Comunicatore GET – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente del comunicatore Ethernet + 4G Trikdis GET: collegamento alla centrale d'allarme, impostazione LAN e SIM in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2.



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

Indice

1. Panoramica

- 1.1 A cosa serve e come funziona
- 1.2 Versioni: GET, 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

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

3. Installazione e collegamento

- 3.1 Le fasi dell'installazione
- 3.2 Posizionamento nel contenitore della centrale, antenna
- 3.3 Collegamento alla centrale d'allarme
  - 3.3.1 DSC – bus dati (Keybus)
  - 3.3.2 Paradox – porta seriale
  - 3.3.3 Paradox SP/MG – Keybus e TIP/RING
  - 3.3.4 UTC Interlogix (Caddx) – bus dati
  - 3.3.5 Texecom – porta seriale
  - 3.3.6 InnerRange Inception
  - 3.3.7 InnerRange Integriti
  - 3.3.8 Honeywell Vista – bus dati
  - 3.3.9 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 Accensione e primo controllo
- 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 della Honeywell Vista
  - 4.2.2 Il combinatore della UTC Interlogix (Caddx) NX

5. Controllo a distanza con l'app Protegus 2

- 5.1 Aggiunta del dispositivo
- A rendszer létrehozása a Protegus 2 alkalmazásban
- 5.2 Inserimento e disinserimento con un'uscita

5.3 Inserimento e disinserimento dall'app

6. Le impostazioni in dettaglio

6.1 Connessione al comunicatore

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Canali verso il ricevitore (CMS settings)

6.4.2 Test, PING e ordine delle connessioni

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 e SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Ripristino delle impostazioni di fabbrica

7. Programmazione a distanza

8. Verifica del funzionamento del comunicatore

9. Aggiornamento del firmware

10. Risoluzione dei problemi e domande frequenti

11. Norme di sicurezza

Vedi anche

1. Panoramica

Il GET è il **comunicatore Ethernet + 4G** di Trikdis: inoltra gli eventi della centrale d'allarme, tramite la rete locale cablata (LAN) o la rete mobile, alla centrale di vigilanza e all'app Protegus 2. Si collega 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 (TIP/RING) di qualsiasi centrale** che invii gli eventi in formato Contact ID con toni DTMF. Il comunicatore inoltra 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 si possono usare anche contemporaneamente. Questo manuale è stato scritto per il comunicatore GET con modem LTE (4G); le differenze tra GET, GT e GT+ 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, sulla rete cablata o sulla rete mobile, al ricevitore software o hardware Trikdis (protocollo TRK8; questi ricevitori collaborano con qualsiasi software di vigilanza), a un ricevitore SIA DC-09 o a un ricevitore SUR-GARD (TL150). Verso un ricevitore SUR-GARD converte i codici Contact ID ricevuti dalla centrale in codici SIA; la tabella di conversione si trova nell'appendice della documentazione in inglese del dispositivo. 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 un canale parallelo gli eventi vanno contemporaneamente a due ricevitori. Puoi stabilire l'ordine dei percorsi di connessione – LAN, SIM1, SIM2: se il percorso principale non funziona, il comunicatore passa al percorso di riserva (paragrafo 6.4.2). 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. Il GET non invia notifiche via SMS né chiamate: le notifiche arrivano tramite l'app Protegus 2.
- **Comanda direttamente la centrale.** 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 tastiera – non serve una zona chiave.
- **Ha ingressi e uscite propri.** Due morsetti I/O a doppia funzione possono essere usati come ingressi (IN) o come uscite comandabili (OUT); di fabbrica sono entrambi uscite. Le uscite si possono comandare dall'app Protegus 2. I morsetti **A 485** e **B 485** non sono usati sul GET; al GET non si può collegare alcun modulo di espansione RS485.
- **Si configura con due strumenti.** Le impostazioni si possono fare con il programma TrikdisConfig per Windows (via cavo USB-C o a distanza) e – con firmware 1.08 o successivo – anche dall'app Protegus 2 (Settings → Advanced settings). Le impostazioni possono essere salvate in un file e scritte in altri comunicatori. Ci sono due livelli di accesso: quello dell'amministratore della centrale di vigilanza e quello dell'installatore. Il comunicatore si può configurare anche a distanza e anche il suo firmware si può aggiornare a distanza.

La struttura del sistema è mostrata nella figura seguente: la centrale d'allarme si collega al comunicatore, il comunicatore raggiunge Internet in due modi – tramite la rete mobile (LTE) o tramite il router (LAN) – 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.

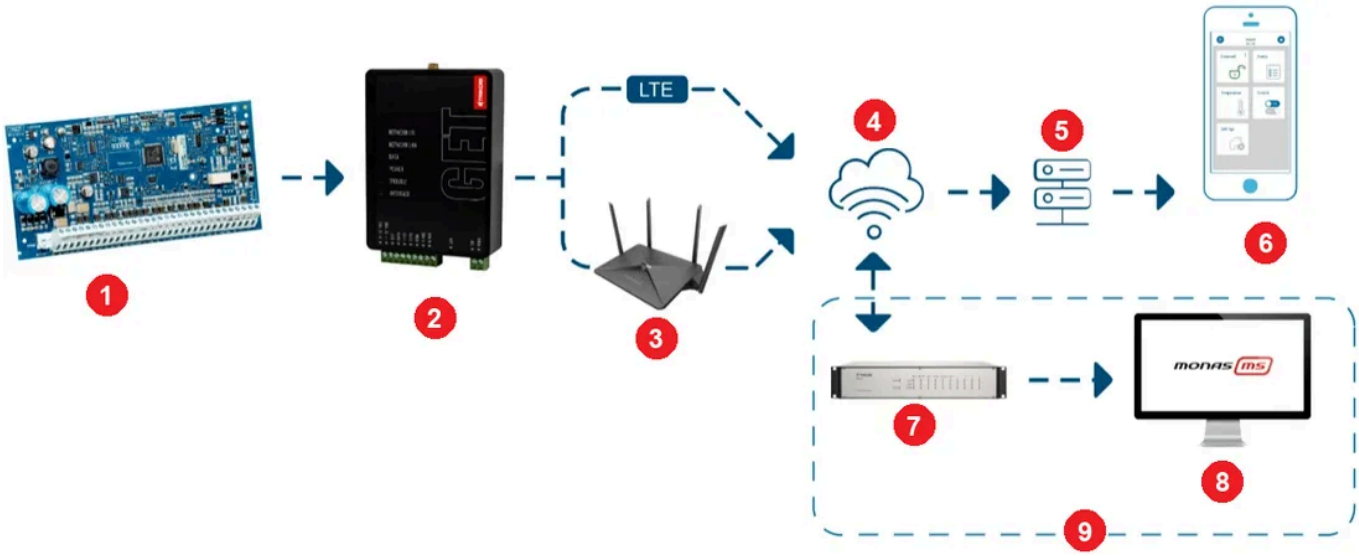


Figura 1. La posizione del comunicatore nel sistema: centrale d'allarme → GET → rete mobile (LTE) o router (LAN) → Internet → ricevitore della centrale di vigilanza e server Protegus → app Protegus 2.

- 1 centrale d'allarme («Alarm panel»)
- 2 comunicatore LTE GET («LTE communicator»)
- 3 router («Router»)
- 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 stazione di vigilanza dell'istituto di vigilanza («Monitoring station in security company») – nel riquadro tratteggiato

1.2 Versioni: GET, GT e GT+

Il GET è il fratello con porta Ethernet dei comunicatori GT e GT+: il collegamento e la programmazione della centrale d'allarme, la gamma delle centrali compatibili, il modem, i protocolli di trasmissione e l'uso di Protegus 2 sono identici, perciò anche l'ordine dei capitoli dei manuali dei tre comunicatori è lo stesso. Le differenze sono riassunte nella tabella seguente.

	GET	GT	GT+
Connessione di rete	**LTE (4G) ed Ethernet (LAN, RJ45)**; l'ordine dei percorsi di connessione è impostabile (Main / Backup / Backup 2: LAN, SIM1, SIM2; paragrafo 6.4.2)	LTE (4G)	LTE (4G)
Scheda SIM	**2 slot nano-SIM** (SIM1, SIM2); si possono inserire una o due schede	1 nano-SIM	1 nano-SIM
Tensione di alimentazione	10–18 V DC	10–18 V DC	10–32 V DC

	GET	**GT**	**GT+**
Assorbimento	al massimo 100 mA a riposo, 300 mA durante l'invio di dati	al massimo 100 / 200 mA	al massimo 100 / 200 mA
Dimensioni, peso	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g
Morsetti	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; presa **LAN** (RJ45) separata e TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Impostazione di fabbrica dei morsetti I/O	uscita (OUT)	ingresso (IN, NO)	ingresso (IN, NO)
Bus RS485, espansione iO-8	i morsetti A 485 / B 485 **non sono usati**; non si può collegare alcuna espansione	al massimo 4 iO-8	al massimo 4 iO-8
LED	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (non usato)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Lampeggi del LED TROUBLE	1 = collegamento fisico LAN (cavo), 2 = guasto SIM1, 3 = guasto SIM2, 7 = centrale	1–8 (SIM, PIN, APN, rete, ricevitore, centrale, ICCID)	1–8
SMS e chiamate	nessuna notifica SMS, nessun comando SMS e nessuna chiamata: notifiche e comandi passano da Protegus 2	notifiche via SMS e chiamata, comandi SMS	notifiche via SMS e chiamata, comandi SMS
Centrale DSC collegata contemporaneamente al bus dati e ai morsetti TIP/RING	no	no	sì
Impostazione del collegamento TIP/RING (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (si può scegliere anche **3. MANUAL**)
Configurazione dall'app Protegus 2	sì (Advanced settings, dal firmware 1.08)	TrikdisConfig	TrikdisConfig
Memoria eventi	60 eventi	dato non disponibile	dato non disponibile
Messaggi interni (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	come il GT
Modem, protocolli di trasmissione (TRK8, DC-09, TL150), cifratura, centrali compatibili, schemi di collegamento, Protegus 2	identici	identici	identici

Tutti e tre i comunicatori sono prodotti con gli stessi tre tipi di modem; per l'Europa è adatta 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 si possono collegare al comunicatore direttamente, tramite bus dati o porta seriale. La colonna «Comando diretto» indica se l'utente può inserire e disinserire da Protegus 2 con il proprio codice tastiera senza ulteriori 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	Comando diretto
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	bus dati (Keybus)	sì
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 della centrale)	no
Honeywell	Ademco Vista-15, Vista-20, Vista-48	bus dati	sì

- Il firmware delle centrali **Paradox** comandate direttamente 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+, invece che alla porta seriale, si possono collegare contemporaneamente al bus dati (Keybus) e ai morsetti TIP/RING – in questo caso non serve lo sblocco a pagamento, ma il firmware del comunicatore deve essere almeno 1.21 (paragrafo 3.3.3).
- 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 frontale si sgancia a scatto e la morsettiera è estraibile. La presa LAN e i morsetti TIP/RING sono accessibili sul lato del contenitore, in un'apertura separata.

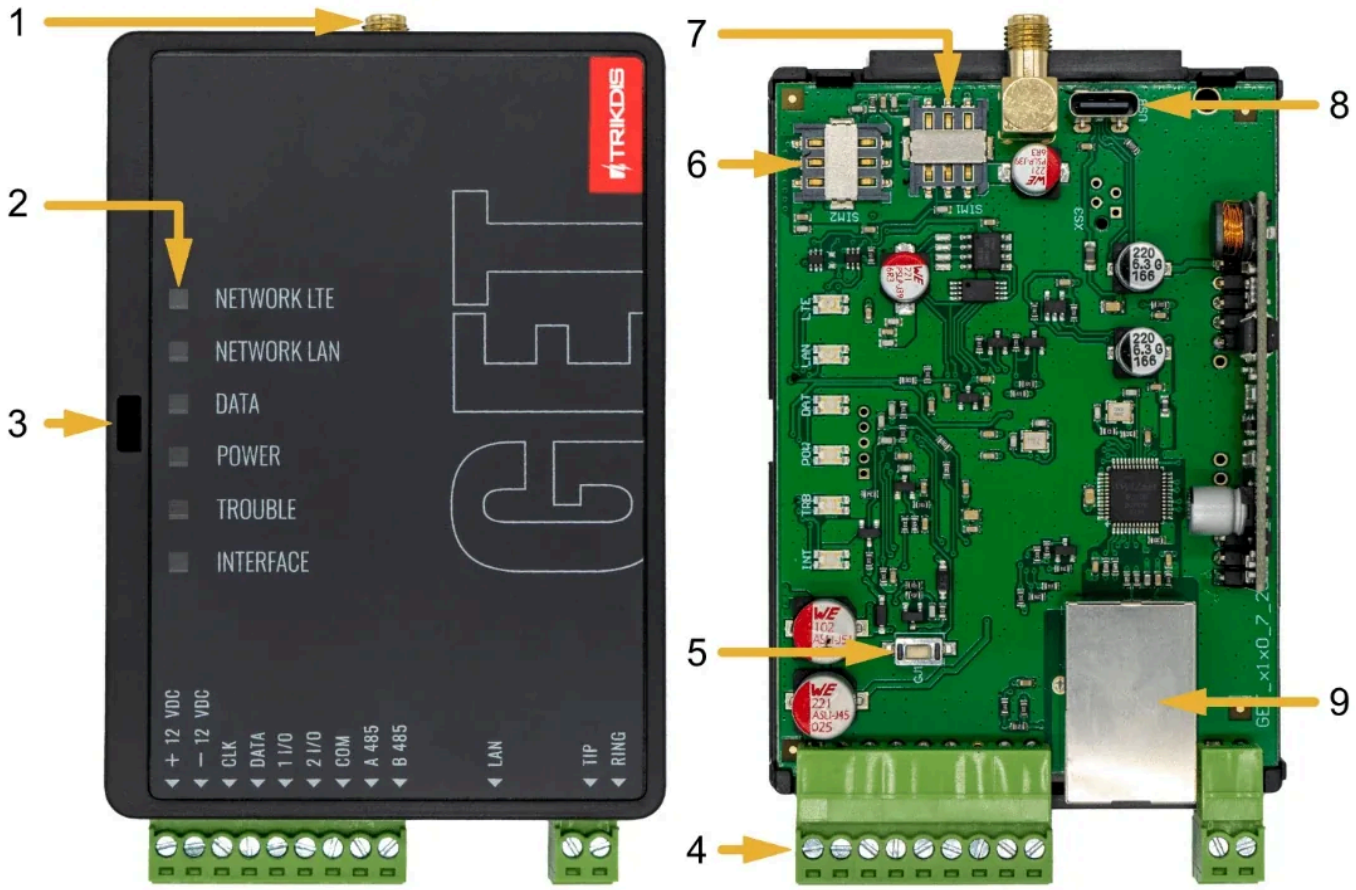


Figura 2. Le parti del comunicatore viste dal davanti (a sinistra) e con il contenitore aperto (a destra).

- 1 Connettore SMA dell'antenna mobile
- 2 LED di segnalazione (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Fessura che aiuta a sganciare il frontale
- 4 Morsettiera estraibile per i collegamenti esterni
- 5 Pulsante RESET
- 6 Slot della scheda SIM2
- 7 Slot della scheda SIM1
- 8 Presa USB-C per la programmazione
- 9 Presa RJ45 Ethernet (LAN)

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

1.5 Morsetti

Morsetto	Funzione
+12 VDC	Alimentazione, positivo: +10–18 V DC

Morsetto	Funzione
–12 VDC	Alimentazione, 0 V
CLK	Bus seriale o bus dati (clock) per il collegamento diretto della centrale
DATA	Bus seriale o bus dati (dati) per il collegamento diretto della centrale
1 I/O	Ingresso/uscita 1 (impostazione di fabbrica: uscita, OUT)
2 I/O	Ingresso/uscita 2 (impostazione di fabbrica: uscita, OUT)
COM	Punto comune (negativo) per ingressi e uscite
A 485	Non usato
B 485	Non usato (la coppia di A 485)
LAN	Presa RJ45 Ethernet (rete locale)
TIP	Morsetto TIP del combinatore telefonico della centrale d'allarme
RING	Morsetto RING del combinatore telefonico della centrale d'allarme

Negli schemi di collegamento i morsetti di alimentazione sono indicati con **+DC** e **–DC** (sul dispositivo +12 VDC / −12 VDC) e i morsetti RS485 con **A RS485** / **B RS485** (sul dispositivo A 485 / B 485). La legenda della morsettiera è riportata anche sul frontale.

1.6 Segnalazioni LED

I LED del frontale sono lo strumento più importante per la messa in servizio e la ricerca dei guasti. Leggili insieme: il POWER indica l'alimentazione, il NETWORK LTE la rete mobile, il NETWORK LAN la rete cablata, il TROUBLE i guasti; il LED INTERFACE sul GET non ha alcuna funzione.

NETWORK LTE – connessione alla rete mobile

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

NETWORK LAN – connessione alla rete cablata

Segnalazione	Significato
spento	Nessuna connessione alla rete informatica
verde fisso	Connesso alla rete informatica

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 comunicatore e 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	Guasto nel collegamento fisico della rete cablata (PHY Link) – controlla il cavo LAN
2 lampeggi rossi	Guasto della scheda SIM1
3 lampeggi rossi	Guasto della scheda SIM2
7 lampeggi rossi	Interrotta la connessione con la centrale d'allarme (bus seriale)

INTERFACE – non usato sul GET.

1.7 Dati tecnici

Parametro	Valore
Connessione di rete	LTE (4G) ed Ethernet (LAN)
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
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
Scheda SIM	2 slot nano-SIM (SIM1, SIM2)
Tensione di alimentazione	10–18 V DC
Assorbimento	al massimo 100 mA a riposo; al massimo 300 mA durante l'invio di dati

Parametro	Valore
Protocolli di trasmissione	TRK8, DC-09_2007, DC-09_2012, TL150
Cifratura	AES-128
Memoria eventi	60 eventi
Programmazione	TrikdisConfig (Windows) via cavo USB-C o a distanza; app Protegus 2 (dal firmware 1.08)
Ambiente di funzionamento	−10 … +50 °C, max. 80 % di umidità relativa (a +20 °C)
Dimensioni	113 × 70 × 25 mm
Peso	110 g

2. Messa in servizio rapida

Le impostazioni del comunicatore si possono fare con due strumenti: con il programma **TrikdisConfig** per Windows – via cavo USB-C o a distanza – e dall'**app Protegus 2** (Settings → Advanced settings). In questo capitolo descriviamo il percorso più breve: quali impostazioni servono perché il comunicatore invii gli eventi alla centrale di vigilanza e perché il sistema sia comandabile dall'app Protegus 2. Per ogni passo indichiamo il percorso sia nell'app sia in TrikdisConfig; la spiegazione dettagliata delle impostazioni si trova nel capitolo 6.

2.1 Preparativi

Cosa ti serve

Cavo USB-C per la programmazione · cavo con almeno 4 conduttori tra comunicatore e centrale · per la porta seriale Paradox un cavo CRP2.4 · cacciavite a taglio da 2,5 mm · un'antenna mobile con guadagno adeguato, se nel sito la copertura è debole · scheda SIM attiva (una o due; la richiesta del PIN si può disattivare), se usi la rete mobile · cavo Ethernet fino al router o allo switch, se usi la rete cablata · il manuale di installazione della centrale d'allarme.

Gli accessori necessari vanno ordinati separatamente dal rivenditore.

