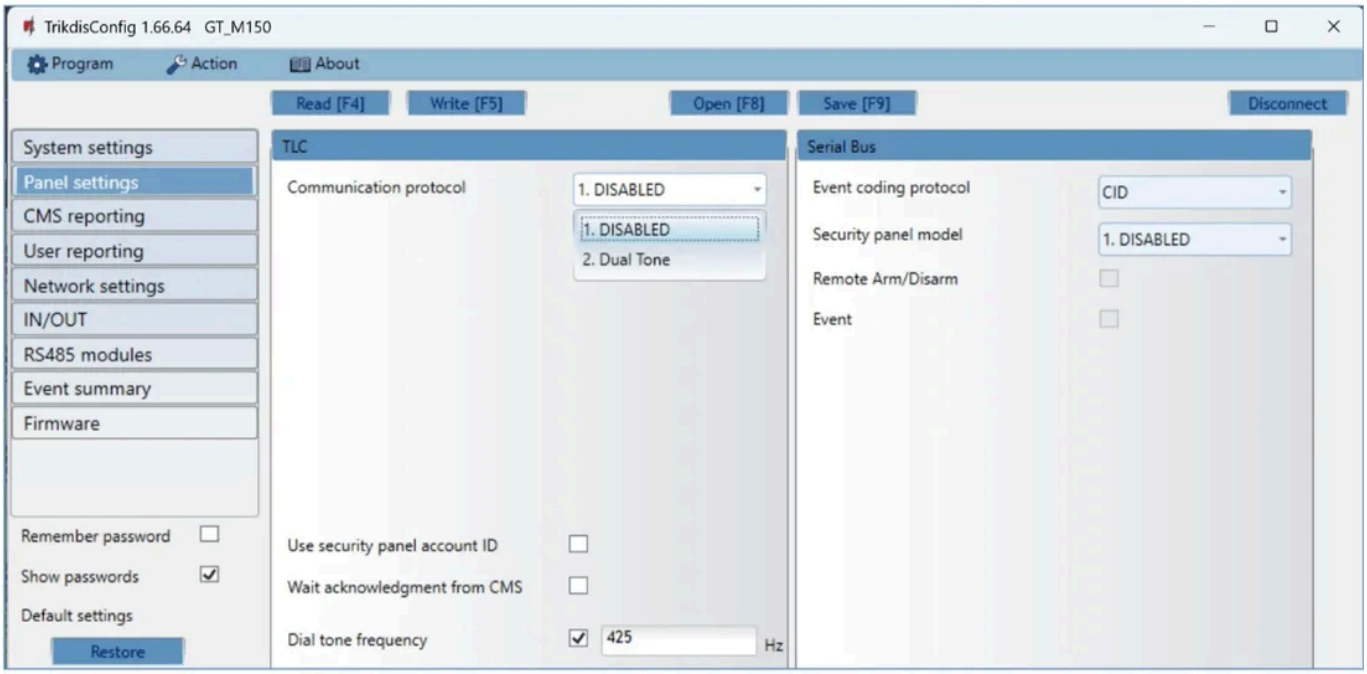


Figura 43. TrikdisConfig – Panel settings sul GT: qui l'elenco Communication protocol contiene 1. DISABLED e 2. Dual tone.

Gruppo TLC – se il comunicatore è collegato ai morsetti TIP/RING della centrale:

- **Communication protocol** – attivazione o disattivazione dell'interfaccia di linea telefonica DTMF del comunicatore. GT+: **1. DISABLED** (disattivato), **2. AUTO**, **3. MANUAL**; GT: **1. DISABLED**, **2. Dual tone**. Con il collegamento TIP/RING scegli il valore AUTO (GT: Dual tone).

Le impostazioni sotto il gruppo, valide per entrambi i collegamenti:

- **Use security panel account ID** – se spuntato, il comunicatore non usa il proprio Object ID, ma il codice impianto impostato nella centrale e inviato dalla centrale.

- **Wait acknowledgment from CMS** – se spuntato, dopo ogni evento il comunicatore attende la conferma del ricevitore (kiss-off) e solo dopo dà la conferma alla centrale; se la conferma non arriva in tempo, invia di nuovo il messaggio. Se il dispositivo non trasmette alla centrale di vigilanza, lascialo disattivato.
- **Dial tone frequency** – la frequenza del tono di linea con cui il comunicatore comunica con il combinatore della centrale (predefinito 425 Hz, il tono di linea usato in gran parte d'Europa, anche in Italia).



Figura 44. TrikdisConfig – Panel settings, gruppo Serial bus: Event coding protocol CID, Security panel model (nella figura Paradox SP/MG), Remote Arm/Disarm ed Event spuntati, Security panel PC download password inserita.

Gruppo Serial bus – se il comunicatore è collegato al bus dati o alla porta seriale della centrale:

- **Event coding protocol** – il protocollo di codifica degli eventi (CID).
- **Security panel model** – il modello della centrale d'allarme collegata, dall'elenco (per il collegamento Keybus + TIP/RING delle Paradox SP / SP+ / MG / MG+ scegli la voce **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – se spuntato, il comunicatore comanda direttamente la centrale (inserimento e disinserimento da Protegus 2). È visibile solo con le centrali a controllo diretto. Per il controllo diretto bisogna configurare anche la centrale secondo il capitolo 4.
- **Security panel PC download password** – per il controllo diretto delle centrali Paradox e Texecom, la password PC o UDL; deve coincidere con la password impostata nella centrale, la cui impostazione è descritta nel capitolo 4.

6.4 CMS reporting

Il comunicatore invia gli eventi alla centrale di vigilanza tramite la connessione dati mobile (IP). Gli eventi possono essere inviati su più canali: il canale **principale** e quello **parallelo** funzionano contemporaneamente (verso due ricevitori insieme), e a ciascuno appartiene un canale **di riserva**, che entra in funzione se il canale corrispondente si interrompe. La comunicazione è cifrata e protetta da password; per la ricezione e per l'inoltro degli eventi al software di vigilanza serve un ricevitore Trikdis (ricevitore software IPcom – Windows o Linux –, ricevitore IP/SMS RL14 o ricevitore multicanale RM14) o un ricevitore universale che supporti i protocolli DC-09 / TL150. GT e GT+ trasmettono alla centrale di vigilanza solo su canale IP, non hanno un canale SMS.

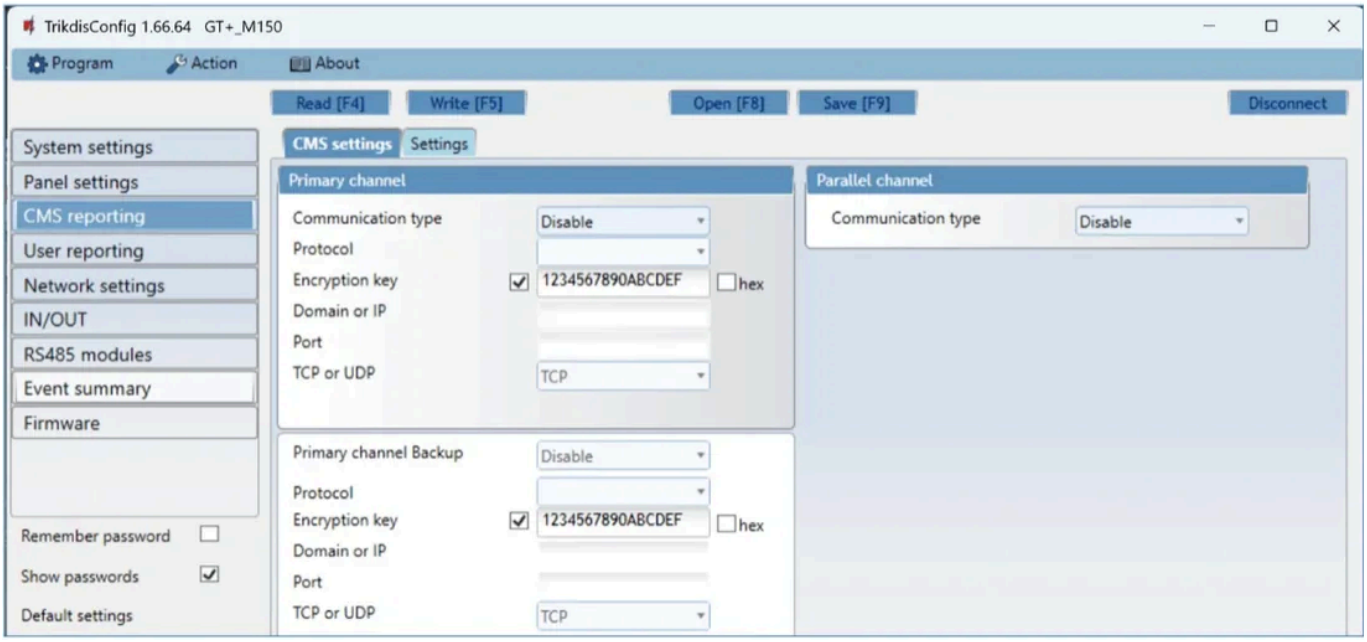


Figura 45. TrikdisConfig – CMS reporting, scheda CMS settings: canale principale, di riserva e parallelo.

Primary channel – canale principale

- **Communication type** – la modalità di connessione con il ricevitore: **IP**.
- **Protocol** – **TRK8** (ricevitori Trikdis), **DC-09_2007** o **DC-09_2012** (ricevitori universali), **TL150** (ricevitori SUR-GARD).
- **Encryption key** – la chiave di cifratura dei messaggi; nel comunicatore e nel ricevitore deve essere la stessa.
- **Domain or IP**, **Port** – il nome di dominio o l'indirizzo IP del ricevitore e la sua porta.
- **TCP or UDP** – il protocollo di trasmissione.

Parallel channel – canale parallelo. Oltre al principale, invia contemporaneamente a un secondo ricevitore (ad esempio alla centrale di vigilanza locale e a quella centrale). Le sue impostazioni sono le stesse del canale principale.

Primary channel Backup – canale di riserva. Assume la comunicazione se il canale principale non funziona; le sue impostazioni coincidono con quelle descritte sopra.

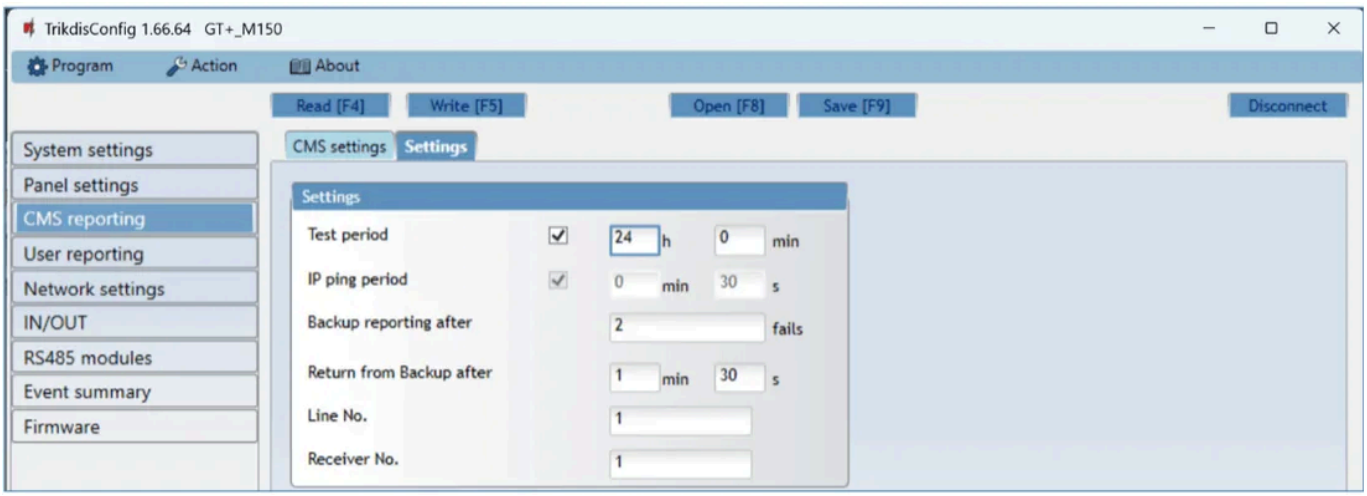


Figura 46. TrikdisConfig – CMS reporting, scheda Settings: rapporto di test, PING, i tempi del canale di riserva e i dati DC-09.

Nella scheda **Settings** imposti i tempi 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.

Nella scheda Settings del GT e del GT+, nel gruppo DC-09 compaiono i campi **Line No.** (numero di linea) e **Receiver No.** (numero di ricevitore); il gruppo compare se nel campo **Protocol** di uno dei canali è selezionato DC-09_2007 o DC-09_2012.

6.5 User reporting

Nella scheda **PROTEGUS Cloud** abiliti il servizio Protegus, con cui l'utente sorveglia e comanda a distanza il comunicatore e il sistema collegato; dettagli: www.protegus.app.