Configurazione con TrikdisConfig. Il dispositivo si configura sul banco, prima del collegamento; poi, nel sito, basta solo collegarlo.

1. Scarica e installa il software TrikdisConfig. Sul sito di Trikdis (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 a taglio: infila il cacciavite in alto, nella fessura accanto all'antenna, e fai leva verso l'esterno, poi in basso, in corrispondenza dell'apertura, verso il basso. La figura mostra anche la posizione della presa USB-C sul bordo del circuito stampato.

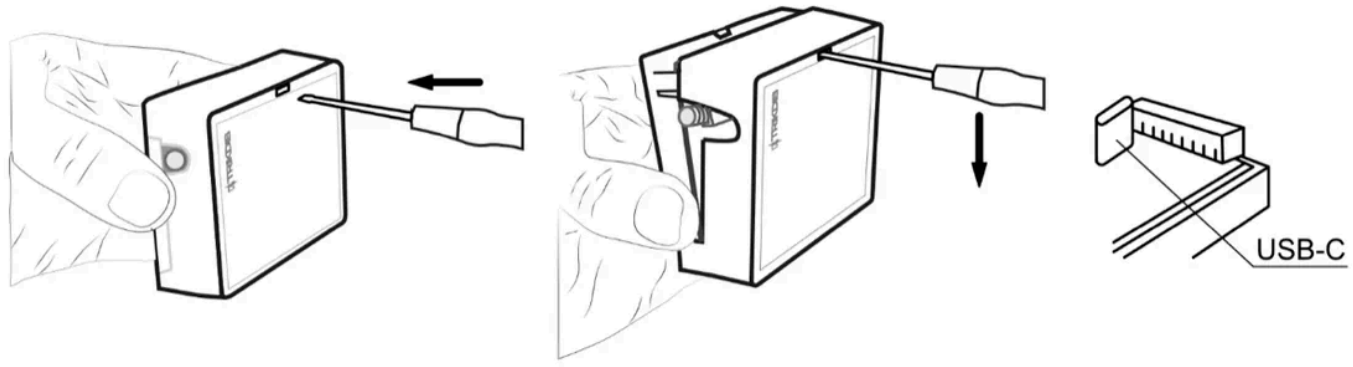


Figura 3. Sgancio del frontale con un cacciavite a taglio; il particolare ingrandito mostra la posizione della presa USB-C.

3. Inserisci la scheda nano-SIM (o le schede) nello slot, nel verso mostrato in figura: lo slot SIM1 è al centro del circuito stampato, lo SIM2 sul bordo. La scheda deve essere attiva, avere un servizio dati mobile e, se possibile, disattiva la richiesta del PIN con un telefono (così non dovrai inserire il PIN nel dispositivo). Se usi il comunicatore solo sulla rete cablata, la scheda SIM non serve.

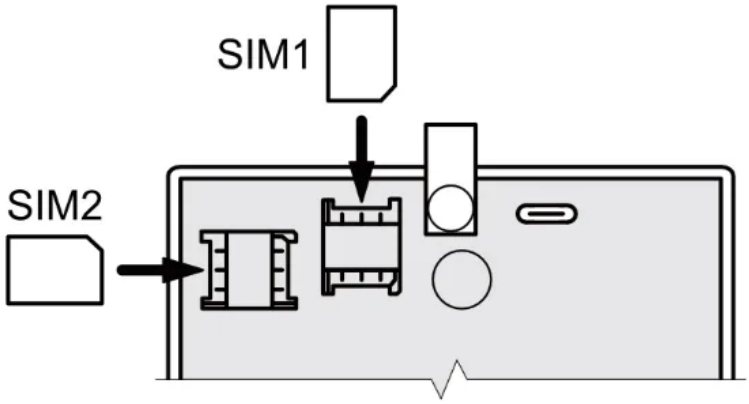


Figura 4. La posizione degli slot SIM1 e SIM2 sul circuito stampato; le frecce indicano il verso di inserimento della scheda.

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`).

Configurazione dall'app Protegus 2. Puoi configurare dall'app se il comunicatore è già online e lo hai aggiunto al tuo account Protegus (paragrafo 5.1). Se il comunicatore non riesce ancora a connettersi – per esempio perché la scheda SIM chiede il PIN o perché l'operatore richiede un altro APN –, fai la prima configurazione con TrikdisConfig.

1. Nell'app apri il sistema e vai nel menu **Settings** → **Advanced settings**.

2. La prima volta l'app ti avvisa (**Proceed with Caution**): queste impostazioni sono destinate ai professionisti. Tocca il pulsante **Accept the risk and continue**; con la spunta **Do not show this again** l'avviso non comparirà più la volta successiva.
3. L'app legge le impostazioni del comunicatore. Se chiede il **Service Access code**, inserisci il codice di accesso Protegus Cloud del comunicatore (di fabbrica `123456`).
4. Fai le impostazioni descritte sotto, poi tocca il pulsante **Write**: l'app le scrive nel comunicatore.

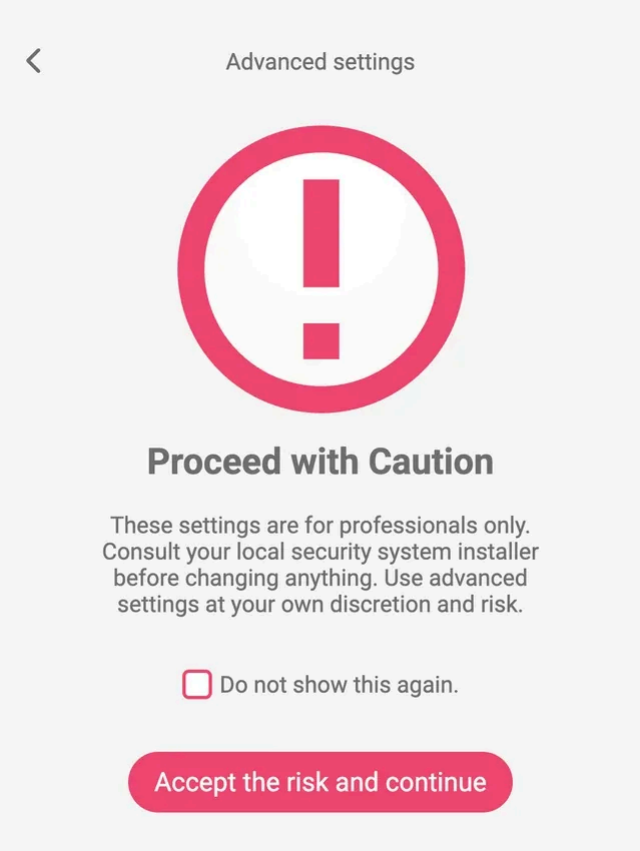


Figura 5. Protegus 2 – l'avviso visualizzato alla prima apertura di Advanced settings (Proceed with Caution) e il pulsante Accept the risk and continue.

Dall'app Protegus 2 il GET si può configurare con **firmware 1.08 o successivo** (l'aggiornamento è descritto nel capitolo 9).

2.2 Connessione all'app Protegus 2

Nell'app (Settings → Advanced settings):

1. **Panel settings** → **TLF** – se il comunicatore è collegato ai morsetti TIP/RING della centrale: il **Security panel model** deve essere **AUTO**.
2. **Panel settings** → **Serial Bus** – se il comunicatore è collegato al bus dati o alla porta seriale della centrale: nel campo **Security panel model** scegli il modello della centrale collegata.
3. Nello stesso punto attiva l'opzione **Remote Arm/Disarm**, se gli utenti vogliono comandare la centrale da Protegus 2 con il proprio codice tastiera. Compare solo con le centrali comandabili direttamente.
4. Per il comando diretto di una centrale Paradox inserisci la **PC download password**, per una centrale Texecom l'**UDL passcode**; deve coincidere con la password impostata nella centrale.
5. **User reporting** → **Cloud**: attiva l'opzione **Enabled** e cambia il **Cloud access code**, se vuoi che l'utente debba inserirlo quando aggiunge il sistema all'app (di fabbrica `123456`).

6. **Network settings** → **LAN** – se il comunicatore è collegato alla rete cablata: attiva l'opzione **Use DHCP**.
7. **Network settings** → **SIM** e **SIM2** – per ogni scheda SIM inserita: inserisci il **SIM card PIN** e l'**APN** e verifica che **DNS1** e **DNS2** funzionino con il tuo operatore.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: nei campi **Main type**, **Backup type** e **Backup type 2** imposta in quale ordine il comunicatore usa le connessioni **LAN**, **SIM** (SIM1) e **SIM2**.
9. Tocca il pulsante **Write**.

In TrikdisConfig. Per prima cosa, nella pagina **Panel settings**, indica come il comunicatore è collegato alla centrale.

Se lo colleghi all'uscita della linea telefonica (TIP/RING) della centrale: nel campo **Communication protocol** scegli il valore **AUTO**.

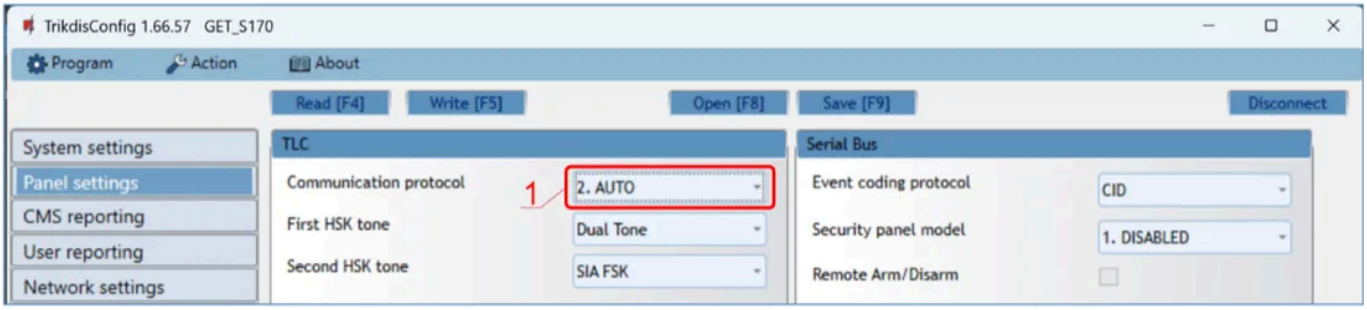


Figura 6. TrikdisConfig – Panel settings, gruppo TLC.

- 1 **Communication protocol** – con il collegamento TIP/RING **2. AUTO**.

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



Figura 7. TrikdisConfig – Panel settings, gruppo Serial bus.

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

Per il comando diretto bisogna configurare anche la centrale d'allarme – è descritto nel capitolo 4, dove trovi anche la procedura per impostare la password PC o UDL.

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

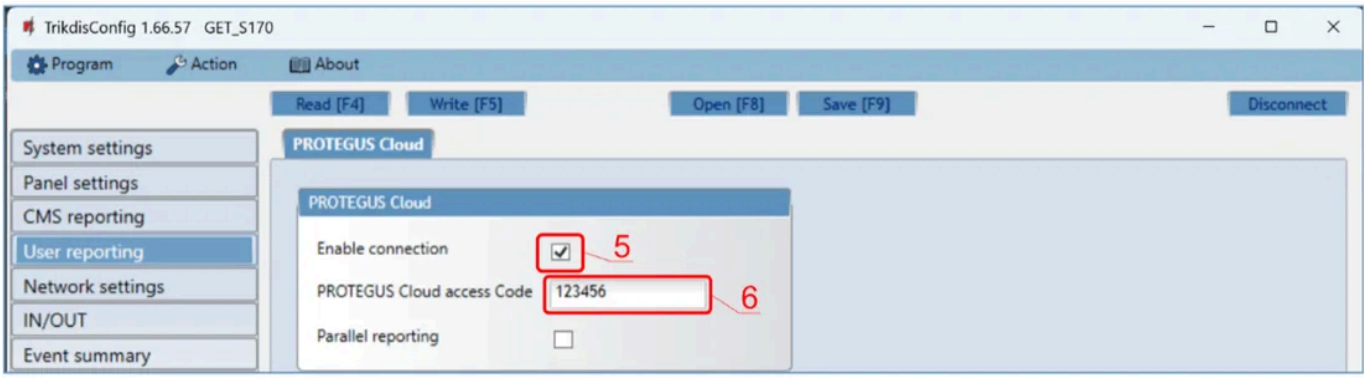


Figura 8. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- 5 **Enable connection** – spunta la casella: 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. Se in seguito modifichi il codice, devi cambiarlo anche nell'app Protegus 2.

Se il comunicatore è collegato alla rete cablata, nella pagina **Network settings**, scheda **LAN**, spunta l'opzione **Use DHCP**: il comunicatore riceve automaticamente le impostazioni di rete (subnet mask, gateway) e un indirizzo IP.

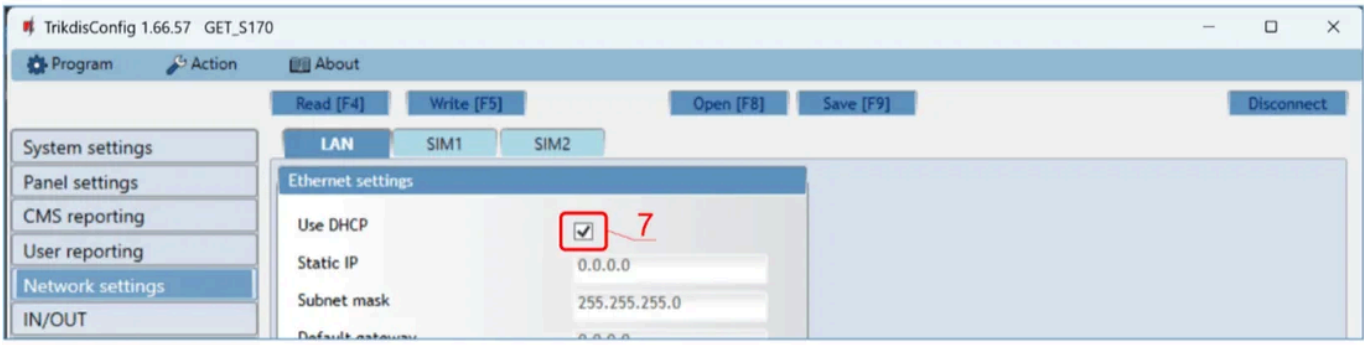


Figura 9. TrikdisConfig – Network settings, scheda LAN (Ethernet settings).

- 7 **Use DHCP** – con la spunta il comunicatore riceve automaticamente dal router l'indirizzo IP e le impostazioni di rete.

Se nel comunicatore c'è una scheda SIM (una o due schede), inserisci i dati della scheda nella scheda **SIM1** (e **SIM2**).

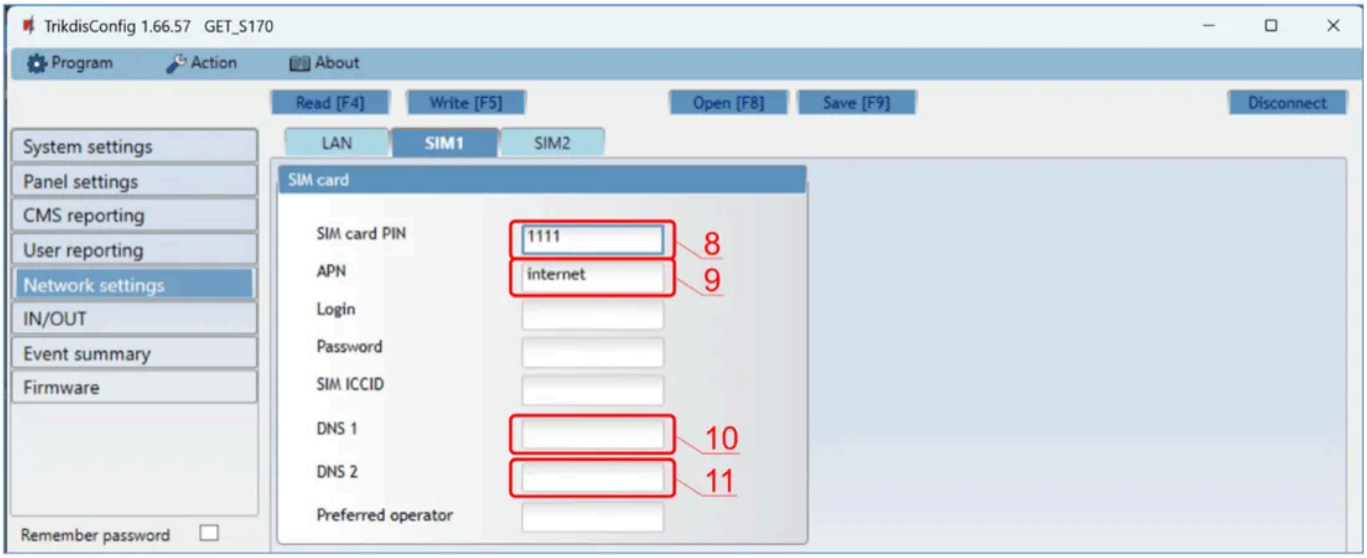


Figura 10. TrikdisConfig – Network settings, scheda SIM1.

- 8 **SIM card PIN** – il codice PIN della scheda (se la richiesta del PIN è disattivata, può restare il valore di fabbrica).
- 9 **APN** – il punto di accesso per la connessione dati dell'operatore (vedi sotto).
- 10 **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.
- 11 **DNS 2** – server dei nomi secondario (di fabbrica anch'esso di Google).

L'APN (Access Point Name) è il punto di accesso per la connessione dati dell'operatore mobile; senza di esso il dispositivo non riesce a collegarsi a Internet tramite la rete mobile. Il valore esatto si trova 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 di uso generale e funziona sulla rete di molti operatori.

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

Infine, nella pagina **CMS reporting**, scheda **Settings**, gruppo **Reporting mode**, indica l'ordine delle connessioni: è il percorso con cui il comunicatore invia i messaggi alla centrale di vigilanza e a Protegus 2.

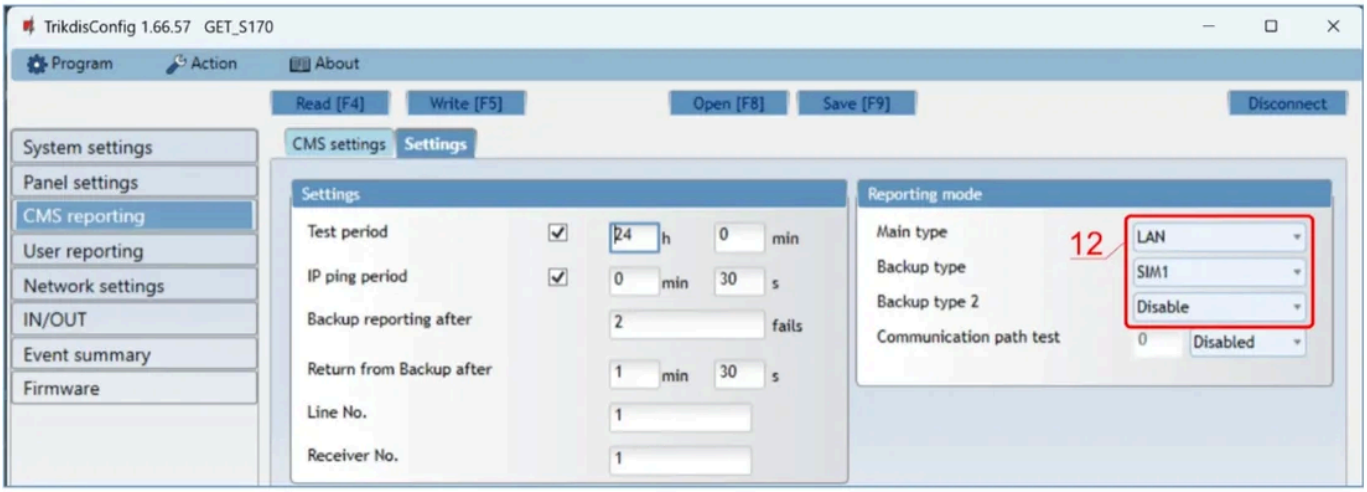


Figura 11. TrikdisConfig – CMS reporting, scheda Settings, gruppo Reporting mode (di fabbrica Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type**: la connessione principale (LAN, SIM1 o SIM2); **Backup type**: quella di riserva; **Backup type 2**: la seconda di riserva.