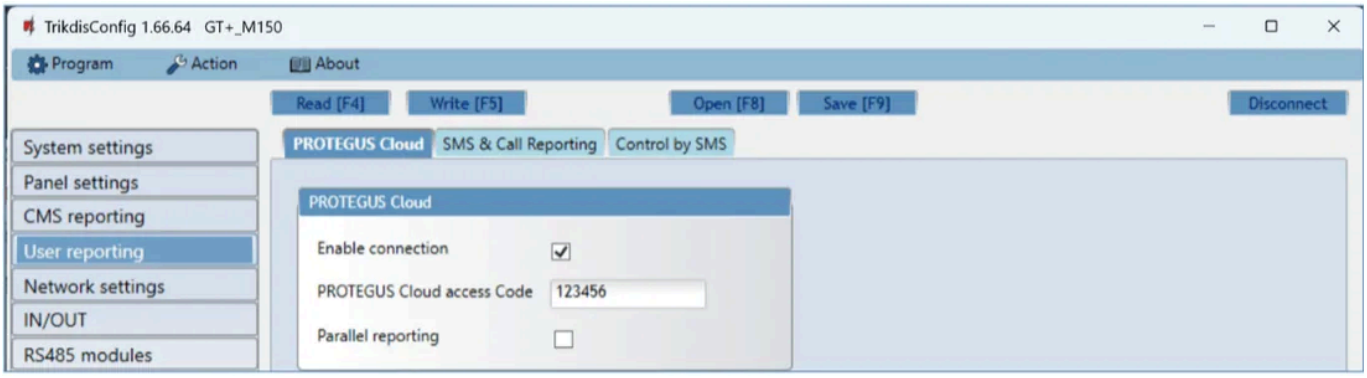


Figura 47. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- **Enable connection** – abilita il servizio Protegus: il dispositivo scambia dati con l'app Protegus 2, e TrikdisConfig può raggiungerlo anche a distanza.
- **PROTEGUS Cloud access Code** – codice a 6 cifre per la connessione a Protegus 2 (di fabbrica `123456`). Se lo cambi in TrikdisConfig, devi aggiornarlo anche nell'app Protegus 2.
- **Parallel reporting** – se spuntato, i messaggi vengono inviati contemporaneamente sul canale principale (alla centrale di vigilanza) e a Protegus 2.

Nella scheda **SMS & Call Reporting** l'utente può ricevere notifiche sugli 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.

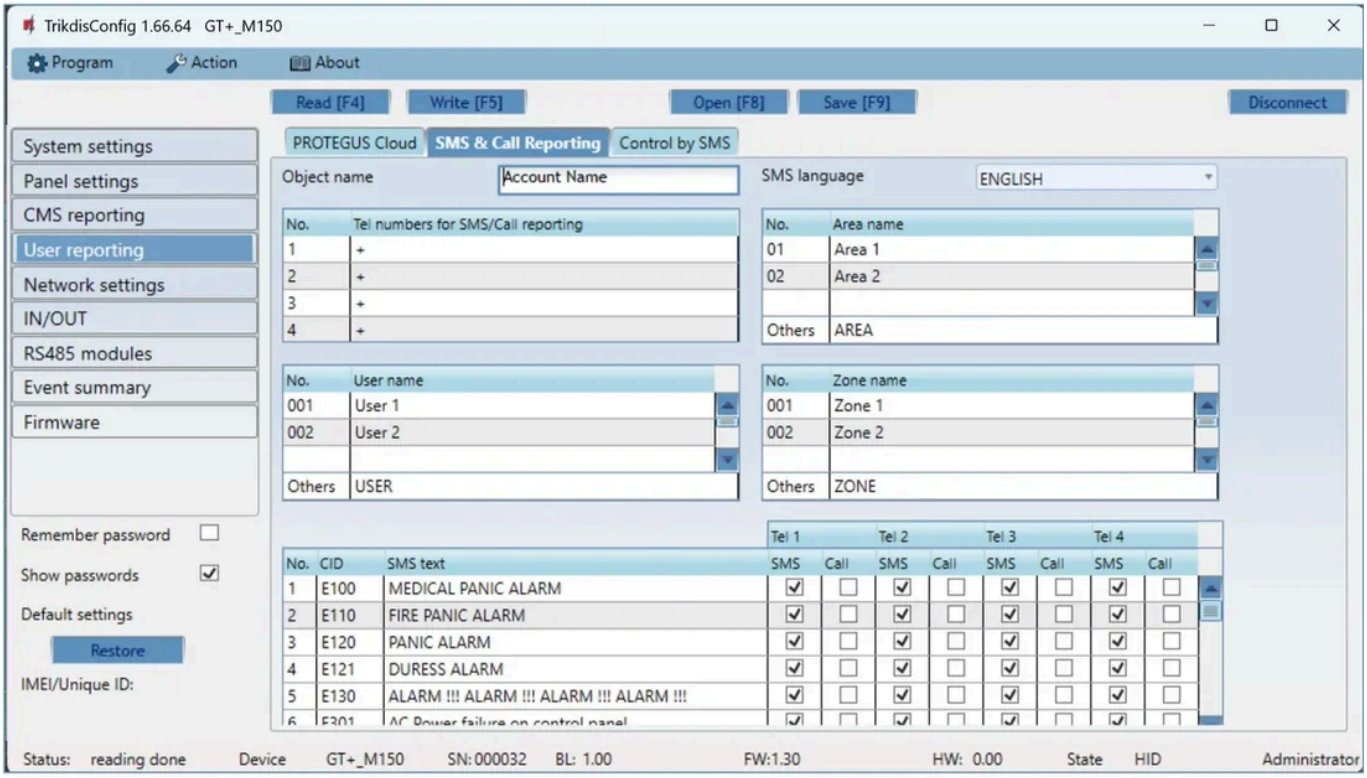


Figura 48. TrikdisConfig – User reporting, scheda SMS & Call Reporting.

- **Object name** – il nome del sistema; compare in ogni SMS.
- **SMS language** – la lingua degli SMS (i messaggi possono essere inviati anche con i caratteri propri della lingua).
- **Tel numbers for SMS/Call reporting** – al massimo 4 numeri di telefono che ricevono SMS o chiamate sugli eventi; inseriscili con il prefisso internazionale (`+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 nome.
- **CID event table** – per ogni evento si può impostare quale numero riceve l'SMS o la chiamata. Il testo SMS e il codice Contact ID degli eventi predefiniti sono modificabili, e si può aggiungere anche un nuovo evento con una descrizione.

Nella scheda **Control by SMS** imposti la ricezione dei comandi SMS: con i comandi si possono comandare le uscite e richiedere informazioni sul dispositivo (i comandi sono descritti nel paragrafo 5.4).

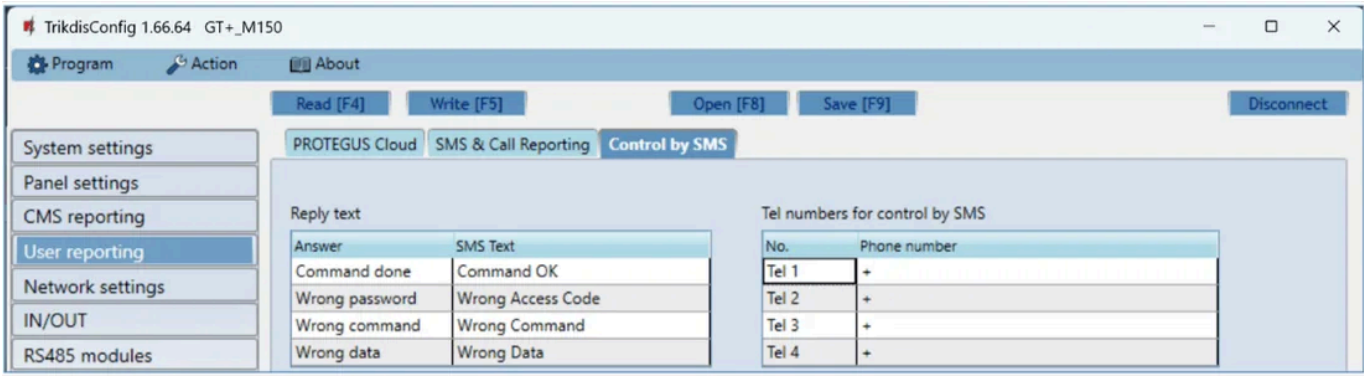


Figura 49. TrikdisConfig – User reporting, scheda Control by SMS.

- **Reply text** – il testo dei messaggi di risposta al comando SMS: comando riuscito (Command done), password errata (Wrong password), comando errato (Wrong command), dati errati (Wrong data). I testi sono modificabili.
- **Tel numbers for control by SMS** – i numeri di telefono da cui il dispositivo accetta comandi.

Se qui non è indicato alcun numero di telefono, il dispositivo accetta comandi 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.

6.6 Network settings

Prima dell'uso assicurati che la scheda SIM sia attiva e funzioni. Se invii gli eventi su canale IP o a Protegus 2 tramite Internet mobile, sulla scheda deve essere abilitato anche il servizio dati mobile.

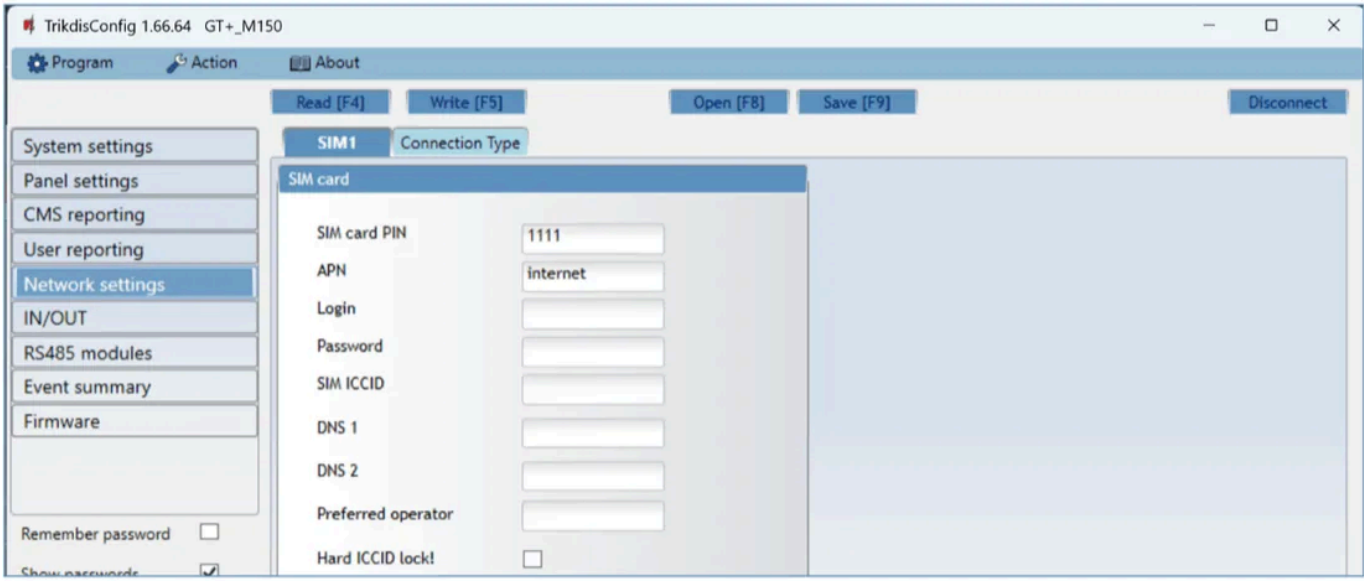


Figura 50. TrikdisConfig – Network settings, scheda SIM1: i dati della scheda SIM.

Scheda SIM1, gruppo SIM card

- **SIM card PIN** – il codice PIN della scheda. Puoi disattivare la richiesta del PIN inserendo la scheda in un telefono cellulare e disabilitandola lì; in questo caso il campo può mantenere il valore di fabbrica.
- **APN** – il punto di accesso dell'operatore (Access Point Name); senza di esso il dispositivo non si connette a Internet. Il valore lo trovi sul sito dell'operatore della scheda SIM; `internet` è generico e funziona nella rete di molti operatori. Gli APN noti degli operatori sono elencati nell'articolo sugli APN (con le schede IoT / M2M l'operatore fornisce un APN a parte, vedi il paragrafo 2.2).
- **Login, Password** – nome utente e password per la connessione Internet, se l'operatore li richiede.

- **SIM ICCID** – il numero ICCID della scheda SIM, se vuoi che il dispositivo funzioni solo con questa scheda. Se l'ICCID della scheda inserita non corrisponde, il LED TROUBLE lampeggia 8 volte (paragrafo 1.6).
- **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 nel campo **Domain or IP** con un nome di dominio e non con un indirizzo IP. Il valore predefinito è il DNS pubblico di Google. Indipendentemente dalle impostazioni IP, verifica che gli indirizzi DNS funzionino con il tuo operatore.
- **Preferred operator** – il codice dell'operatore mobile (MCC + MNC); se lo indichi, il dispositivo si connette solo alla rete dell'operatore scelto.
- **Hard ICCID lock** – se spuntato e dopo il riavvio del dispositivo, il comunicatore resta vincolato rigidamente alla scheda SIM con il numero ICCID indicato.