I tipi di connessione si indicano in ordine. Se il comunicatore non riesce a connettersi con la connessione **Main type**, passa al **Backup type**, e così via. Se la connessione di riserva ha inoltrato con successo il messaggio alla centrale di vigilanza, trascorso il tempo impostato il comunicatore tenta di tornare alla connessione principale (paragrafo 6.4.2).

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

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 comando 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

Nell'app (Settings → Advanced settings):

1. **System options → System general**: inserisci il codice impianto ricevuto dalla centrale di vigilanza (**Account No.**; 0–9, A–F; `FFFE` e `FFFF` non si possono usare). Sulla versione hardware **x1x1**, con firmware **1.31** o successivo, il codice impianto si indica per canale: **Reporting to CMS → CMS settings → Primary channel → Primary Account no.** Lo riconosci dalla schermata: se System general mostra solo il campo **Time set**, usa l'impostazione del canale.
2. **Panel settings → TLF** (collegamento TIP/RING): il **Security panel model** deve essere **AUTO**; oppure **Panel settings → Serial Bus** (collegamento al bus dati o seriale): scegli il **Security panel model**.
3. **Reporting to CMS → CMS settings → Primary channel**: attiva l'opzione **Enabled**, poi inserisci: **Communication type**: **IP**; l'indirizzo **Domain or IP** e la **Port** del ricevitore; **TCP or UDP**; **Protocol**: **TRK8** per un ricevitore Trikdis, **DC-09_2007** o **DC-09_2012** per un ricevitore universale, **TL150** per un ricevitore SUR-GARD; e la chiave di cifratura impostata nel ricevitore: con il protocollo TRK nel campo **TRK encryption key**, con DC-09 attiva l'opzione **Enable encryption key** e inserisci la **DC-09 encryption key**.
4. (Consigliato) Imposta allo stesso modo il **Backup channel** (canale di riserva).
5. **Reporting to CMS → CMS settings → Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.

6. **Network settings** → **LAN** (rete cablata): attiva l'opzione **Use DHCP**. **Network settings** → **SIM** e **SIM2** (per ogni scheda SIM): **SIM card PIN**, **APN**, e verifica i campi **DNS1**, **DNS2**.
7. Tocca il pulsante **Write**.

In TrikdisConfig. Per prima cosa, nella pagina **System settings**, inserisci il codice impianto.



Figura 12. 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 si possono usare.

Nella pagina **Panel settings** indica il collegamento della centrale, se non l'hai già fatto nel paragrafo 2.2: con il collegamento TIP/RING il **Communication protocol** deve essere **AUTO**; con il 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**, scheda **CMS settings**, nella parte **Primary channel** (canale primario), imposta i dati del ricevitore. La figura mostra la finestra prima della configurazione: il campo **Communication type** del canale primario è ancora **Disable**.

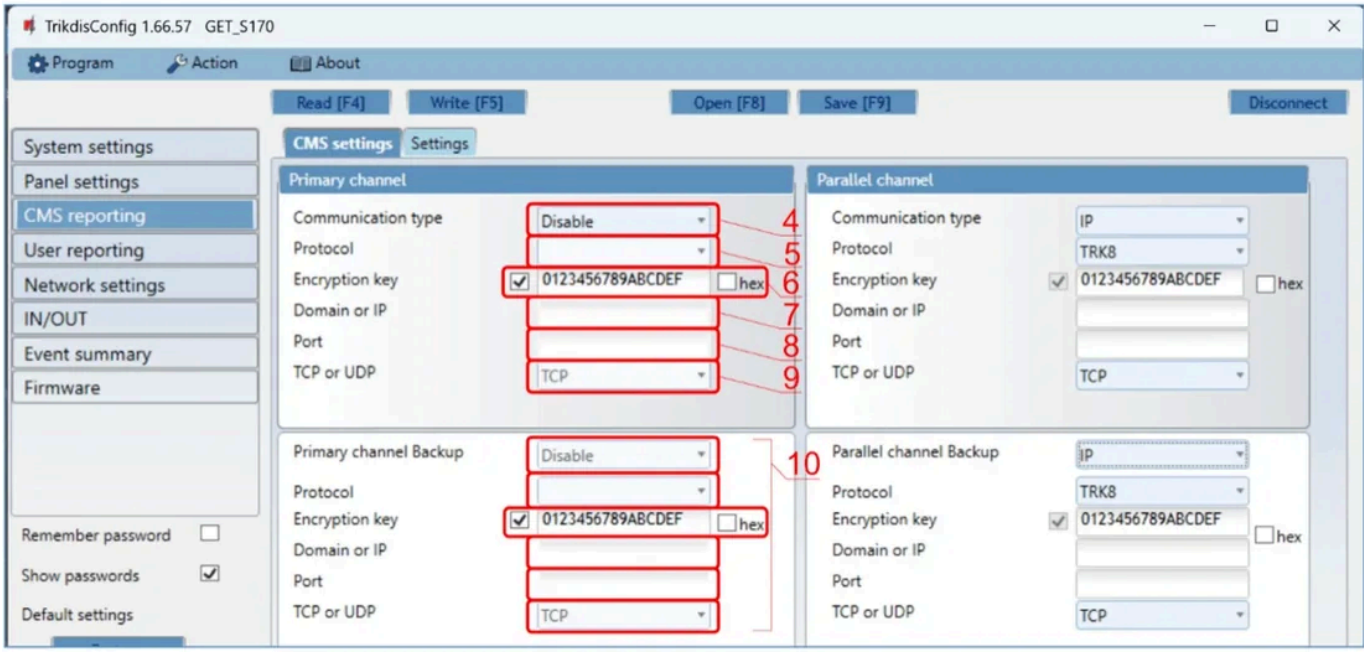


Figura 13. TrikdisConfig – CMS reporting, scheda CMS settings.

- 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 primario; compilalo allo stesso modo, è consigliato impostarlo.

Nella scheda **Settings**, gruppo **Reporting mode**, indica l'ordine delle connessioni (**Main type**, **Backup type**, **Backup type 2**), se non l'hai già fatto nel paragrafo 2.2 – lì trovi anche la figura e la descrizione del funzionamento.

Infine, nella pagina **Network settings**, inserisci i dati di rete, se non l'hai già fatto nel paragrafo 2.2: nella scheda **LAN** la spunta **Use DHCP**, nella scheda **SIM1** (e **SIM2**) i dati della scheda (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Con il protocollo **DC-09** inserisci nella scheda **Settings** anche il numero di linea e di ricevitore (**Line No.**, **Receiver No.**, paragrafo 6.4.2). Il GET trasmette alla centrale di vigilanza solo tramite connessione IP – sulla rete cablata o su Internet mobile –, non ha un canale di riserva SMS.

Al termine 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 qui 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 Le fasi dell'installazione

1. Togli il frontale (vedi il paragrafo 2.1) ed estrai la morsettiera.
2. Inserisci la scheda nano-SIM – o entrambe – nel suo slot, se non l'hai già fatto durante la messa in servizio.
3. Estrai il circuito stampato dal fondo del contenitore: apri il fermo accanto al connettore dell'antenna e solleva la scheda (vedi la figura).
4. Fissa il fondo con viti nel punto scelto (nella figura i fori per le viti sono cerchiati), oppure, come descritto nel paragrafo 3.2, con il nastro biadesivo in dotazione.
5. Rimetti il circuito stampato nel fondo e reinserisci la morsettiera.
6. Avvita l'antenna mobile.
7. Rimetti il frontale.
8. Se invii gli eventi alla centrale di vigilanza anche tramite la rete cablata (LAN), inserisci il cavo di rete nella presa LAN del comunicatore.

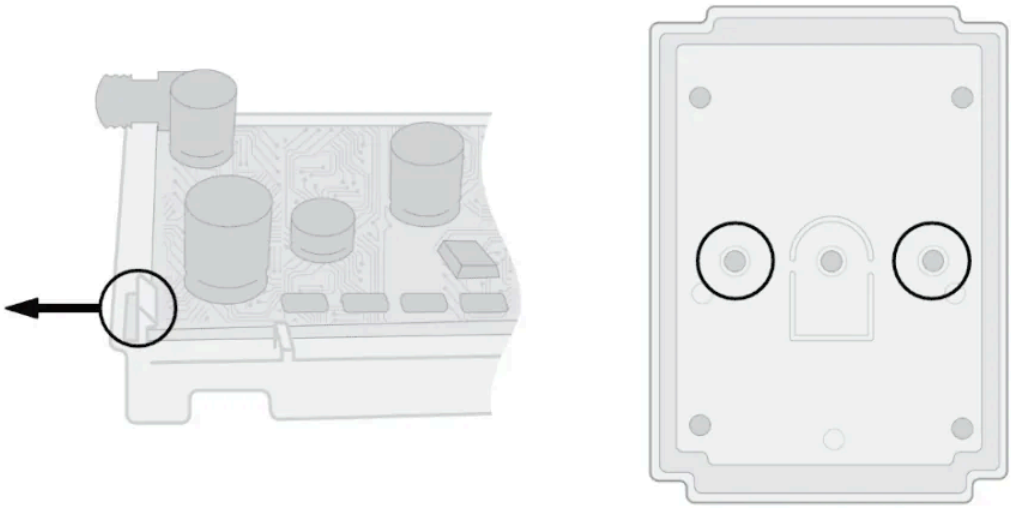


Figura 14. Estrazione del circuito stampato dal fondo (a sinistra: il fermo e la direzione di estrazione) e i fori per le viti del fondo (a destra).

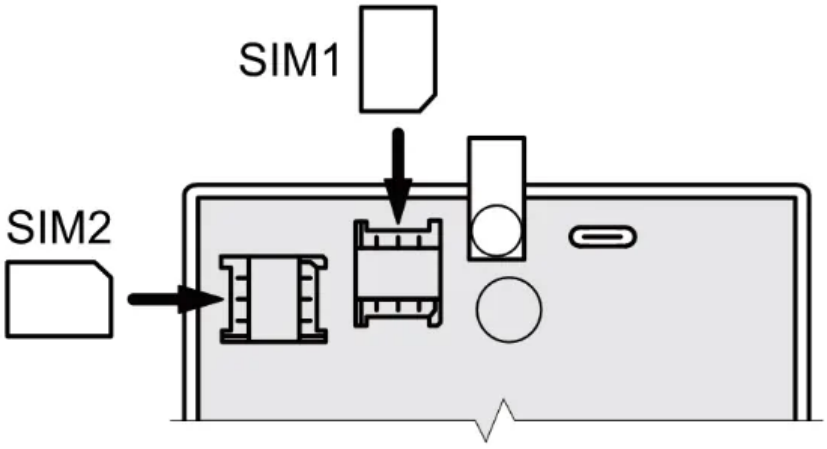


Figura 15. La posizione dei due slot SIM sul circuito stampato: SIM1 al centro della scheda, SIM2 sul bordo sinistro; le frecce indicano il verso di inserimento della scheda.

Nel comunicatore si possono inserire una o due schede SIM. La scheda deve essere attiva e, per l'uso su 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 nel contenitore della centrale, antenna

Il comunicatore va installato nel **contenitore della centrale d'allarme protetto da tamper antiapertura**. Fissalo alla parete interna di fondo del contenitore con il nastro in schiuma acrilica biadesivo di qualità industriale in dotazione: incolla il nastro su una superficie pulita e asciutta, premendo con forza, perché tenga in modo sicuro. Se il contenitore della centrale non consente questo fissaggio sicuro, il comunicatore si può montare anche in un contenitore separato protetto da tamper.

- **In un contenitore metallico** il segnale mobile si attenua molto. Se il comunicatore va nel contenitore metallico della centrale, porta l'antenna all'esterno del contenitore o usa un'antenna con cavo più lungo.
- Prima del fissaggio definitivo **verifica il livello del segnale**: il numero dei lampeggi gialli del LED NETWORK LTE in 4G deve essere almeno 3 (paragrafo 1.6). Se sono meno, cerca per l'antenna una posizione 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 di rete elettrica.
- Fai passare il cavo LAN attraverso il passacavo del contenitore fino alla presa RJ45 sul lato del comunicatore; il cavo non deve tirare sui morsetti.



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 **+12 VDC** / **–12 VDC** del comunicatore, mentre **A RS485** / **B RS485** sono i morsetti **A 485** / **B 485** (sul GET non vanno collegati). Il comunicatore riceve l'alimentazione dall'uscita di alimentazione ausiliaria (AUX) della centrale, così durante un'interruzione di corrente la batteria della centrale alimenta anche il comunicatore.

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**.

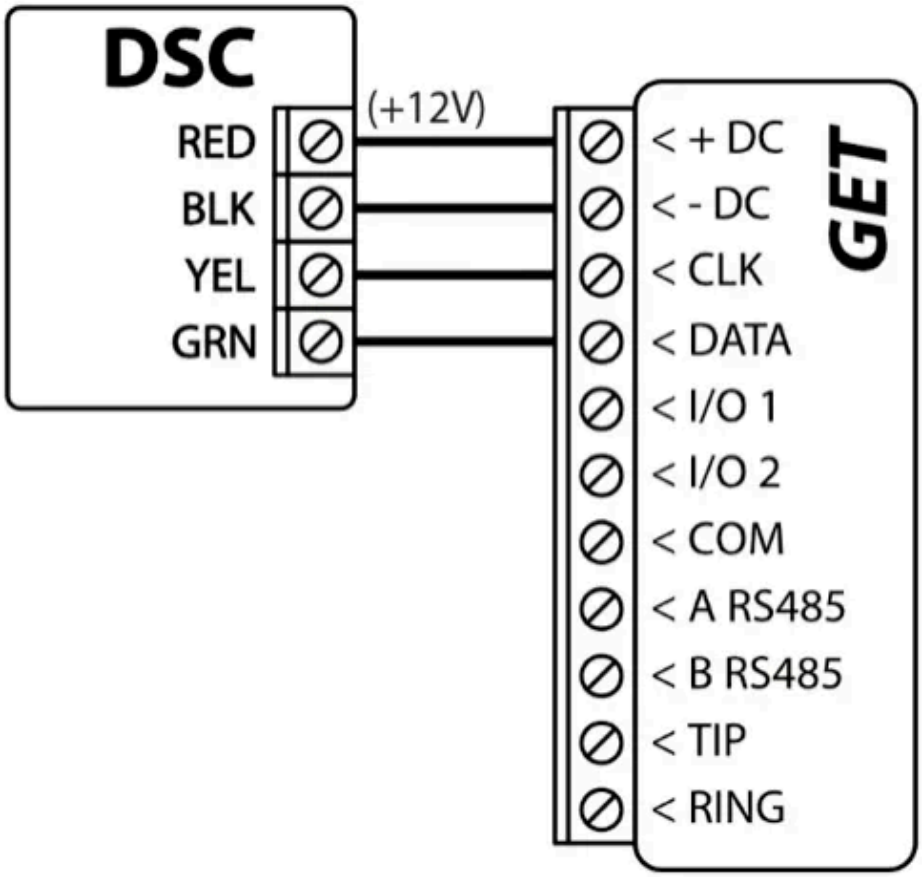


Figura 16. Collegamento di una centrale DSC al bus dati (Keybus, «Keypad bus»): RED → +DC, BLK → –DC, YEL → CLK, GRN → DATA.

Il GET gestisce la centrale DSC solo tramite il bus dati; il collegamento contemporaneo del Keybus e dei morsetti TIP/RING è disponibile solo sul comunicatore GT+. Collegato solo al Keybus, il comunicatore riceve dalla centrale lo stato generale delle zone, ma non il tipo di zona (incendio, intrusione, perdita d'acqua ecc.), perciò trasmette ogni allarme come **allarme generico, con il codice Contact ID E130**. Se alla centrale di vigilanza servono i codici propri della centrale (per esempio allarme incendio: E110), puoi inviare gli eventi con il combinatore telefonico della centrale, con il collegamento TIP/RING (paragrafi 3.3.9 e 4.2); in questo caso non c'è il comando diretto.

3.3.2 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**.

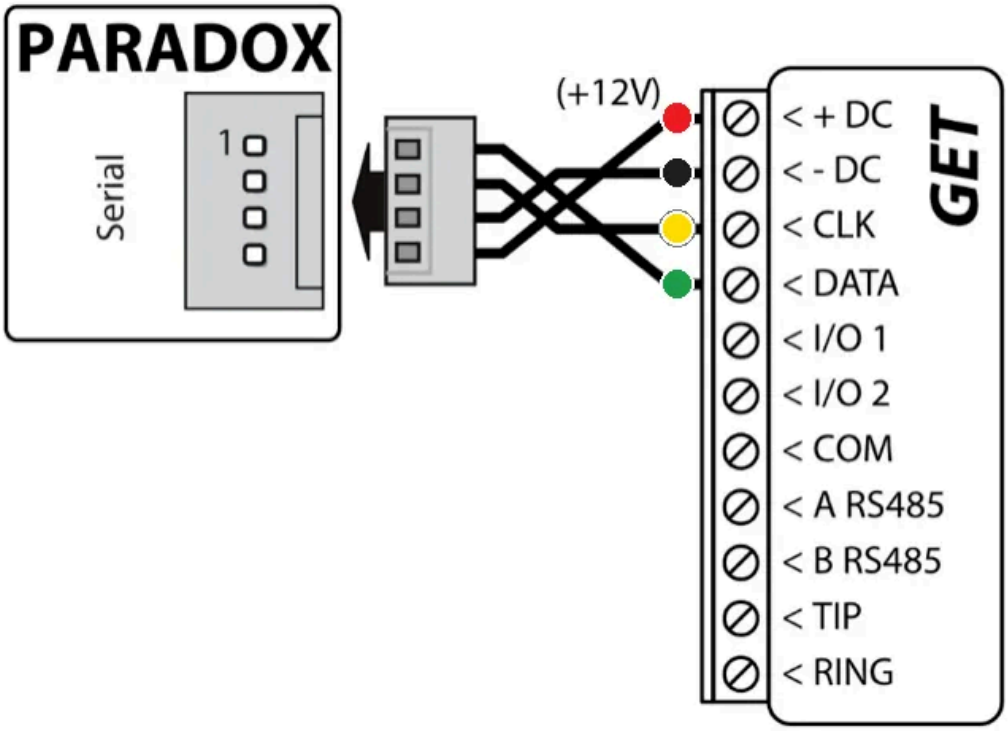


Figura 17. Collegamento di una centrale Paradox alla porta seriale con il cavo EX-CRP2.4 (da ordinare separatamente; «Use the EX-CRP2.4 cable (ordered separately)»): rosso → +DC, nero → −DC, giallo → CLK, verde → DATA.

- 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+, invece della porta seriale, si può usare anche il collegamento descritto nel paragrafo seguente.