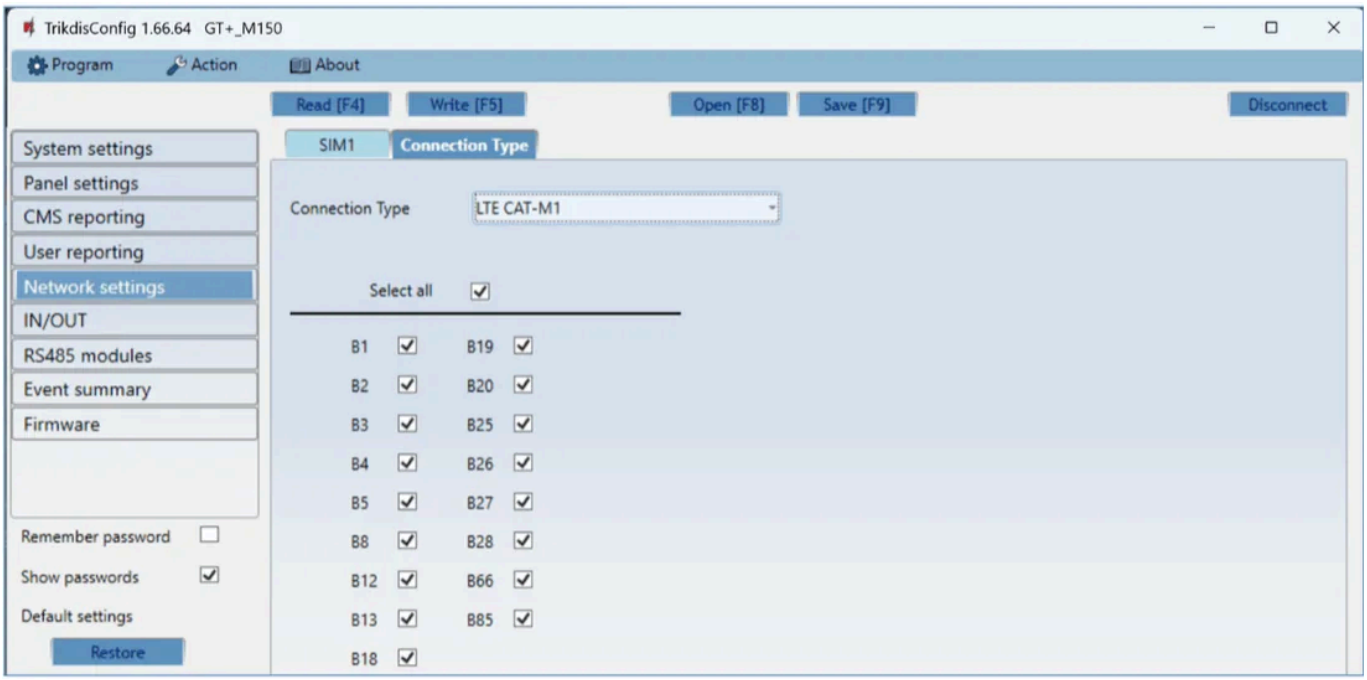


Figura 51. TrikdisConfig – Network settings, scheda Connection Type: selezione delle bande LTE della versione con modem CAT-M1.

Scheda Connection Type – valida solo per la versione con modem CAT-M1 (BG95-M5): qui puoi indicare su quali bande di frequenza LTE deve funzionare il modem del dispositivo (**Select all** = tutte).

6.7 IN/OUT

Qui indichi il ruolo dei due morsetti I/O a doppia funzione del comunicatore: **Off** (non usato), **IN** (ingresso) o **OUT** (uscita). Per l'ingresso bisogna indicare nel campo **Type** anche il tipo del circuito collegato (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

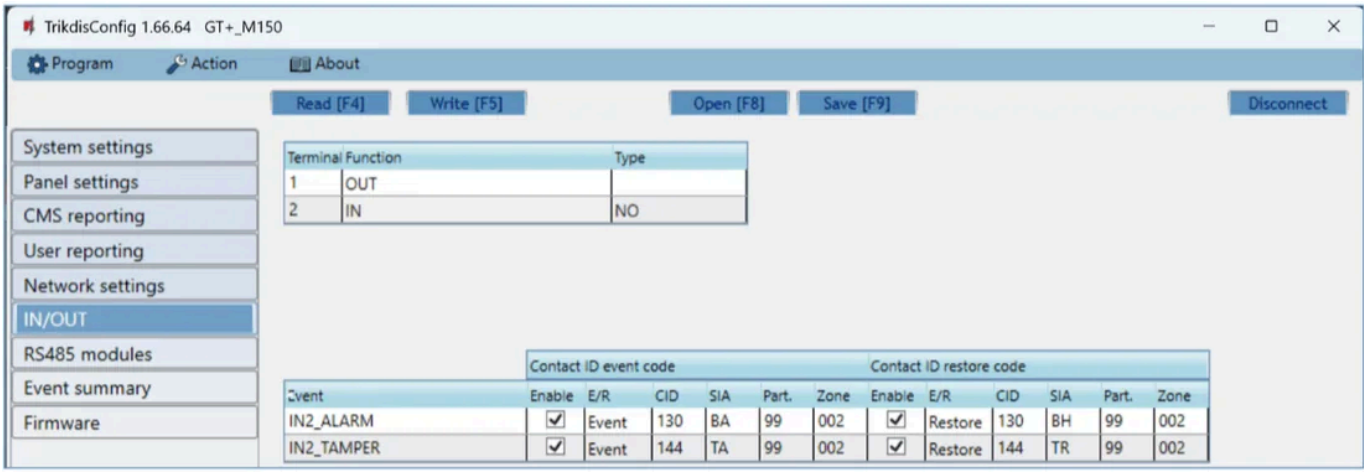


Figura 52. TrikdisConfig – pagina IN/OUT: il morsetto 1 è un'uscita (OUT), il 2 un ingresso (IN, NO); sotto gli eventi di allarme e di manomissione dell'ingresso 2 con codice CID e SIA.

Quando il sensore collegato all'ingresso viene attivato, il comunicatore invia un proprio evento (**INx_ALARM**, Contact ID 130, SIA BA; ripristino BH), e quando viene violato il circuito antimanomissione invia un evento di manomissione (**INx_TAMPER**, 144, SIA TA; ripristino TR) 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 alla centrale di vigilanza e a Protegus 2.
- **E/R** – il tipo di messaggio: Event (evento) o Restore (ripristino).
- **CID** – il codice Contact ID (modificabile, oppure può restare quello di fabbrica).
- **SIA** – il codice SIA (modificabile, oppure può restare quello di fabbrica).
- **Part.** – il numero dell'area nel messaggio.
- **Zone** – il numero della zona nel messaggio.

6.8 RS485 modules

Con le espansioni **iO-8** collegate al bus RS485 si possono aggiungere al comunicatore altri ingressi e uscite. Le espansioni collegate vanno aggiunte nella scheda **Modules list**.

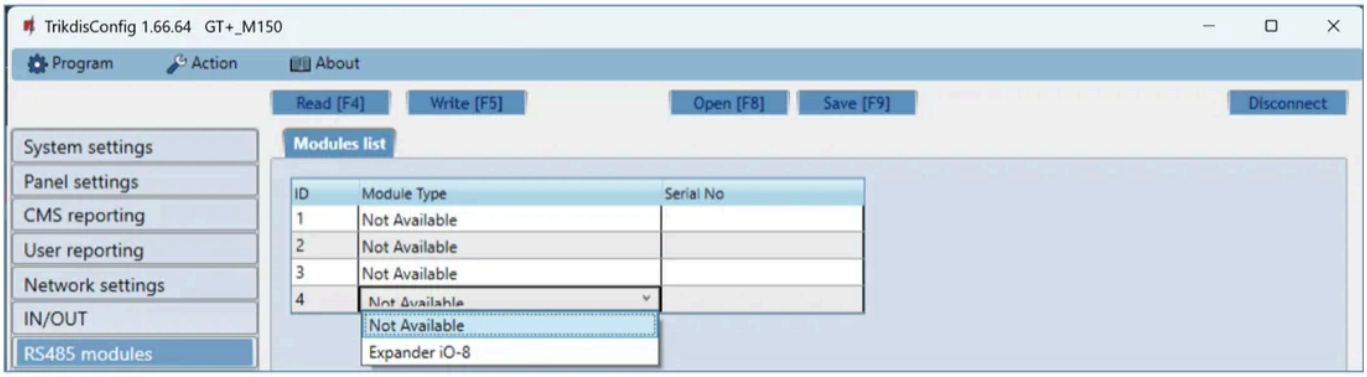


Figura 53. TrikdisConfig – RS485 modules, scheda Modules list: alla posizione 4 l'elenco Module type (Not Available, Expander iO-8).

- **Module type** – il tipo del modulo collegato al bus, dall'elenco (**Expander iO-8**).
- **Serial No** – il numero di serie a 6 cifre del modulo (sul contenitore del modulo e sull'adesivo della confezione).