3.3.3 Paradox SP/MG – Keybus e TIP/RING

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

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

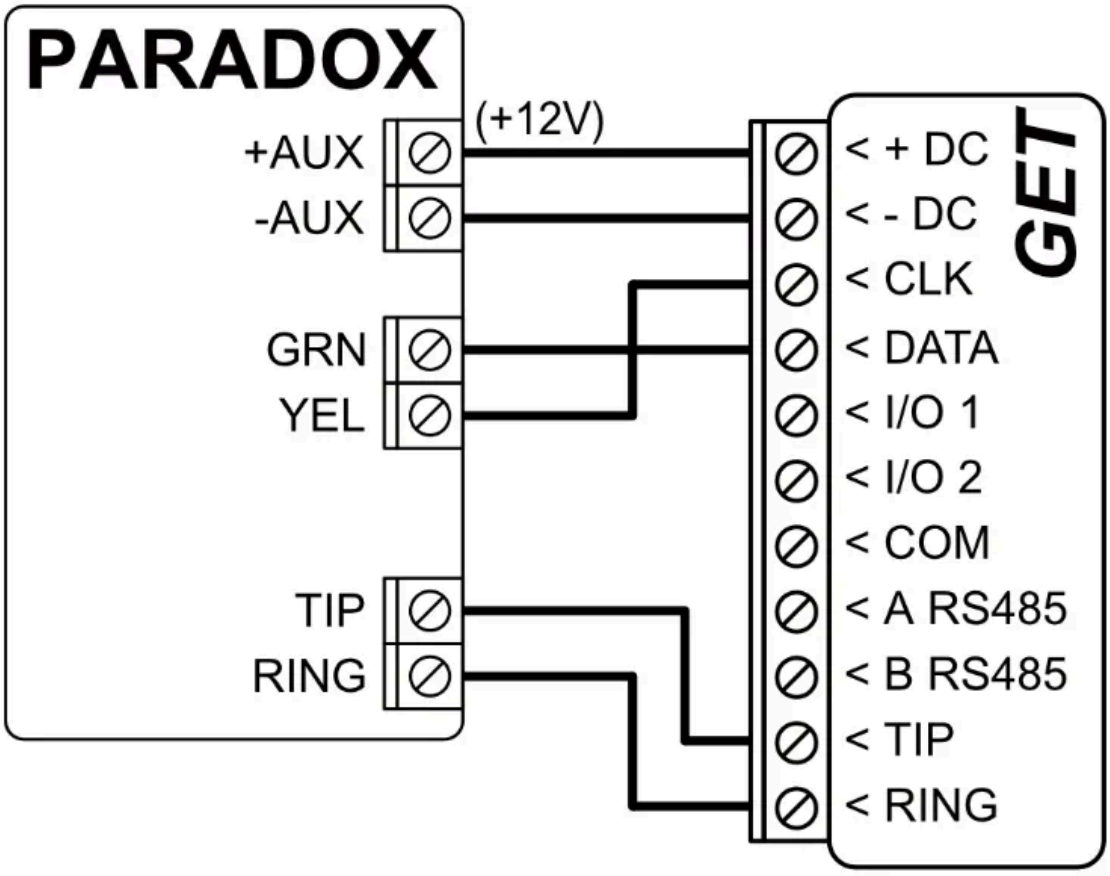


Figura 18. Collegamento di una centrale Paradox SP / SP+ / MG / MG+ contemporaneamente al Keybus (bus dati, «Keypad bus») e ai morsetti TIP/RING: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

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

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

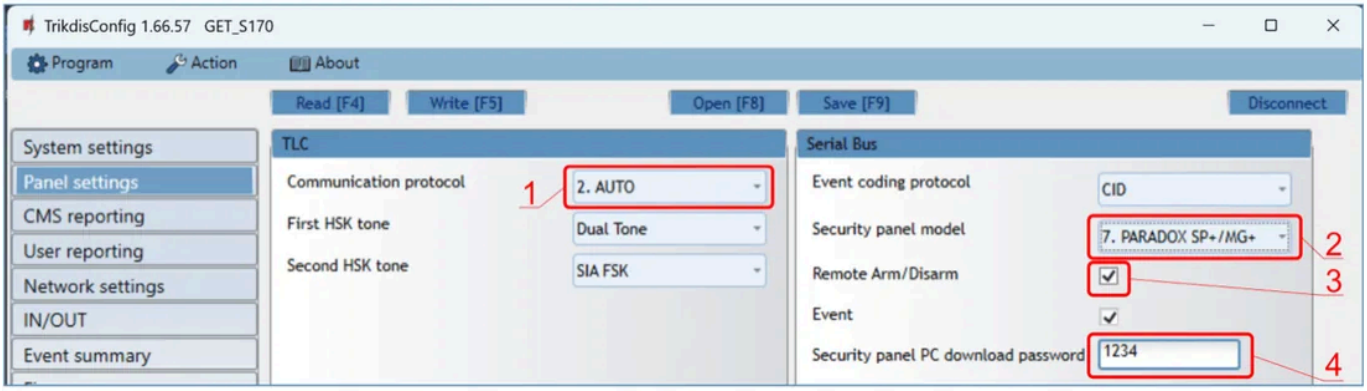


Figura 19. TrikdisConfig – Panel settings per il collegamento Keybus + TIP/RING: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm spuntato (3), Security panel PC download password inserita (4).

Nell'app Protegus 2 le stesse impostazioni si trovano nelle pagine **Panel settings** → **TLF** (Security panel model = Communication protocol) e **Panel settings** → **Serial Bus** (paragrafo 6.3).

Bisogna programmare anche la centrale Paradox, perché invii gli eventi alla centrale di vigilanza e sia comandabile da Protegus 2 – sulla tastiera collegata alla centrale imposta le sezioni seguenti:

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

La password PC scritta nella sezione **911** deve coincidere con il campo **Security panel PC download password** del comunicatore (paragrafo 4.1.2).

3.3.4 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 CLK, TIP e RING non servono.

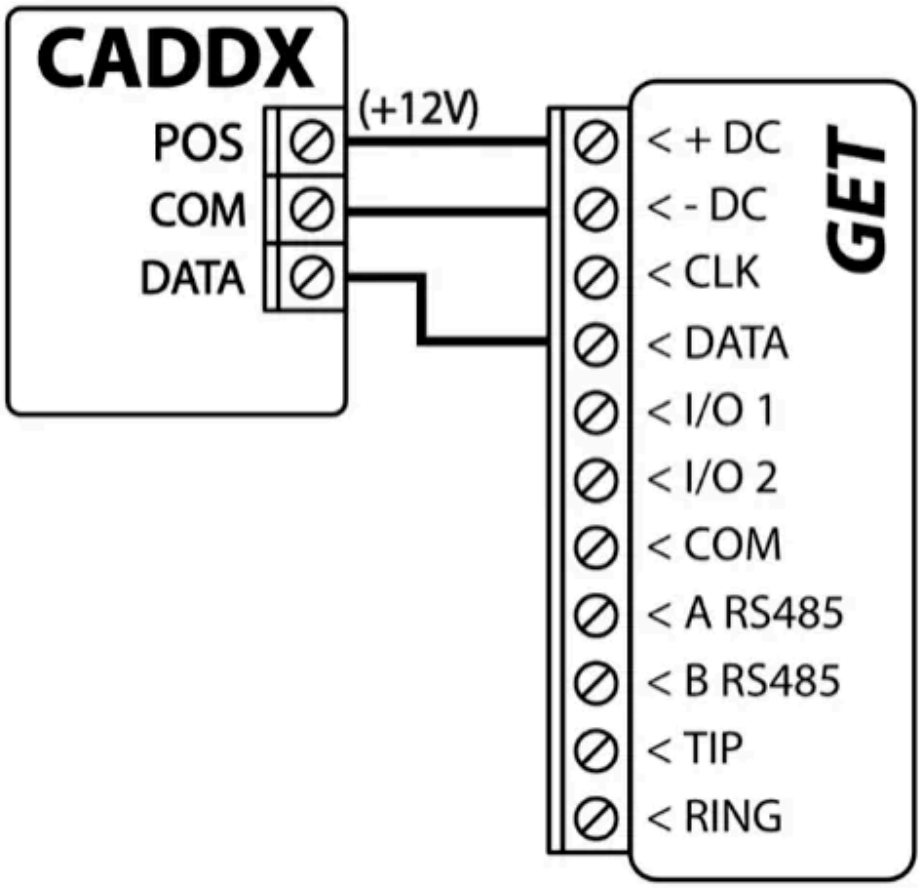


Figura 20. Collegamento di una centrale UTC Interlogix (Caddx) NetworX al bus dati («Keypad bus»): POS → +DC, COM → −DC, DATA → DATA.

3.3.5 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**.

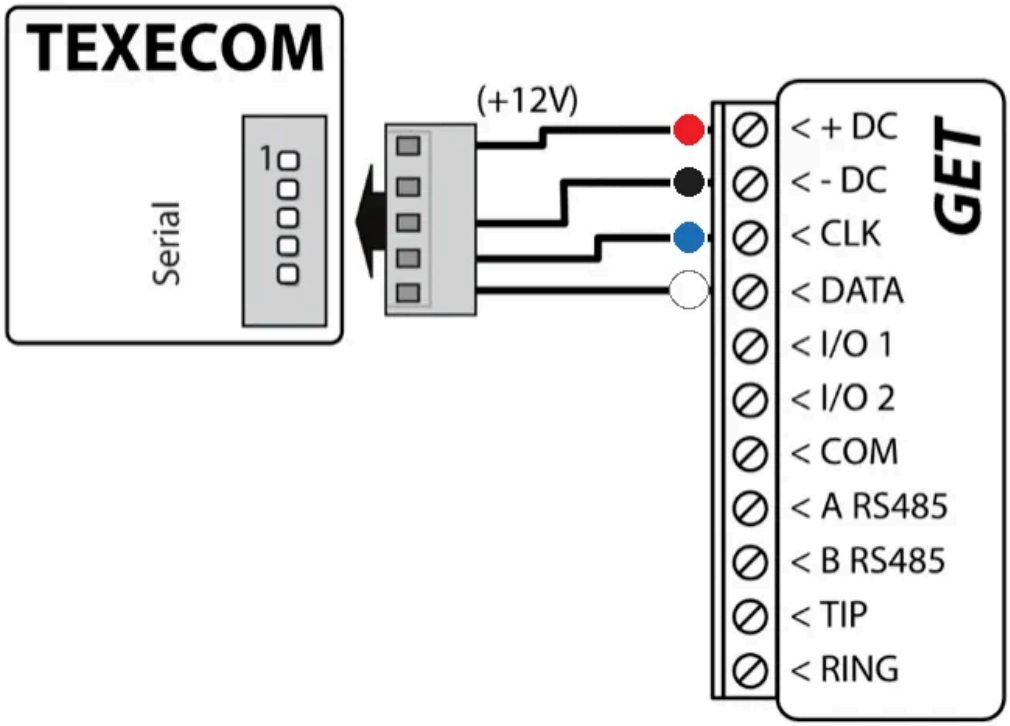


Figura 21. Collegamento di una centrale Texecom alla porta seriale con il cavo EX-CRP4 (da ordinare separatamente; «Use the EX-CRP4 cable (ordered separately)»): rosso → +DC, nero → −DC, blu → CLK, bianco → DATA.

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

3.3.6 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**.

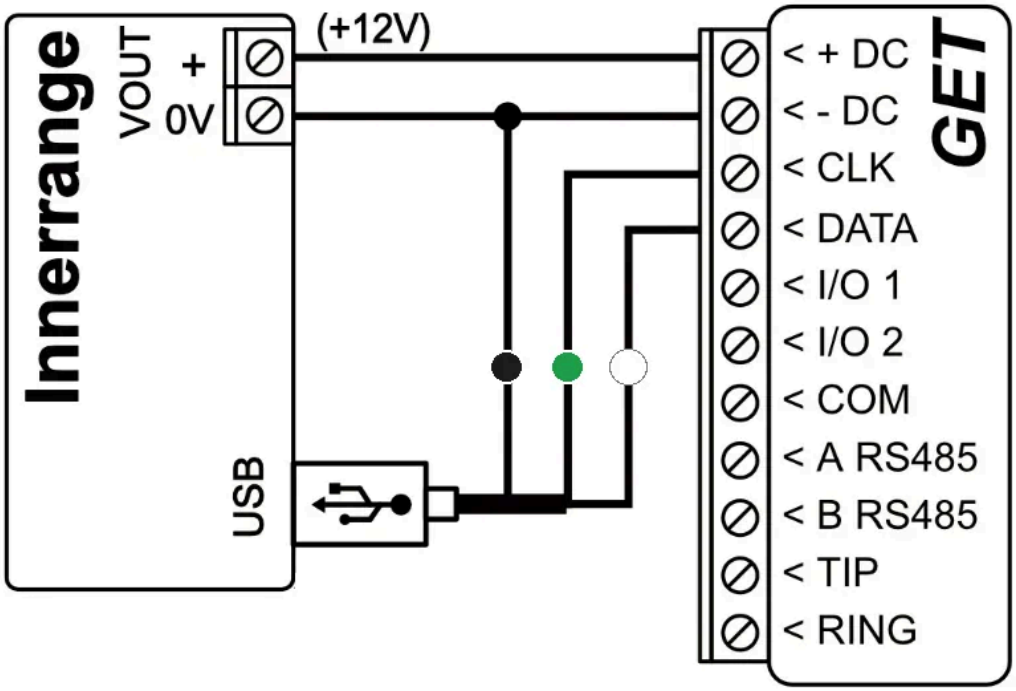


Figura 22. Collegamento di una InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; dalla porta USB con il cavo 993030USB («Cable, Inner Range part number 993030USB») nero → −DC, verde → CLK, bianco → DATA.

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

3.3.7 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**.

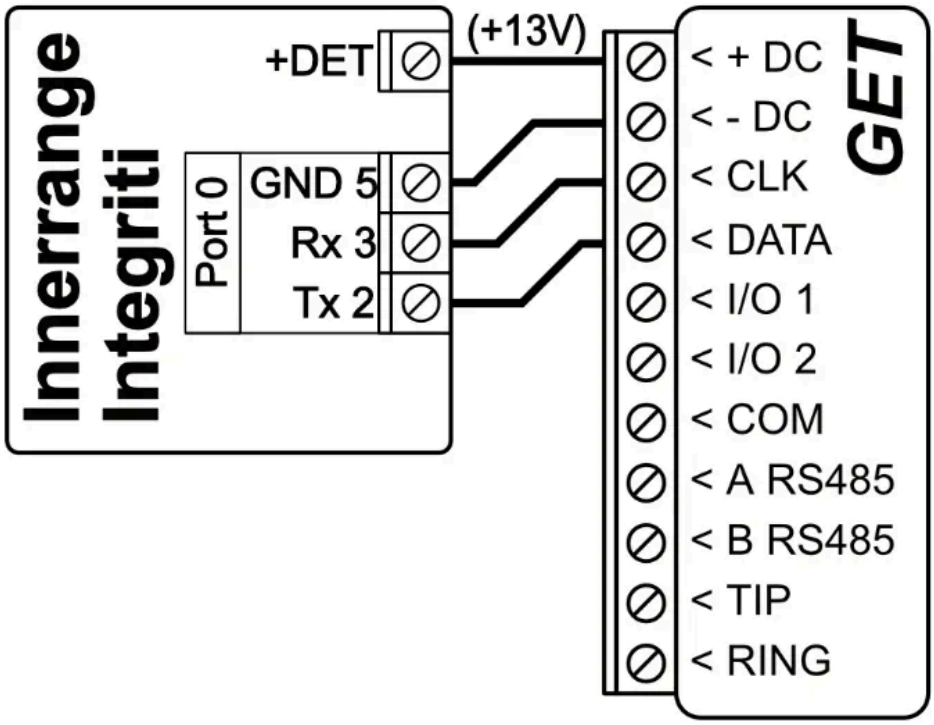


Figura 23. Collegamento di una InnerRange Integriti alla Port 0 con il cavo INTG-996795 («Cable, Inner Range part number INTG-996795»): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – bus dati

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

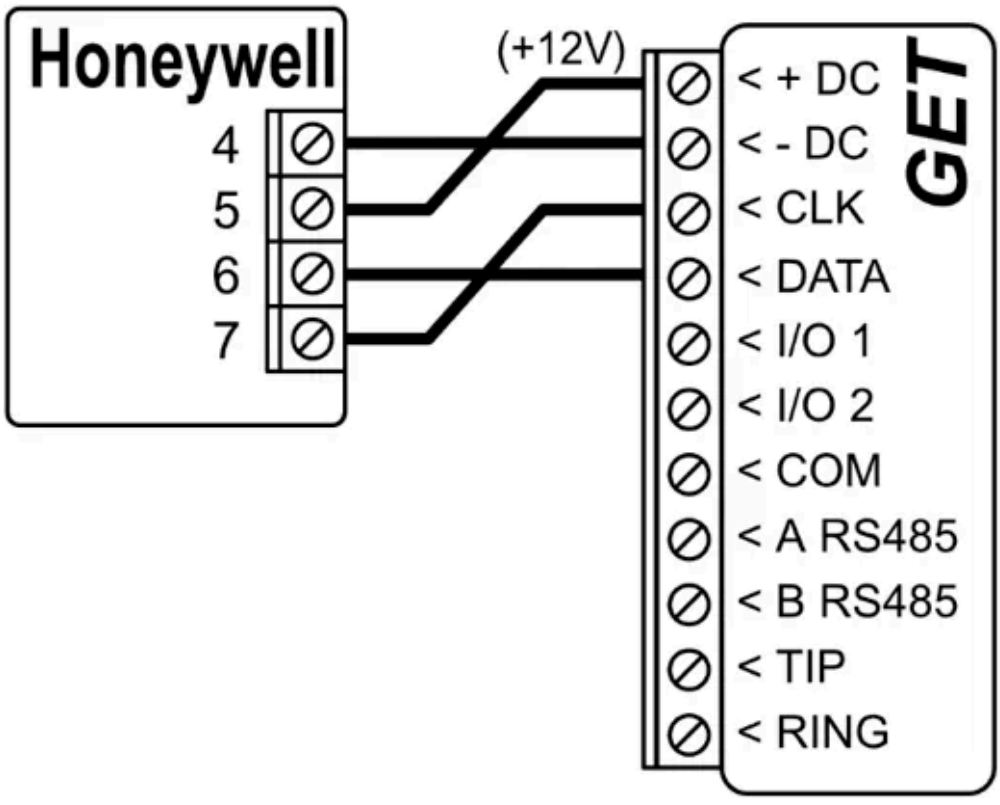


Figura 24. Collegamento di una centrale Honeywell Vista-15 / -20 / -48 al bus dati («Keypad bus»): morsetto 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Qualsiasi centrale – TIP/RING

Qualsiasi altra centrale si può collegare tramite il suo combinatore telefonico: l'alimentazione dall'uscita 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).