Dopo aver scelto il modulo e inserito il numero di serie, passa alla scheda **RS485 modules** → **Module**: per il modulo aggiunto compare una scheda propria, numerata (Module 1 …), con le sue impostazioni.

Espansione iO-8 – 8 morsetti I/O a doppia funzione; al comunicatore si possono collegare al massimo quattro iO-8.

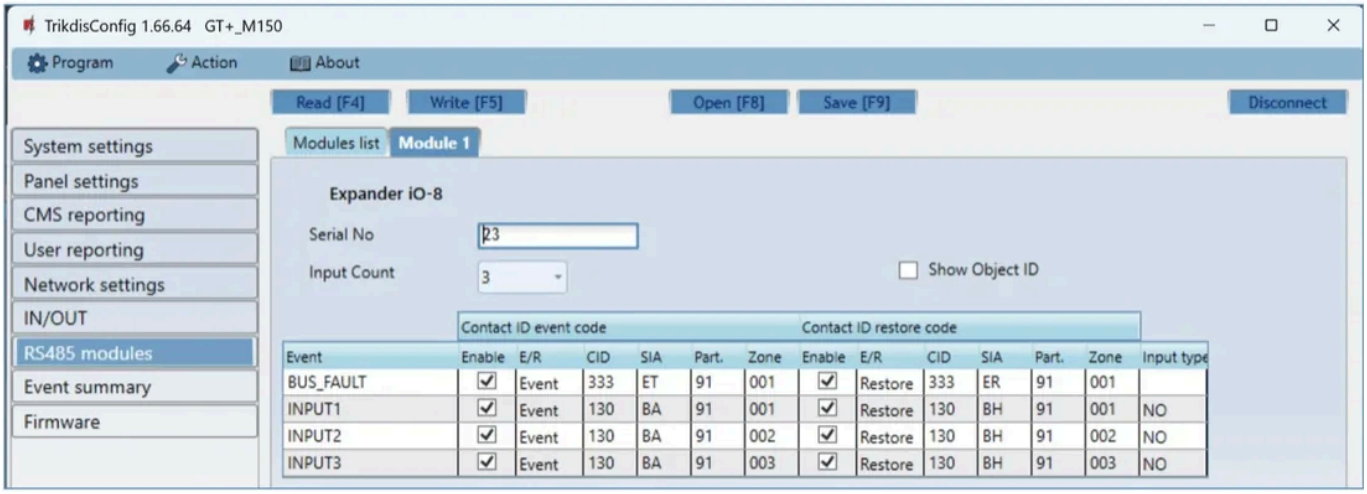


Figura 54. TrikdisConfig – RS485 modules, scheda Module 1 (iO-8): Input Count, Show Object ID, e gli eventi BUS_FAULT, INPUT1–INPUT3 con codice CID e SIA, con l'area 91.

- **Input Count** – quanti morsetti devono essere ingressi (IN); gli altri saranno uscite (OUT). Il ruolo delle uscite (inserimento / disinserimento o comando di un dispositivo) si imposta direttamente nell'app Protegus 2.
- Nella tabella puoi assegnare un codice di evento e di ripristino al guasto del bus (**BUS_FAULT**, Contact ID 333) e agli ingressi (**INPUTx**, 130); quando l'ingresso viene attivato, il comunicatore invia un evento con il codice impostato al ricevitore della centrale di vigilanza e a Protegus 2. Le colonne delle righe dell'evento (Contact ID event code) e del ripristino (Contact ID restore code): **Enable** (abilitazione), **E/R** (Event o Restore), **CID** (codice Contact ID), **SIA** (codice SIA), **Part.** (l'area – dipende automaticamente dal numero d'ordine del modulo: 91 per il modulo 1, 94 per il modulo 4), **Zone** (il numero della zona).
- **Object ID** – per l'ingresso si può indicare anche un codice impianto diverso da quello del comunicatore (la colonna compare spuntando **Show Object ID**).
- **Input type** – il tipo di ingresso: NO, NC o EOL.

6.9 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.

Messaggio	Contact ID	Quando viene generato
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**.

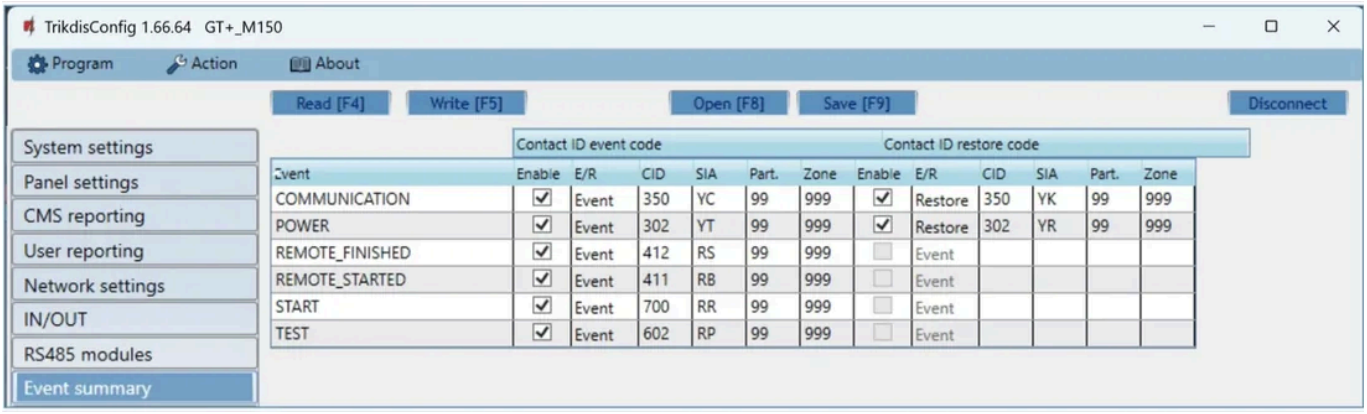


Figura 55. TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo con codice CID e SIA (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

Nell'elenco del GT e del GT+ compaiono i messaggi **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** e **TEST**, ciascuno anche con il codice SIA. Il messaggio COMMUNICATION indica un guasto della connessione tra la centrale e il comunicatore: con il collegamento al bus dati o seriale il comunicatore lo rileva direttamente (il LED TROUBLE lampeggia 7 volte).

6.10 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**.



Figura 56. TrikdisConfig – il pulsante Restore del gruppo Default settings.

Le impostazioni di fabbrica possono essere ripristinate anche sul dispositivo, senza computer: con l'alimentazione accesa premi e tieni premuto il pulsante **RESET** sul circuito stampato (paragrafo 1.4) **per 10 secondi**, finché i LED NETWORK, POWER e TROUBLE si spengono e poi il LED POWER si accende. A quel punto rilascia il pulsante: le impostazioni di fabbrica sono state ripristinate.

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.