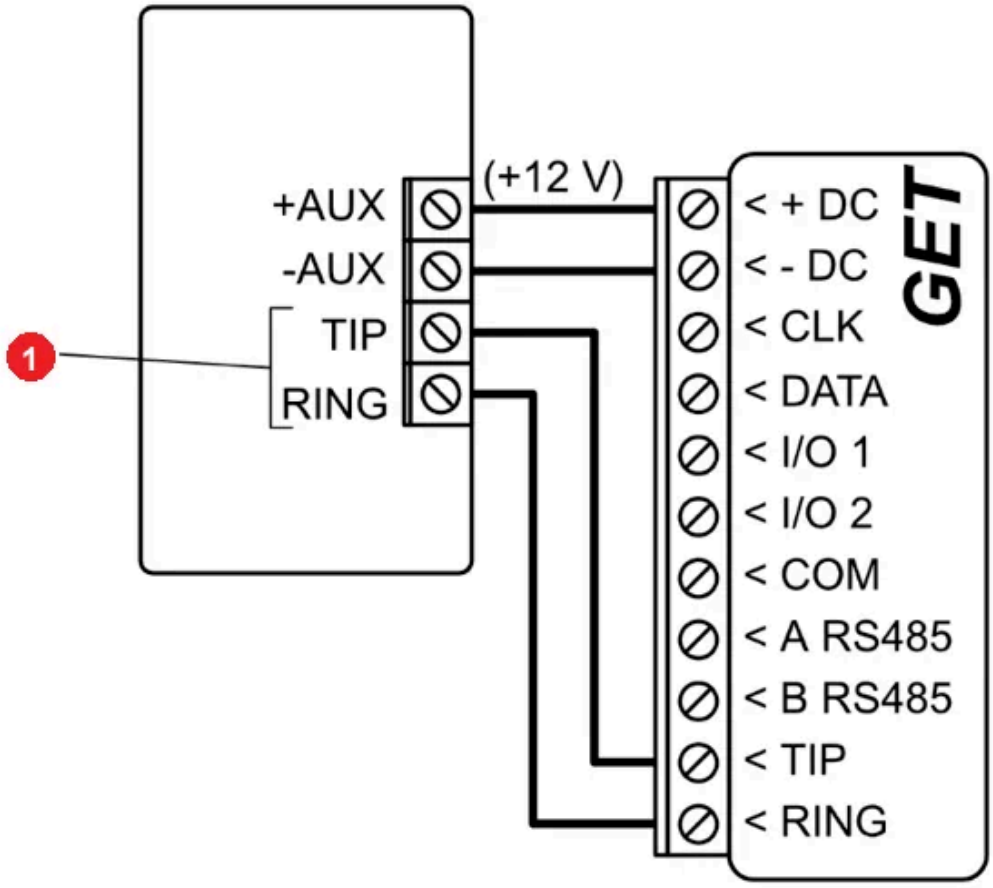


Figura 25. Collegamento al combinatore telefonico della centrale («Control panel»): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

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

3.4 Collegamento della zona chiave

Se vuoi inserire e disinserire la centrale dall'app Protegus 2 facendo in modo che l'uscita (PGM) del comunicatore comandi la **zona chiave** della centrale, segui questo collegamento. I due morsetti I/O a doppia funzione del comunicatore funzionano come uscite (OUT, PGM) – sul GET di fabbrica sono entrambi uscite –, quindi le due uscite possono comandare due aree del sistema: collega la zona chiave dell'area 1 al morsetto **1 I/O** e quella dell'area 2 al morsetto **2 I/O**. Con questo collegamento, nella pagina **Panel settings** di TrikdisConfig togli la spunta **Remote Arm/Disarm**, nella pagina **IN/OUT** i morsetti devono avere la 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 centrale e comunicatore resta (il comunicatore legge gli eventi dal bus), mentre l'inserimento e il disinserimento avvengono tramite la zona chiave:

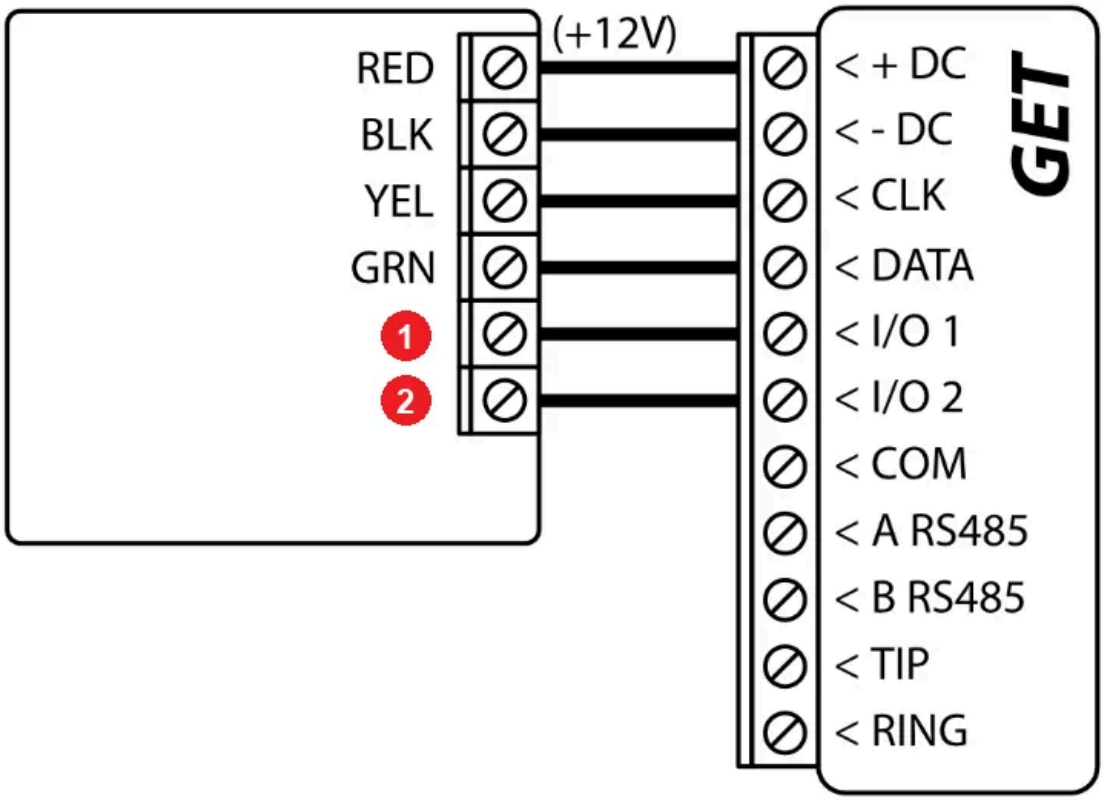


Figura 26. Inserimento e disinserimento con zona chiave («Zone (keyswitch)»), con collegamento al bus dati o seriale («Keypad bus or Serial port»): morsetto RED della centrale d'allarme («Control panel») → +DC, BLK → −DC, YEL → CLK, GRN → DATA; la zona dell'area 1 → 1 I/O, quella dell'area 2 → 2 I/O.

- 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 con il suo combinatore, e l'inserimento e il disinserimento avvengono allo stesso modo tramite la zona chiave:

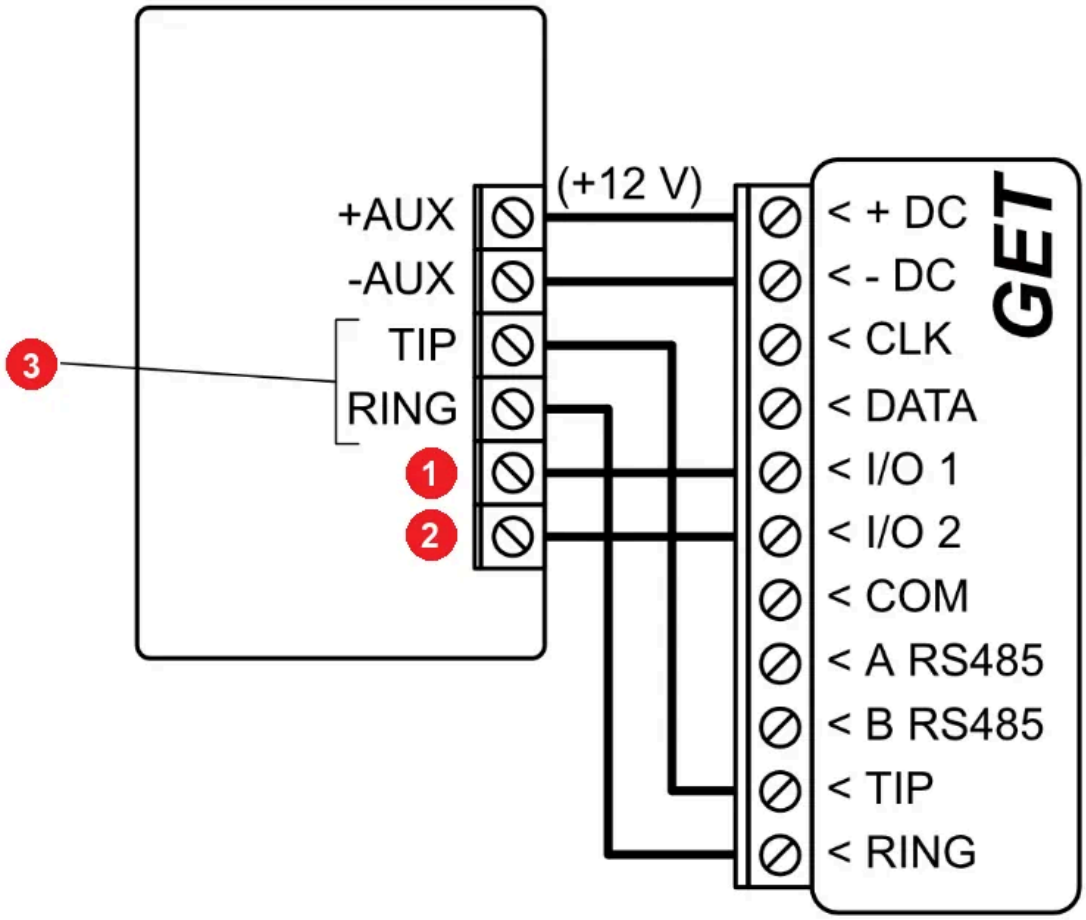


Figura 27. Inserimento e disinserimento con zona chiave («Zone (keyswitch)»), con collegamento alla linea telefonica: morsetto +AUX della centrale d'allarme («Control panel») → +DC, −AUX → −DC, TIP → TIP, RING → RING; la zona dell'area 1 → 1 I/O, quella dell'area 2 → 2 I/O.

- 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 impulsiva 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, come ingressi (IN), si possono usare anche per ricevere altri sensori (per es. contatto tamper, 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. Sul GET i morsetti di fabbrica sono uscite: imposta il morsetto usato sulla funzione **IN** nella pagina **IN/OUT** di TrikdisConfig e indica nel campo **Type** il tipo di circuito collegato; nell'app Protegus 2 la stessa impostazione si trova nella pagina **Advanced settings** → **IN/OUT**, nel campo **Type** del morsetto 1 o 2 (paragrafo 6.7). L'ingresso va collegato tra l'I/O scelto e il morsetto **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	–
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 i punti COM e INx: NO, NC, NC/EOL, NO/EOL e, 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.

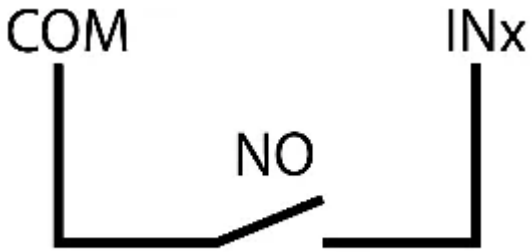


Figura 28. NO – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

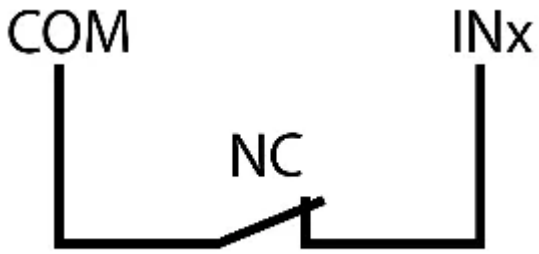


Figura 29. NC – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

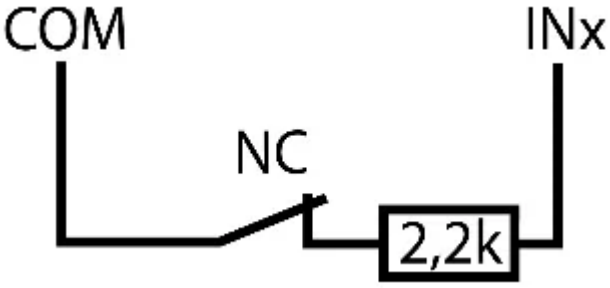


Figura 30. NC/EOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

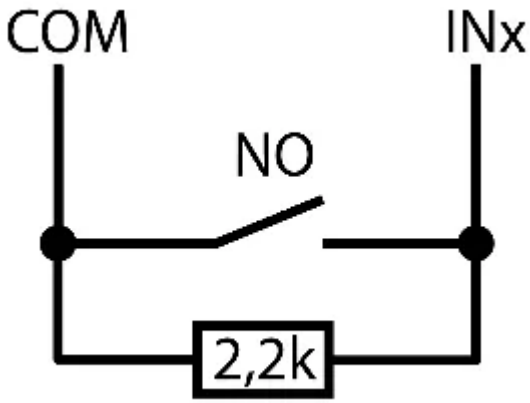


Figura 31. NO/EOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

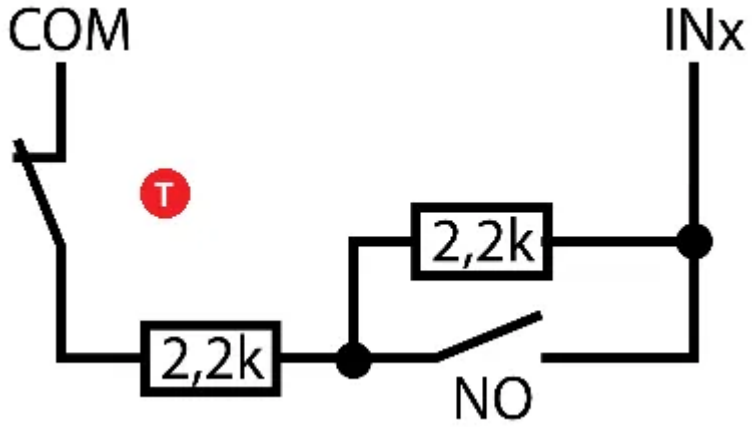


Figura 32. NO/DEOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

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

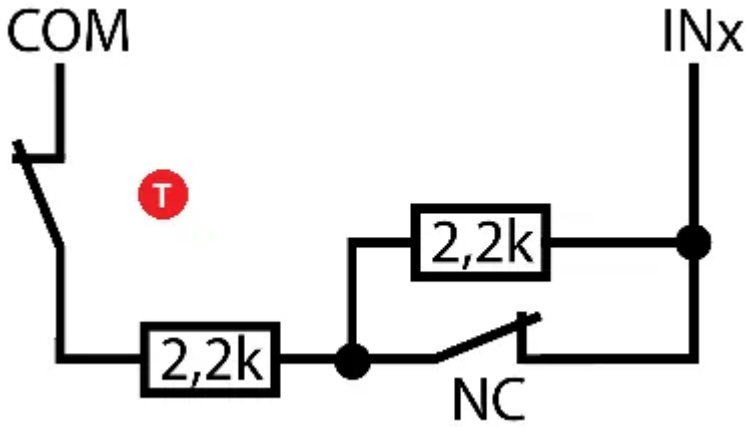


Figura 33. NC/DEOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

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

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 capo della bobina del relè va su **+DC**, l'altro sul morsetto **x I/O**, e l'utilizzatore è comandato dai contatti del relè (NC, C, NO). Il morsetto I/O usato deve essere un'uscita (**OUT**) nella pagina **IN/OUT** di TrikdisConfig (o nella pagina IN/OUT dell'app) – sul GET è l'impostazione di fabbrica.

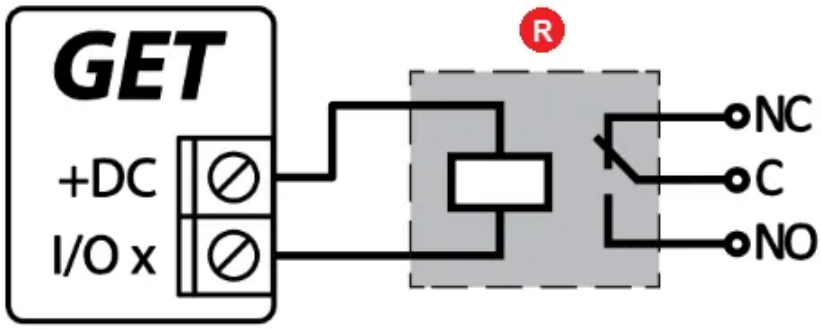


Figura 34. Collegamento di un relè all'uscita del comunicatore: la bobina va tra +DC e il morsetto x I/O, i contatti (NC, C, NO) comandano l'utilizzatore.

- R relè («Relay»)

Puoi comandare le uscite dall'app Protegus 2 (capitolo 5).

3.7 Accensione e primo controllo

A TRIKDIS átjelző elindítása

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

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

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

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

- **POWER** verde fisso – l'alimentazione è adeguata;
- **NETWORK LTE** verde fisso e lampeggia in giallo – connesso alla rete mobile; il numero dei lampeggi gialli è il livello del segnale: in 4G 3 lampeggi sono adeguati; se ne conti meno, il segnale è debole: cerca un'altra posizione per il comunicatore o per l'antenna, oppure usa un'antenna più sensibile (paragrafo 3.2);
- **NETWORK LAN** verde fisso, se hai inserito anche il cavo di rete – connesso alla rete cablata;
- **TROUBLE** spento.

Se il TROUBLE lampeggia, il numero dei lampeggi indica la causa (paragrafo 1.6); anche ogni altra segnalazione LED diversa da questa indica un guasto, cercane la causa 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

La configurazione 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). Per il collegamento Keybus + TIP/RING della Paradox SP / SP+ / MG / MG+ l'impostazione delle sezioni della centrale è indicata nella tabella del paragrafo 3.3.3.

4.1 Collegamento al bus dati o seriale

Qui descriviamo come configurare 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 (nell'app: **Panel settings** → **Serial Bus**) l'opzione **Remote Arm/Disarm** deve essere spuntata (paragrafi 2.2 e 6.3).

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.

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.

Sul comunicatore GET il campo **Security panel PC download password** si trova nella pagina **Panel settings** di TrikdisConfig, nel gruppo **Serial bus**; nell'app Protegus 2 in **Panel settings** → **Serial Bus** → **PC download password** (paragrafi 2.2 e 6.3).

Collegamento Keybus e TIP/RING (SP / SP+ / MG / MG+, paragrafo 3.3.3): in aggiunta, la centrale va programmata perché invii gli eventi alla centrale di vigilanza e sia comandabile da Protegus 2 – i valori delle sezioni (801, 811, 812, 815, 911) sono indicati nella tabella del paragrafo 3.3.3.

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]**.

Sul comunicatore GET il campo **Security panel PC download password** si trova nella pagina **Panel settings** di TrikdisConfig, nel gruppo **Serial bus** (nell'app in **Panel settings** → **Serial Bus** → **PC download password**); 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

Locazione (location)	Segmento	Impostazione
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.

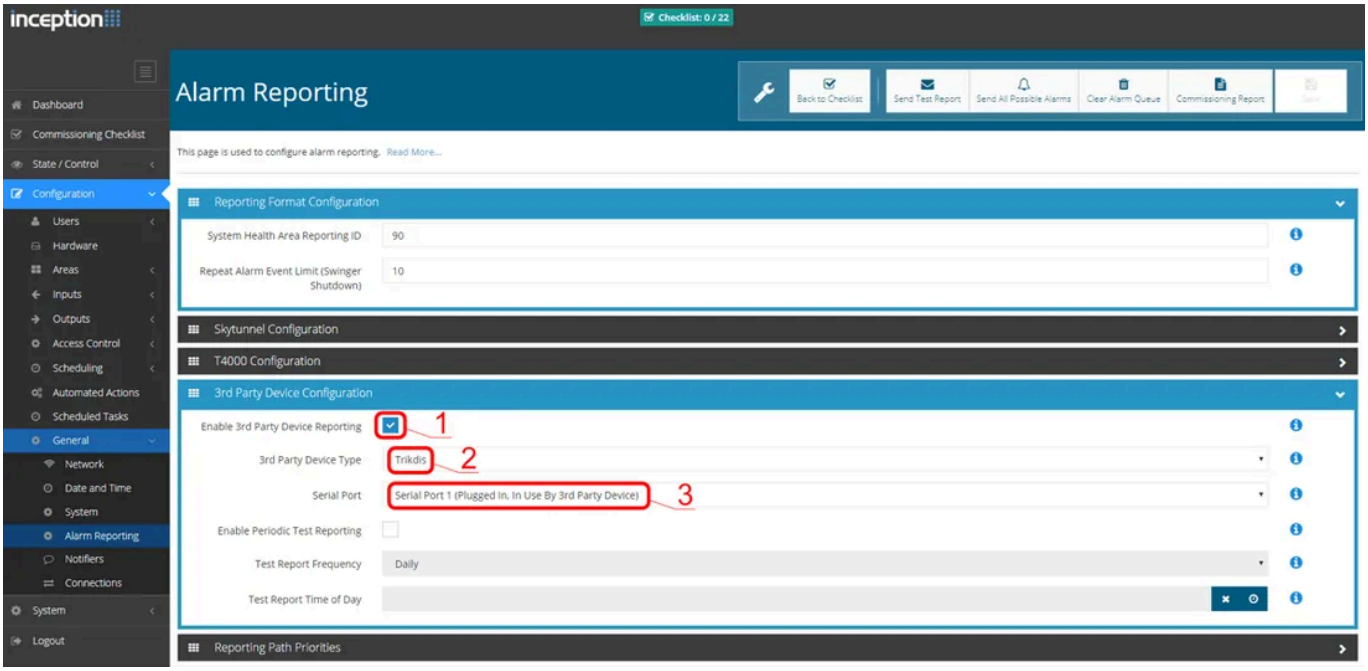


Figura 35. InnerRange Inception – Configuration → General → Alarm Reporting, gruppo 3rd Party Device Configuration: Enable 3rd Party Device Reporting spuntato, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

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 si possono collegare al comunicatore tramite la loro uscita della linea telefonica (paragrafo 3.3.9) – in questo caso anche per queste bisogna configurare il combinatore, e il comando diretto non è disponibile.

4.2.1 Programmazione del combinatore della 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 della 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 digita in sequenza quanto segue:

Posizione (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. Controllo 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 usa dal browser: web.protegus.app. Accedi con il tuo nome utente e la tua password, oppure registra un nuovo account. Il GET non invia notifiche via SMS né con chiamate telefoniche e non accetta comandi SMS: il comando a distanza e le notifiche passano dall'app; anche le impostazioni del comunicatore sono accessibili dall'app (**Settings** → **Advanced settings**, capitolo 6).

5.1 Aggiunta del dispositivo

Prima di aggiungere il dispositivo verifica che:

1. La scheda SIM sia attiva e il suo codice PIN sia inserito nel dispositivo, oppure la richiesta del PIN sia disattivata – **oppure** il comunicatore sia collegato alla rete locale con un cavo di rete (LAN).
2. Nella pagina **User reporting** → **PROTEGUS Cloud** di TrikdisConfig sia spuntato **Enable connection** (paragrafo 6.5).
3. Il LED **POWER** sia verde fisso.
4. Il LED **NETWORK LTE** sia verde fisso e lampeggi in giallo (il dispositivo è sulla rete mobile); con la sola connessione cablata è il LED **NETWORK LAN** a essere verde fisso.

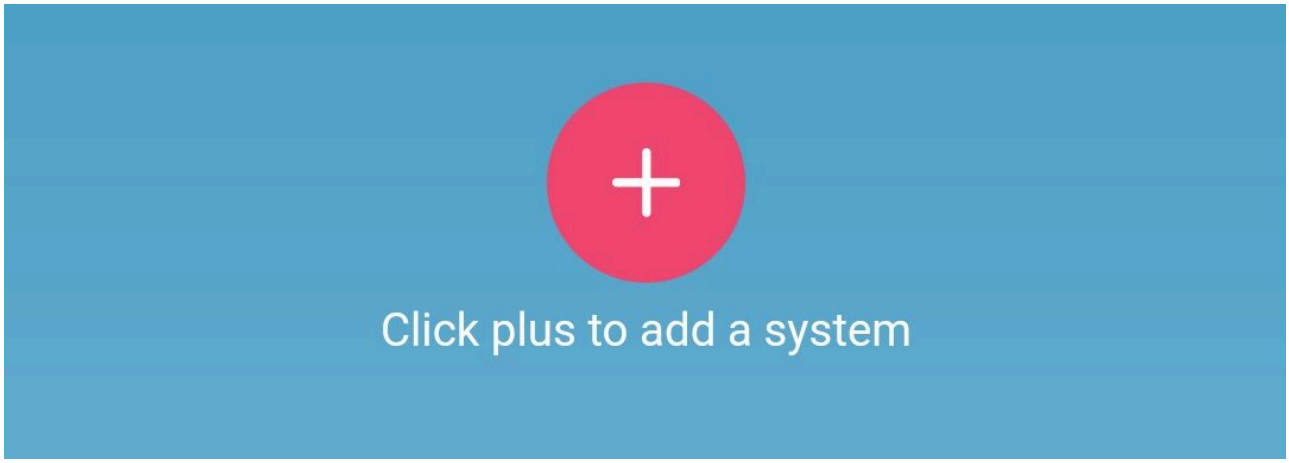
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è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



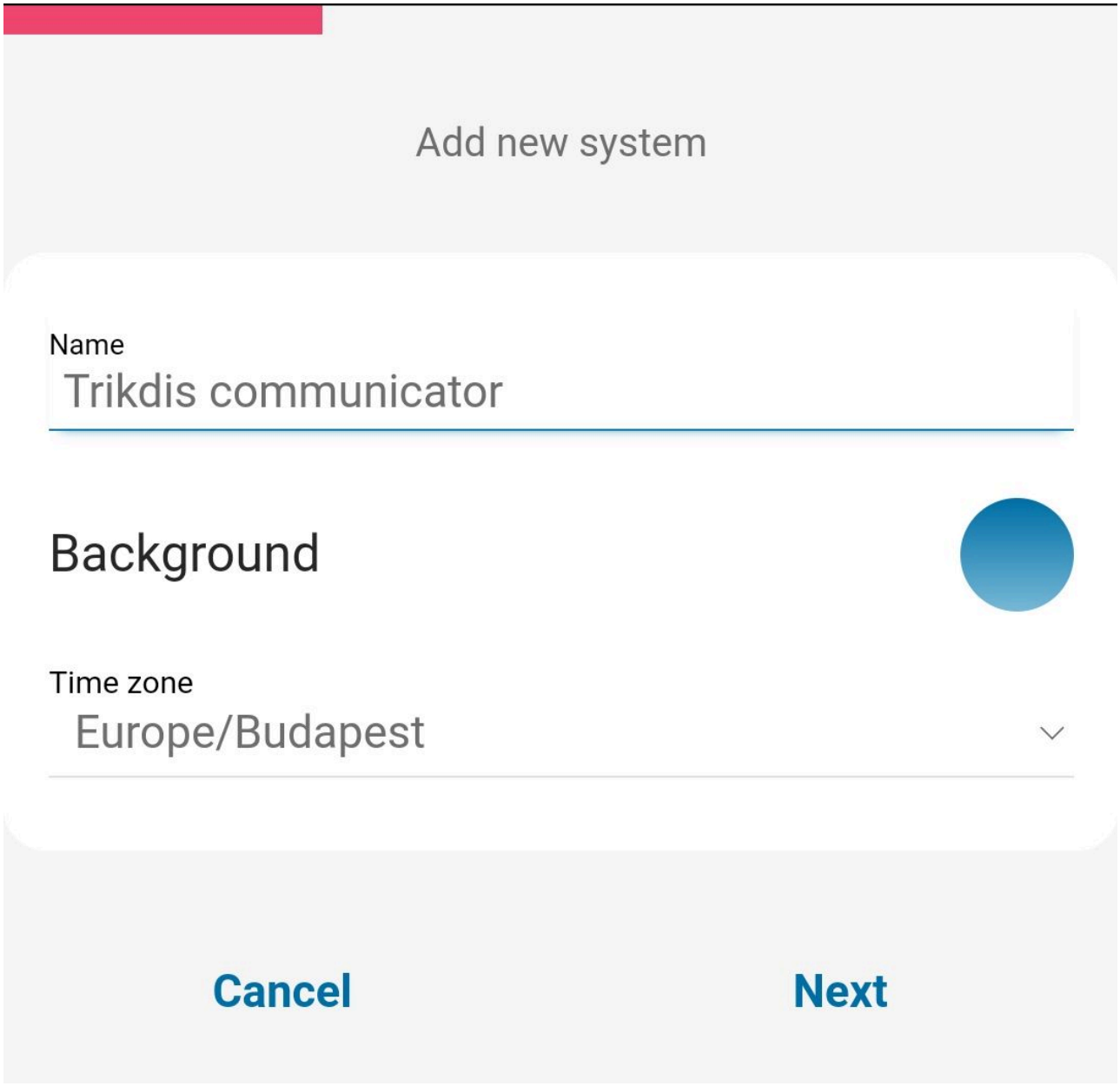
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



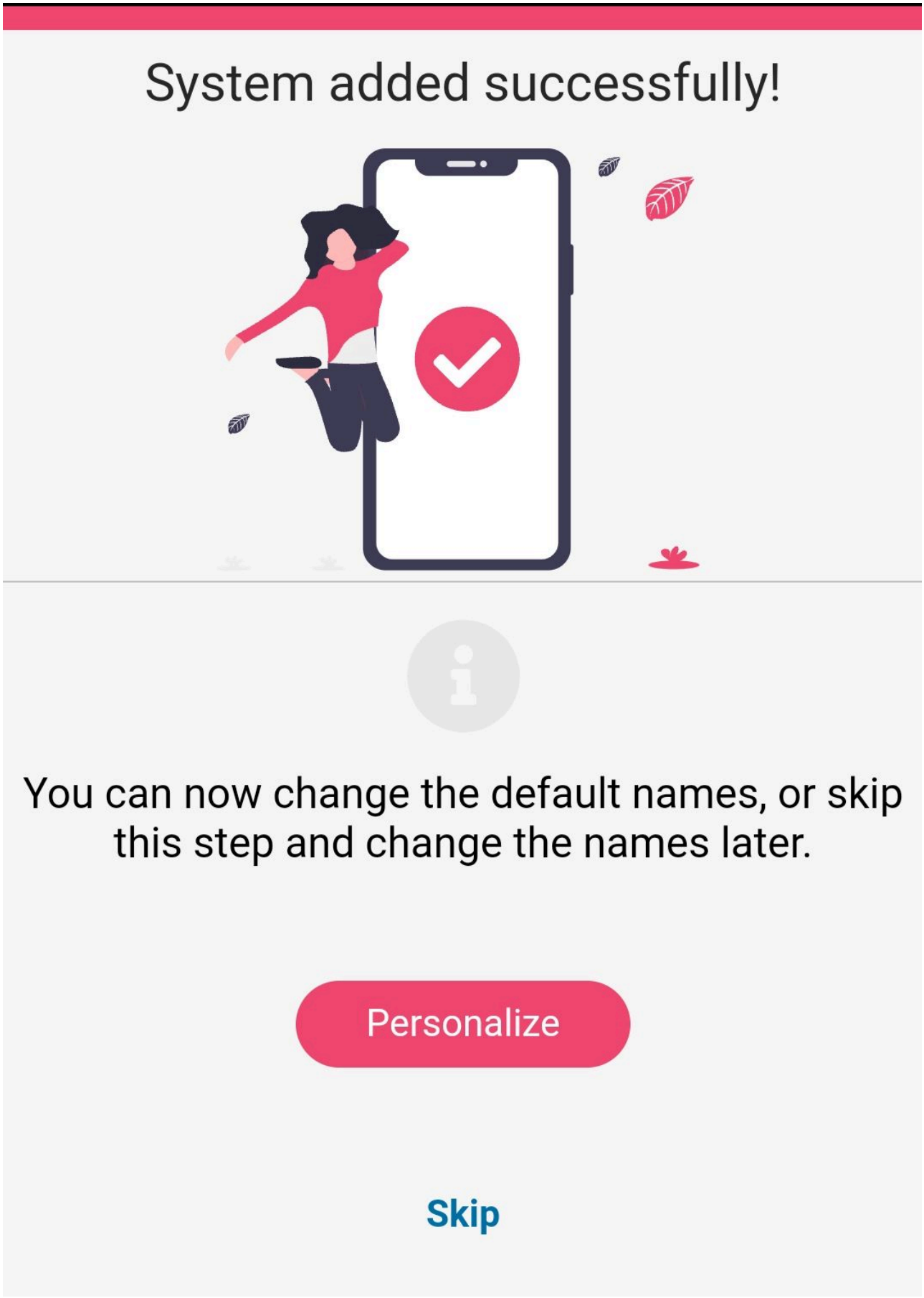
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



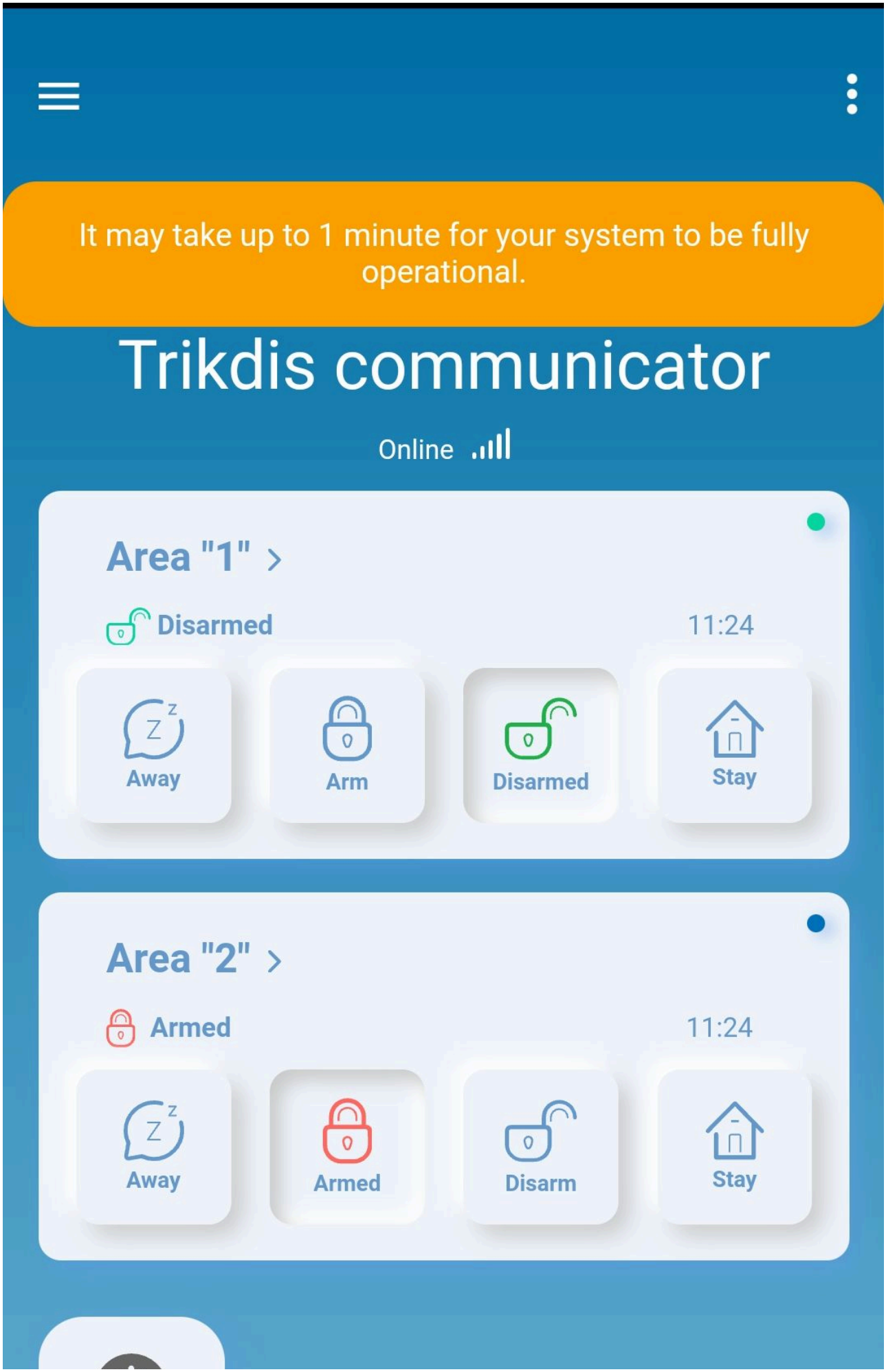
6. Add meg a rendszer nevét és válassz idozónát



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

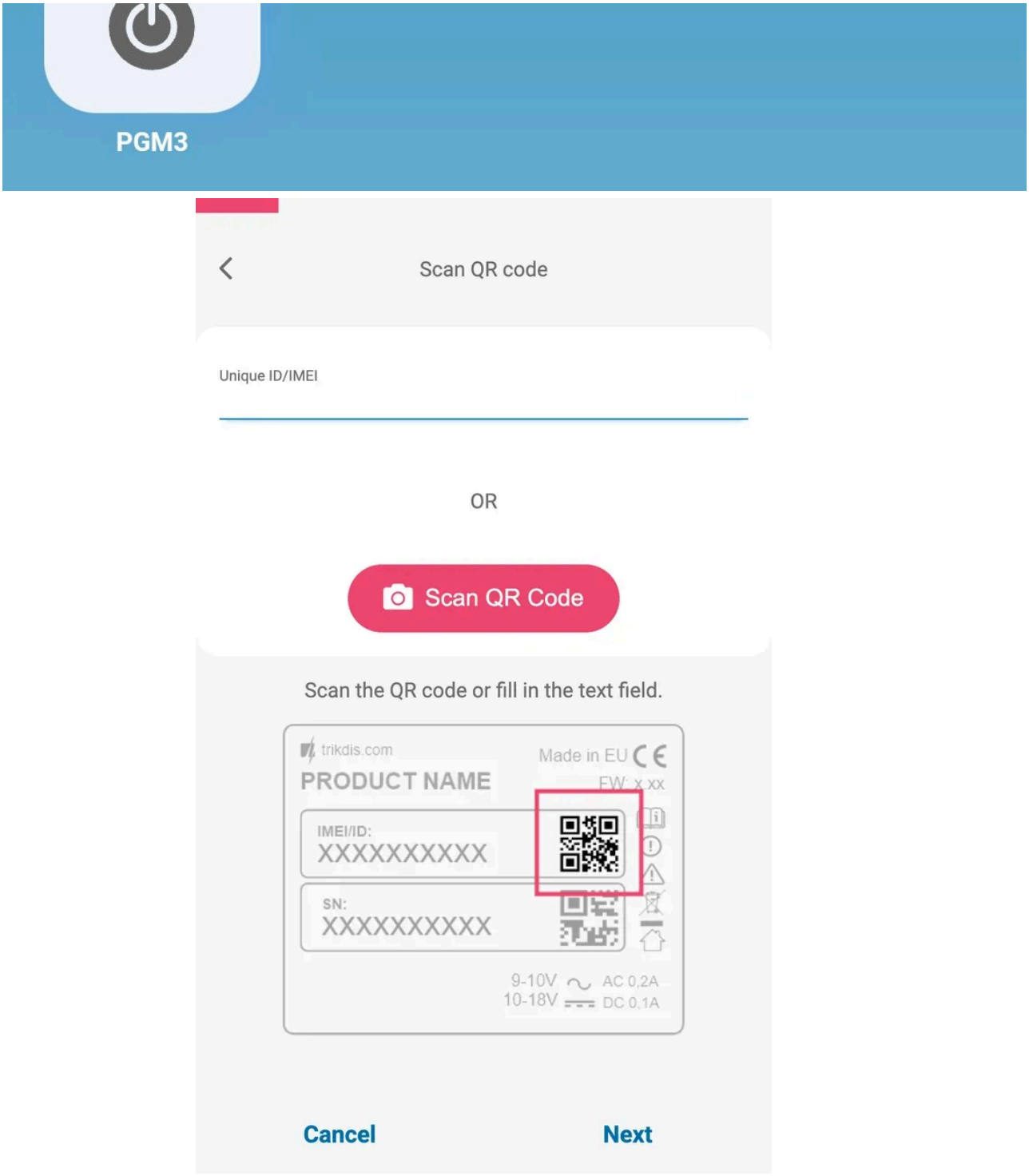


Figura 36. Protegus 2 – aggiunta di un nuovo sistema: inserimento dell'IMEI / Unique ID o scansione del codice QR dell'etichetta, poi Next.