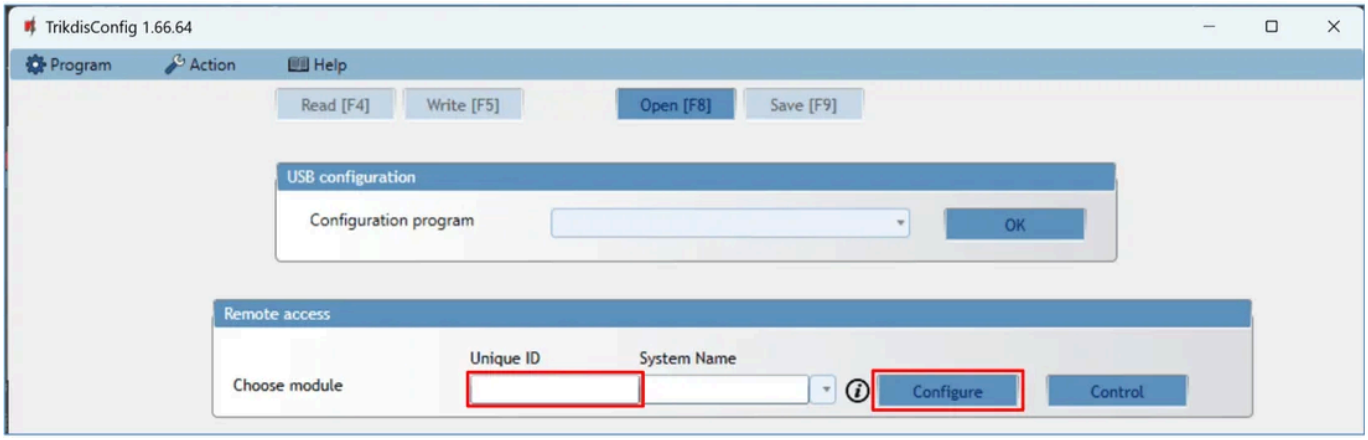


Figura 57. TrikdisConfig – il gruppo Remote access: il campo Unique ID, l'elenco System name e il pulsante Configure.

L'identificativo univoco del GT e del GT+ è l'**IMEI**; si legge sull'etichetta del dispositivo e sull'adesivo della confezione. Per l'accesso a distanza la scheda SIM deve essere attiva, con il codice PIN inserito o la richiesta del PIN disattivata; nella scheda **User reporting** → **PROTEGUS Cloud** deve essere spuntato **Enable connection** (paragrafo 6.5); il LED **POWER** deve essere verde fisso, il LED **NETWORK** verde fisso e lampeggiare in giallo.

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.
6. **Centrale DSC con collegamento Keybus + TIP/RING (GT+).** Inserisci il sistema e provoca un allarme della zona incendio. La centrale di vigilanza deve ricevere l'evento con il codice Contact ID corrispondente al tipo di zona (ad esempio E110 – allarme incendio), non come allarme generico (E130).

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.

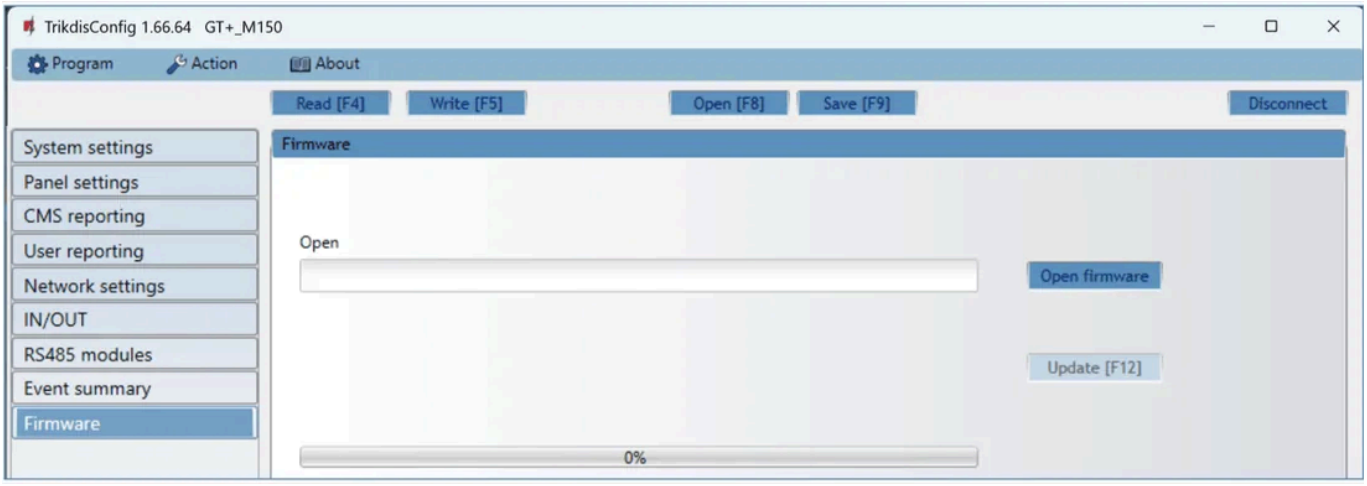


Figura 58. TrikdisConfig – pagina Firmware: pulsante Open firmware, pulsante Update [F12] e indicatore di avanzamento.

Per l'aggiornamento serve una connessione Internet. Un antivirus, un firewall o impostazioni restrittive di accesso a Internet possono impedire l'aggiornamento automatico del firmware; in questo caso bisogna modificare le impostazioni dell'antivirus. Per il collegamento Keybus + TIP/RING delle Paradox SP / SP+ / MG / MG+ (paragrafo 3.3.4) serve un firmware almeno 1.21.

10. Ricerca guasti 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 non si accende – nessuna rete

1. Osserva i lampeggi del LED **TROUBLE**: 1 = nessuna SIM, 2 = PIN errato, 3 = manca l'APN, 4 = non riesce a registrarsi sulla rete mobile, 5 = non riesce a connettersi alla rete dati (paragrafo 1.6).
2. Verifica che la scheda SIM sia attiva, abbia il servizio dati e sia ben inserita nell'alloggiamento.
3. Se sulla scheda è attiva la richiesta del PIN, inserisci il PIN nella scheda **Network settings → SIM1**, oppure disattiva la richiesta del PIN con un telefono.
4. Verifica l'APN (paragrafo 2.2): con le schede IoT / M2M l'operatore fornisce un APN a parte.
5. Verifica l'antenna: è avvitata, non è in un contenitore metallico, il livello del segnale è adeguato (il LED NETWORK lampeggia in giallo almeno 3 volte; paragrafi 1.6 e 3.2).

C'è la 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: verifica l'indirizzo del ricevitore, la porta, l'impostazione TCP/UDP, il protocollo e la chiave di cifratura (**CMS reporting**).
2. Se il ricevitore è indicato con un nome di dominio, verifica l'impostazione DNS (**Network settings** → **SIM1** → **DNS 1, DNS 2**).
3. Controlla che il piano dati della scheda SIM non blocchi la porta necessaria (alcune schede M2M consentono solo determinati indirizzi).

Il LED TROUBLE lampeggia 7 volte – nessuna connessione con la centrale

1. Con il collegamento al bus dati o seriale verifica i fili CLK e DATA, e che nel campo **Panel settings** → **Security panel model** sia selezionato il modello della centrale collegata (paragrafo 6.3).
2. Con una centrale Paradox controlla che la porta seriale non sia bloccata (paragrafo 4.1.2); con le centrali Texecom e Paradox la **Security panel PC download password** deve coincidere con quella impostata nella centrale.
3. Con il collegamento alla linea telefonica il combinatore della centrale deve essere attivo, in modalità DTMF, con formato Contact ID e con un numero di telefono impostato (paragrafo 4.2), e il **Communication protocol** deve essere AUTO (GT: Dual tone).

Il LED TROUBLE lampeggia 8 volte – ICCID non corrispondente

Il numero indicato nel campo **Network settings** → **SIM1** → **SIM ICCID** non corrisponde all'ICCID della scheda SIM inserita: il dispositivo funziona solo con la scheda indicata. Rimetti la scheda originale, oppure modifica (cancella) l'ICCID; con **Hard ICCID lock** riavvia il dispositivo dopo la modifica (paragrafo 6.6).

DSC: ogni allarme arriva come allarme generico E130

Se collegato solo al Keybus, il comunicatore riceve dalla centrale lo stato delle zone, ma non il tipo di zona, perciò trasmette ogni allarme con il codice E130 (paragrafo 3.3.1). Se la centrale di vigilanza si aspetta il codice corrispondente al tipo di zona (ad esempio incendio: E110): collega il **GT+**, oltre che al Keybus, anche ai morsetti TIP/RING, e programma il combinatore della centrale (paragrafi 3.3.2 e 4.1.1). Il GT non ha questo doppio collegamento; con il GT i codici propri della centrale vengono inviati tramite il combinatore della centrale, solo con il collegamento TIP/RING, ma allora non c'è controllo diretto e per l'inserimento serve una zona chiave (paragrafo 3.4).

Paradox: la porta seriale è bloccata, oppure non c'è connessione

Sulle centrali Paradox più recenti (SP+, MG+, EVOHD+) la porta seriale può essere bloccata di fabbrica; lo sblocco è descritto nel paragrafo 4.1.2 e nell'articolo Sblocco della porta seriale bloccata sulle centrali d'allarme Paradox. Con le centrali Spectra SP / SP+ e Magellan MG / MG+ si può usare, invece della porta seriale, anche il collegamento Keybus + TIP/RING (paragrafo 3.3.4), che non richiede lo sblocco, ma il firmware del comunicatore deve essere almeno 1.21 (capitolo 9).

Non riesco a inserire da Protegus 2

1. Con il controllo diretto, **Panel settings** → **Remote Arm/Disarm** deve essere spuntato e la centrale deve essere impostata secondo il paragrafo 4.1 (Paradox: password PC, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: le impostazioni descritte). Dalla tabella del paragrafo 1.3 verifica se la centrale è davvero a controllo diretto.
2. Con l'inserimento tramite zona chiave (paragrafo 3.4) il morsetto deve essere **OUT** nella pagina **IN/OUT**, la zona della centrale deve essere una zona chiave e in Protegus 2 l'uscita deve essere assegnata all'area, nella stessa modalità della centrale (a impulso o bistabile; paragrafo 5.2).
3. Protegus 2 mostra lo stato dell'area in base agli eventi di inserimento e disinserimento della centrale: la centrale deve trasmetterli (Opening/Closing).

Protegus 2 non vede il dispositivo

1. Nella scheda **User reporting** → **PROTEGUS Cloud** deve essere spuntato **Enable connection**.
2. Durante l'aggiunta bisogna inserire il **PROTEGUS Cloud access Code** impostato nel dispositivo; se hai cambiato il codice in TrikdisConfig, aggiornalo anche nell'app.
3. Inserisci l'IMEI esattamente, copiandolo dall'etichetta del dispositivo o dall'adesivo della confezione (oppure leggi il codice QR).
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, lampeggia in giallo) e la connessione Protegus deve essere abilitata (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** non deve superare i 5 minuti: il PING mantiene la connessione necessaria per l'accesso a distanza.
3. Verifica la password dell'amministratore o dell'installatore.

Ho dimenticato la password

Con TrikdisConfig non è possibile, perché anche il ripristino richiede la password. È possibile invece con il pulsante **RESET** del dispositivo (paragrafo 6.10): con l'alimentazione accesa, tienilo premuto per 10 secondi. Tutte le impostazioni vengono cancellate.

GT o GT+ – quale serve?

Collegamento, configurazione e funzionamento delle due versioni sono identici; le differenze sono riassunte nella tabella del paragrafo 1.2. Il GT+ funziona anche con alimentazione 10–32 V DC (anche nei sistemi a 24 V), e con le centrali DSC supporta anche il collegamento Keybus + TIP/RING, così gli eventi vengono inviati con i codici Contact ID propri della centrale. Se queste funzioni non servono, il GT fa la stessa cosa.

Quanto traffico dati usa il dispositivo?

I messaggi di evento e i PING sono molto piccoli; il traffico dipende soprattutto dal periodo del PING e dalla frequenza dei rapporti di test. In un tipico sistema domestico il traffico mensile resta in genere sotto i 10 MB. Il valore esatto dipende dalle impostazioni e dall'unità di fatturazione dell'operatore, perciò 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.

- L'installazione e la manutenzione delle apparecchiature di sicurezza possono essere eseguite solo da un installatore qualificato.
- Prima dell'installazione leggi il manuale; ignorare le istruzioni può causare malfunzionamenti o guasti dell'apparecchiatura.
- Prima del collegamento, a ogni collegamento elettrico e prima di ogni intervento di assistenza, scollega l'apparecchiatura dall'alimentazione.
- Modifiche, trasformazioni e riparazioni non autorizzate dal produttore invalidano la garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare il dispositivo divenuto inutilizzabile e i suoi componenti nei rifiuti domestici. Il simbolo del bidone barrato (RAEE) sul dispositivo indica che va consegnato separatamente, come rifiuto elettronico.

Vedi anche

- Motore di ricerca della compatibilità – quale comunicatore Trikdis e quale collegamento sono adatti alla tua centrale d'allarme.
- Comunicatore Trikdis + centrale d'allarme DSC: breve guida per l'installatore – i passaggi del collegamento DSC in breve.
- Comunicatore Trikdis + centrale d'allarme Paradox: breve guida per l'installatore – i passaggi del collegamento Paradox in breve.
- DSC PowerSeries NEO e comunicatori Trikdis: compatibilità e soluzioni – perché la NEO non può essere collegata al bus dati, e qual è la soluzione.
- Sblocco della porta seriale bloccata sulle centrali d'allarme Paradox – lo sblocco della porta seriale delle centrali SP+, MG+ ed EVOHD+.
- Inserimento a distanza con zona chiave dall'app Protegus 2 – i dettagli e le insidie dell'inserimento con zona chiave.
- Impostazione dell'APN – elenco degli operatori mobili europei – gli APN degli operatori, anche per le schede IoT / M2M.
- Documentazione in inglese: docs.trikdis.com – nella pagina del GT e del GT+ si trova anche la tabella di conversione dei codici Contact ID → SIA (allegato).

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

Prodotti correlati

Trikdis GT 4G comunicatore intelligente | **Trikdis GT+ 4G comunicatore intelligente**

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-gt