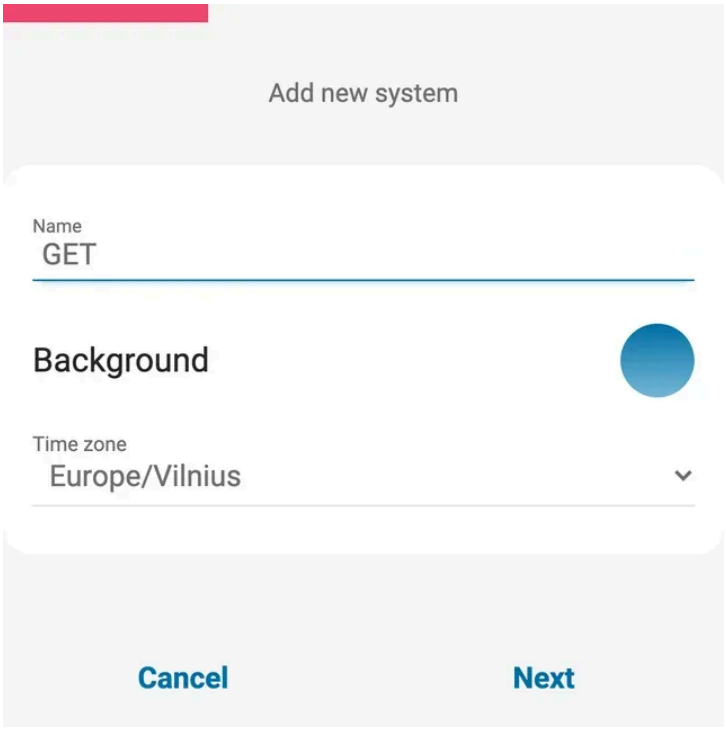


Figura 37. Protegus 2 – inserimento del nome del sistema (Name), poi Next.

L'identificativo univoco del dispositivo (**IMEI / Unique ID**) si legge sull'etichetta del dispositivo e sull'adesivo della scatola, 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 con un'uscita

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

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

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

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

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



Figura 38. 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.

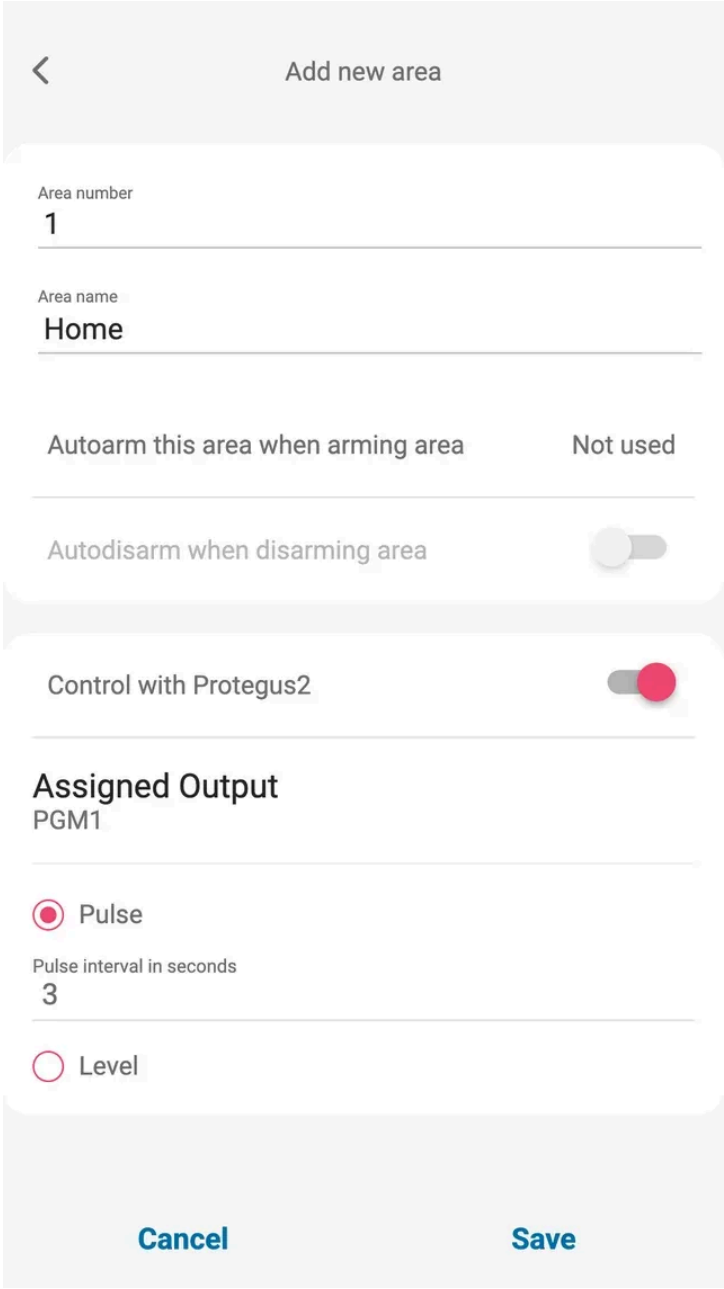


Figura 39. Protegus 2 – aggiunta di un'area (Add new area): Area number, Area name, Control with Protegus2 attivato, Assigned Output PGM1, Pulse (3 s) o Level, poi Save.

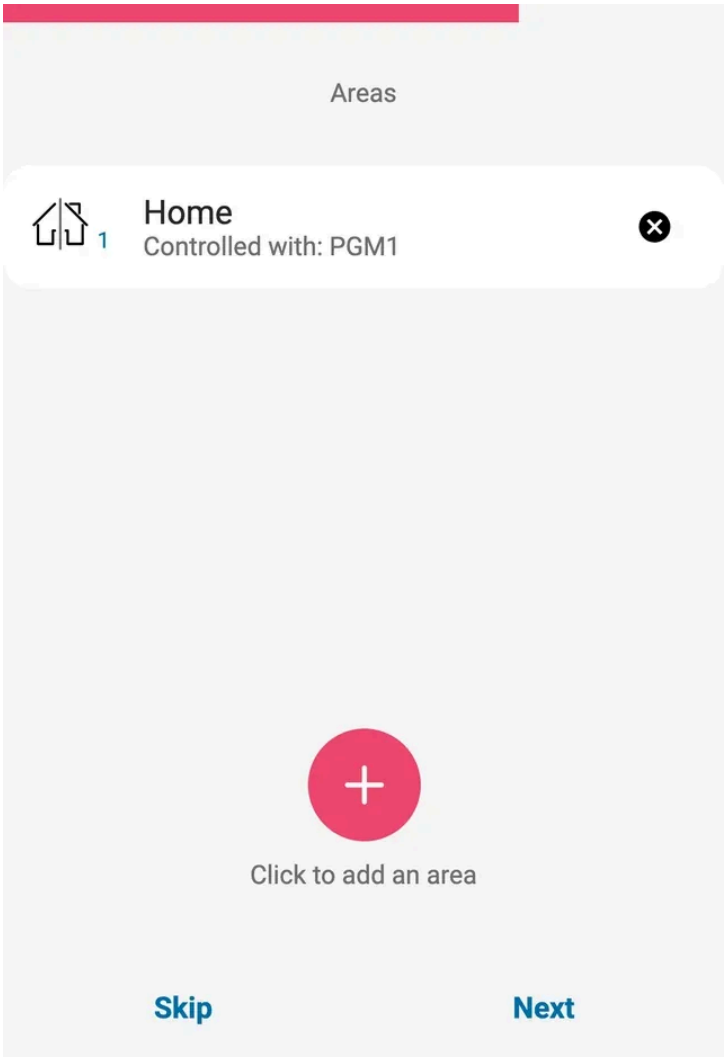


Figura 40. Protegus 2 – l'elenco delle aree (Areas): l'area Home è comandata da PGM1; altre aree con il pulsante Click to add an area, la procedura guidata si chiude con il pulsante Skip.

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.

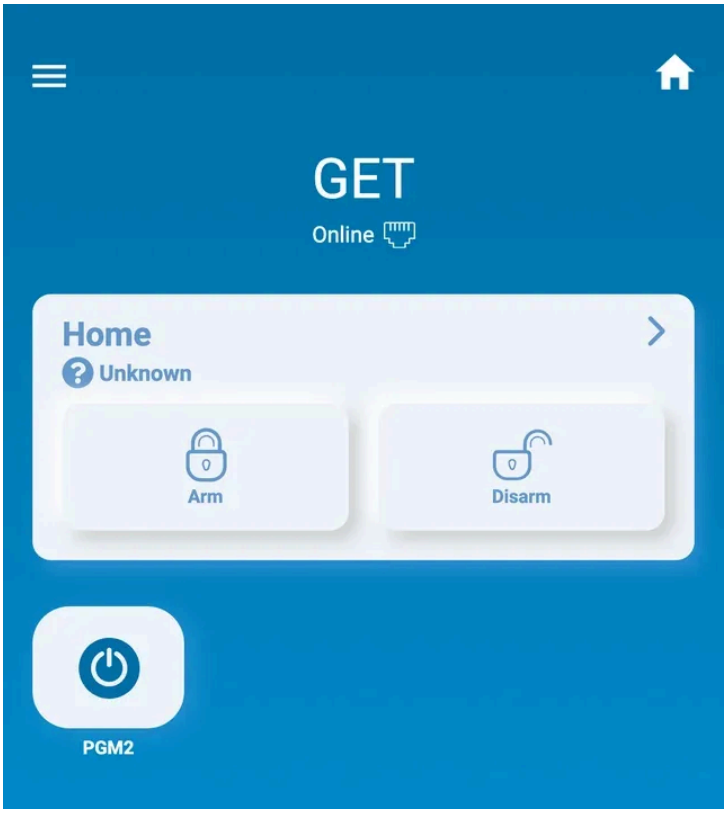


Figura 41. Protegus 2 – la schermata iniziale del sistema: lo stato dell'area, i pulsanti Arm e Disarm e, sotto, l'uscita PGM comandabile.

6. Le impostazioni in dettaglio

La maggior parte delle impostazioni del GET è disponibile sia nel programma **TrikdisConfig** per Windows sia nell'app **Protegus 2** (**Settings** → **Advanced settings**, paragrafo 2.2); dove qualcosa si trova solo in uno dei due, lo indichiamo. Ogni impostazione viene descritta una sola volta e per ogni paragrafo indichiamo dove la trovi nei due strumenti; tra parentesi c'è la dicitura dell'app, se diversa da quella di TrikdisConfig. Sul lato sinistro della finestra di TrikdisConfig c'è l'elenco delle pagine (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), in alto la barra dei pulsanti (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), in basso la barra di stato.

6.1 Connessione al comunicatore

App Protegus 2. Apri il sistema e vai nel menu **Settings** → **Advanced settings**. In cima a ogni schermata sono visibili i dati del dispositivo connesso: **Unique ID** (IMEI), **Serial** (numero di serie), versione **Firmware** e **Boot**. I gruppi di impostazioni nel menu: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** e **System events**. Dopo la modifica scrivi le impostazioni nel dispositivo con il pulsante **Write**; **Read** rilegge dal dispositivo i valori attuali.

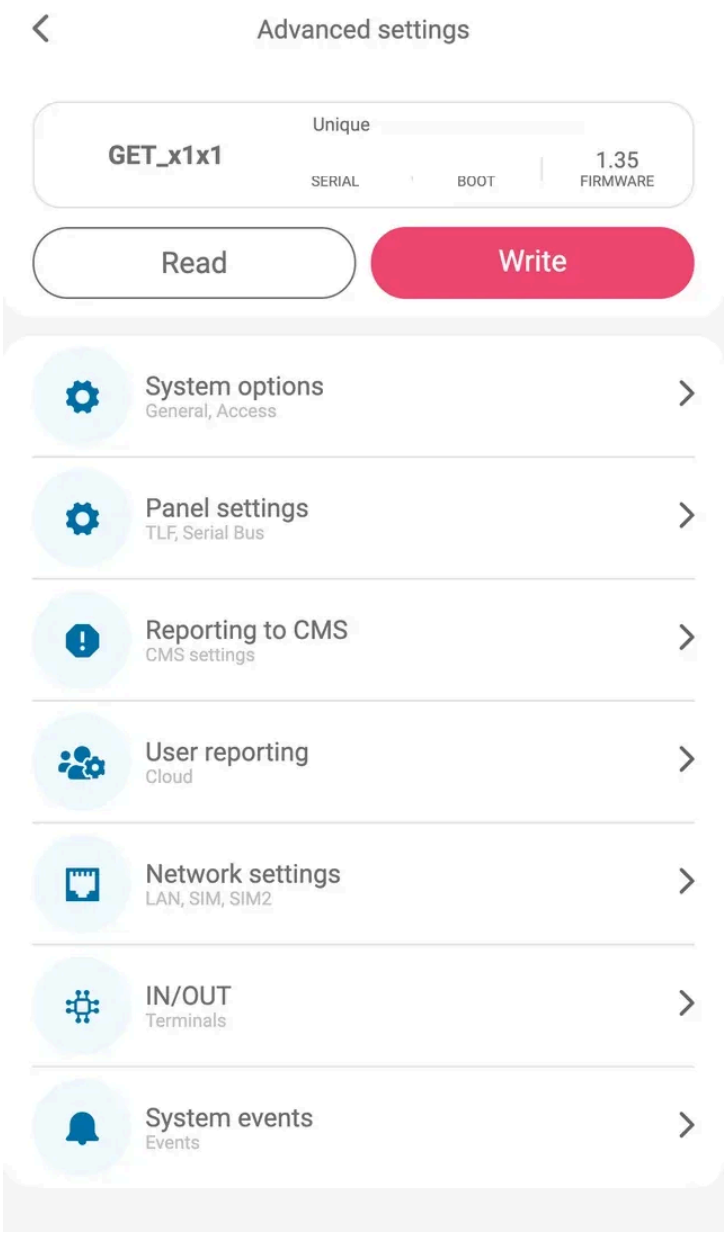


Figura 42. Protegus 2 – menu Advanced settings: in alto i dati del dispositivo (tipo, Unique ID, numero di serie, versione boot e firmware), i pulsanti Read e Write, sotto i gruppi di impostazioni.

TrikdisConfig. Dopo aver collegato il comunicatore e premuto **Read [F4]**, il programma mostra i dati del dispositivo nella 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.

Etichetta	Significato
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 43. La barra di stato di TrikdisConfig con un GET letto: identificativo, stato, tipo (Device: GET_S170), numero di serie, versione BL (bootloader), FW e HW, modalità di connessione e livello di accesso.

Nel campo **Device** deve comparire una sigla GET (nella figura GET_S170; il suffisso alfanumerico indica la versione hardware), **BL** è la versione del bootloader. Dopo **Read [F4]** il programma legge e mostra i valori impostati nel dispositivo; fai le impostazioni necessarie secondo le descrizioni delle pagine riportate sotto.

6.2 System settings (System options)

Nell'app: Advanced settings → System options → System general (identificativi, sincronizzazione dell'ora) e **System options → Access** (codici e diritti dell'installatore). Dove si trovano l'**Account No.** e il **Device account No.** dipende dalla versione hardware e dal firmware: su hardware **x1x1**, con firmware **1.31** o successivo, li trovi nella pagina **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.**; sul canale parallelo **Parallel Account no.**) e nella pagina **Reporting to CMS → Settings** (**Device account No.**), mentre nella pagina System general resta solo **Time set**; altrimenti sono entrambi nella pagina System general.

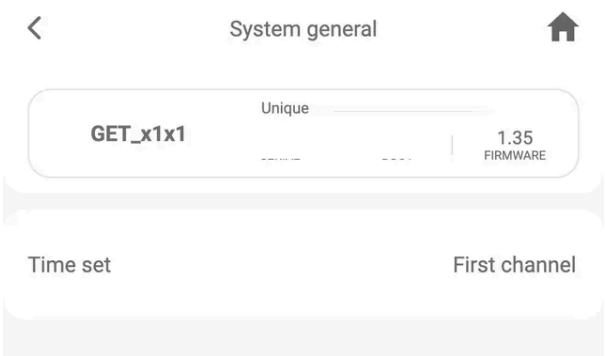


Figura 44. Protegus 2 – System options → System general su hardware x1x1 (firmware 1.35): è visibile solo Time set, gli identificativi sono tra le impostazioni CMS.

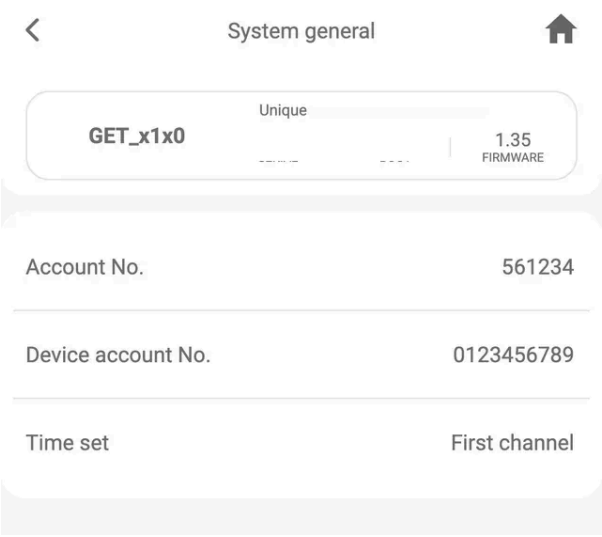


Figura 45. Protegus 2 – System options → System general su hardware x1x0: Account No., Device account No. e Time set.

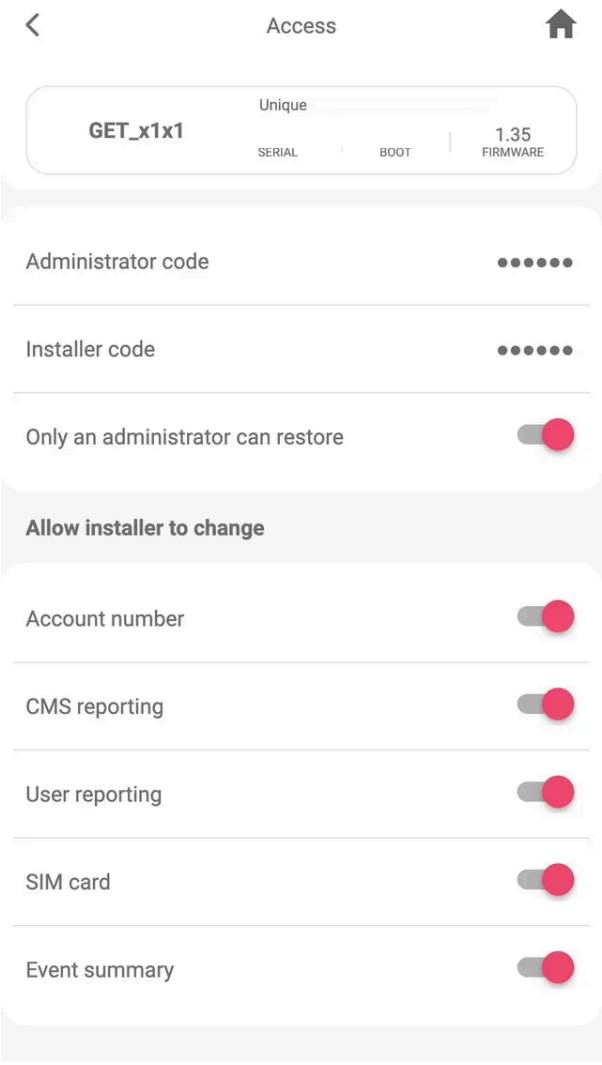


Figura 46. Protegus 2 – System options → Access: Administrator code, Installer code, Only an administrator can restore e l'elenco Allow installer to change (Account number, CMS reporting, User reporting, SIM card, Event summary).

In TrikdisConfig: la pagina **System settings** è composta da due gruppi: nel gruppo **General** imposti gli identificativi del dispositivo, nel gruppo **Access** i livelli di accesso.

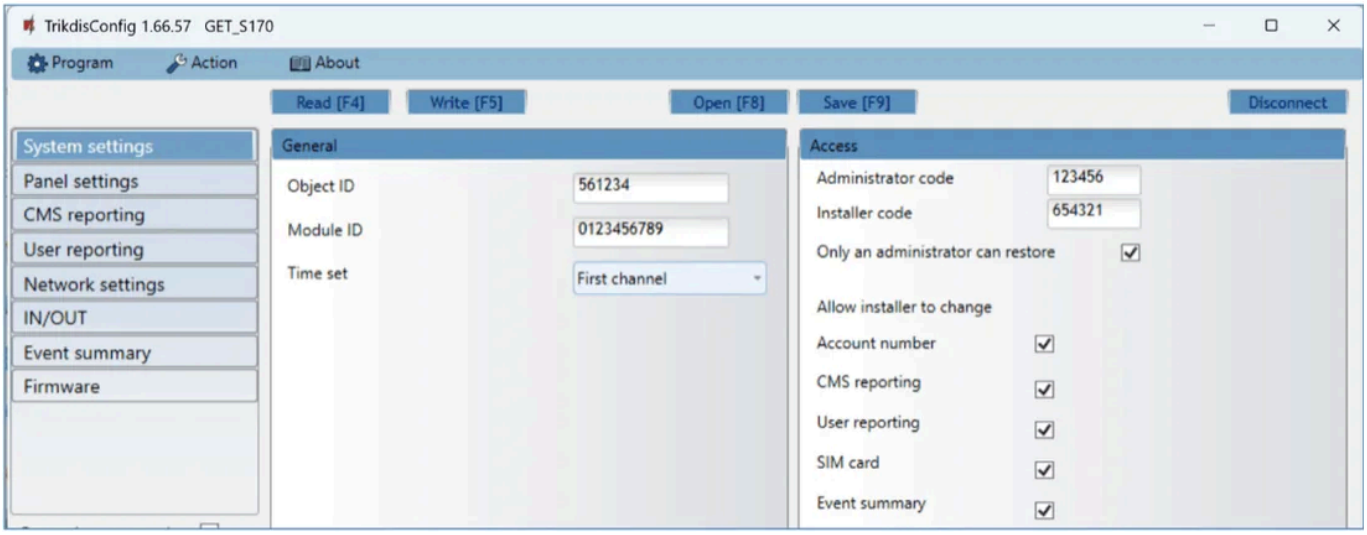


Figura 47. TrikdisConfig – pagina System settings: gruppo General (Object ID, Module ID, Time set) e gruppo Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – il codice impianto ricevuto dalla centrale di vigilanza (6 caratteri esadecimali: 0–9, A–F; `FFFE` e `FFFF` non si possono usare). Obbligatorio se il dispositivo trasmette anche alla centrale di vigilanza.
- **Module ID** (Device account No.) – il numero identificativo del modulo.
- **Time set** – da quale server 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.

Accesso come installatore nell'app. Se apri il comunicatore con il codice installatore, Protegus 2 nasconde i campi **Administrator code** e **Only an administrator can restore**, e mostra in sola lettura le impostazioni non consentite dall'amministratore. Nell'app il diritto **SIM card** vale anche per le impostazioni LAN; dove gli identificativi si trovano tra le impostazioni CMS (vedi sopra), per essi vale il diritto **CMS reporting**.

6.3 Panel settings

In questa pagina indichi come il comunicatore è collegato alla centrale d'allarme: il gruppo **TLC** (nell'app **TLF**) contiene le impostazioni del collegamento alla linea telefonica (TIP/RING), il gruppo **Serial bus** (**Serial Bus**) quelle del collegamento al bus dati o seriale. Nell'app: **Advanced settings** → **Panel settings** → **TLF** oppure **Panel settings** → **Serial Bus**.

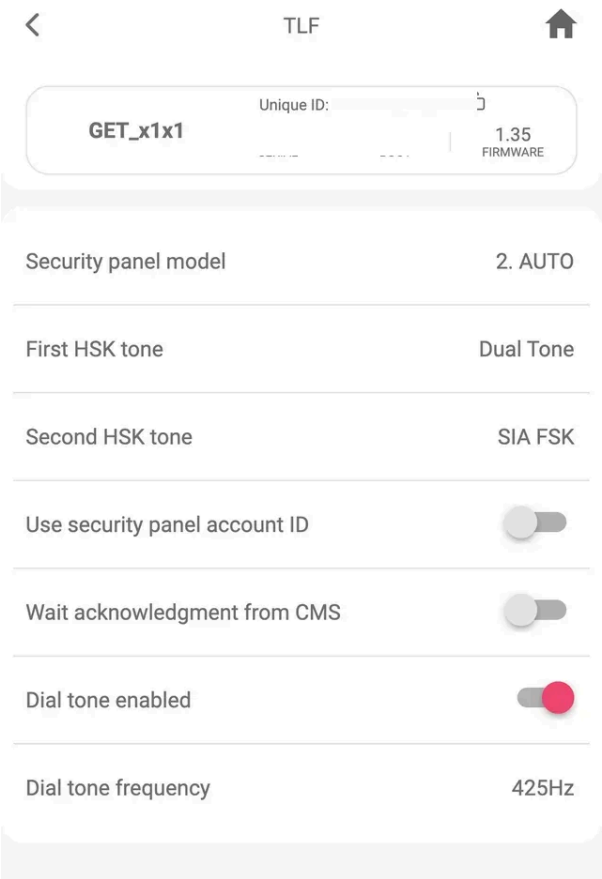


Figura 48. Protegus 2 – Panel settings → TLF: Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.

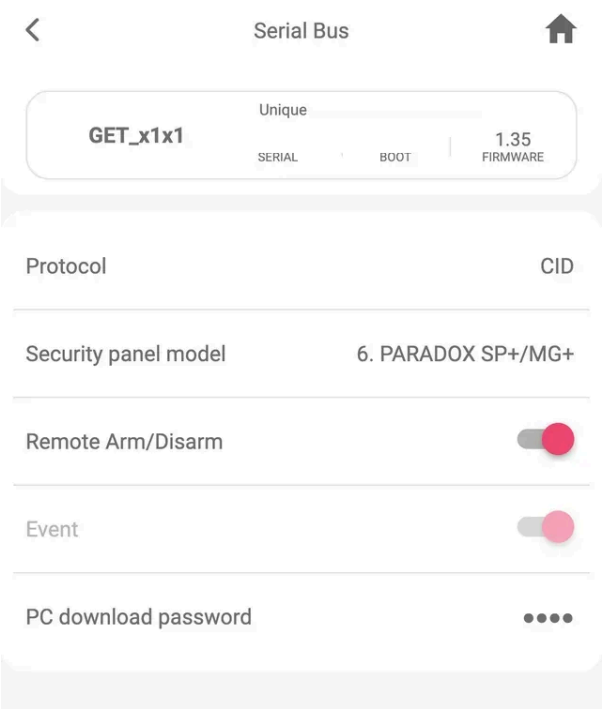


Figura 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm attivato, Event (sola lettura), PC download password.

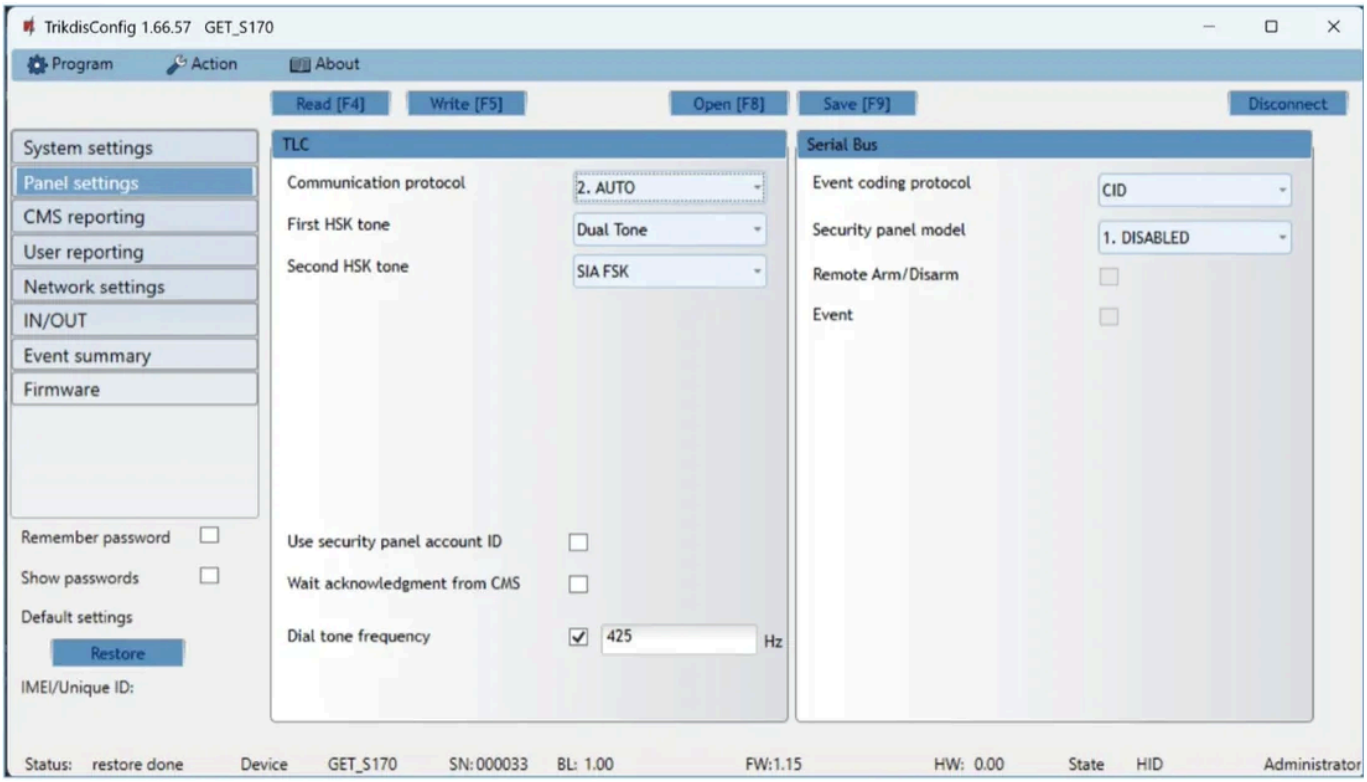


Figura 50. TrikdisConfig – Panel settings con collegamento TIP/RING: nel gruppo TLC Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; il gruppo Serial bus in questo caso è grigio.

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

- **Communication protocol** (Security panel model) – attivazione (**2. AUTO**) o disattivazione (**1. DISABLED**) dell'interfaccia di linea telefonica DTMF del comunicatore. Con il collegamento TIP/RING scegli il valore AUTO.
- **First HSK tone**, **Second HSK tone** – il tono di handshake della centrale, con cui il comunicatore riceve il combinatore della centrale (nella figura Dual Tone e SIA FSK).
- **Use security panel account ID** – con la spunta il comunicatore non invia il valore del proprio campo **Object ID**, ma il codice impianto impostato nella centrale e inviato dalla centrale.
- **Wait acknowledgment from CMS** – con la spunta, dopo l'invio di ogni evento il comunicatore attende la conferma del ricevitore IP che il messaggio è arrivato; se la conferma non arriva, non dà alla centrale il segnale di «kiss-off» e il combinatore telefonico della centrale ripete il messaggio.
- **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, Italia compresa). Nella pagina TLF dell'app c'è inoltre l'interruttore **Dial tone enabled**: attiva o disattiva il tono di linea; la frequenza si può modificare solo con il tono di linea attivato.

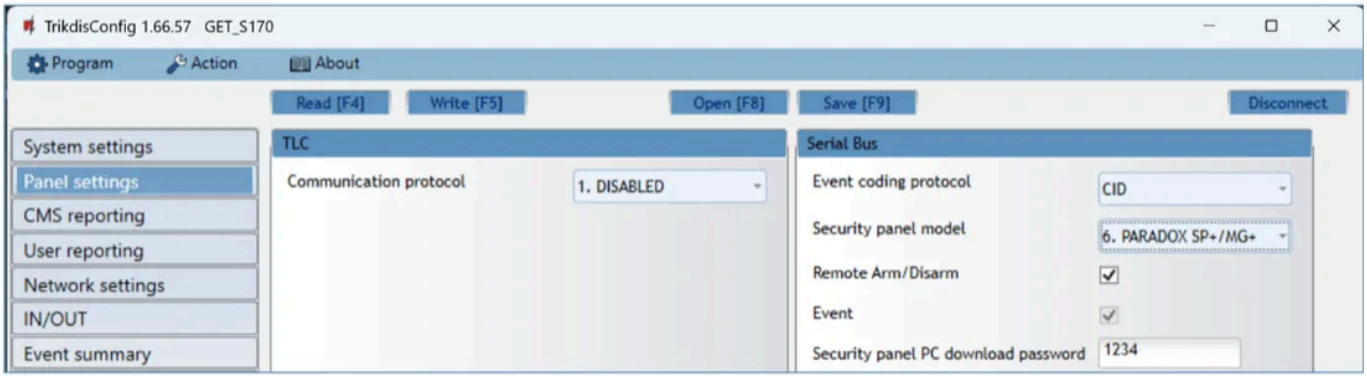


Figura 51. TrikdisConfig – Panel settings con collegamento al bus dati o seriale: Communication protocol 1. DISABLED; nel gruppo Serial bus Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm ed Event spuntati, Security panel PC download password inserita.

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

- **Event coding protocol** (Protocol) – il protocollo di trasmissione degli eventi: **CID** o **SIA**.
- **Security panel model** – il modello della centrale d'allarme collegata, dall'elenco (per il collegamento Keybus + TIP/RING della Paradox SP / SP+ / MG / MG+ scegli la voce **Paradox SP+/MG+ series KeyBus**, paragrafo 3.3.3).
- **Remote Arm/Disarm** – con la spunta il comunicatore comanda direttamente la centrale (inserimento e disinserimento da Protegus 2). È visibile solo con le centrali comandabili direttamente. Per il comando diretto bisogna configurare anche la centrale secondo il paragrafo 4.1.
- **Event** – con la spunta il comunicatore invia gli eventi della centrale alla centrale di vigilanza e a Protegus 2. L'app mostra questo interruttore, ma lì non si può modificare.
- **Security panel PC download password** (PC download password; con Texecom l'UDL passcode) – per il comando diretto di una centrale Paradox o Texecom, la password PC o UDL; deve coincidere con la password impostata nella centrale, la cui impostazione è descritta nel paragrafo 4.1.

6.4 CMS reporting (Reporting to CMS)

Il comunicatore invia gli eventi alla centrale di vigilanza tramite connessione IP – sulla rete cablata (LAN) o sulla rete mobile (SIM1, SIM2), nell'ordine impostato nel paragrafo 6.4.2. Gli eventi possono viaggiare su più canali: il canale **primario** 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 i protocolli TRK serve un ricevitore Trikdis, che riceve

gli eventi e li inoltra al software di vigilanza: per la connessione IP il ricevitore software IPcom (Windows o Linux), il ricevitore IP/SMS RL14 o il ricevitore multicanale RM14; i protocolli DC-09 e TL150 sono destinati rispettivamente ai ricevitori universali e ai ricevitori SUR-GARD (vedi sotto, **Protocol**).

6.4.1 Canali verso il ricevitore (CMS settings)

Nell'app: Advanced settings → Reporting to CMS → CMS settings, poi **Primary channel**, **Backup channel** o **Parallel channel** (al suo interno **Parallel primary channel** e **Parallel backup channel**). Attivando l'interruttore **Enabled** compaiono le impostazioni del canale.

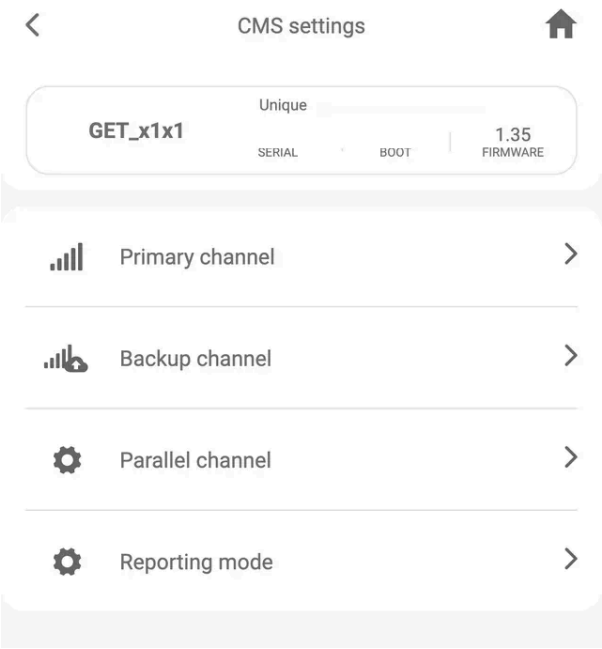


Figura 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel e Reporting mode.

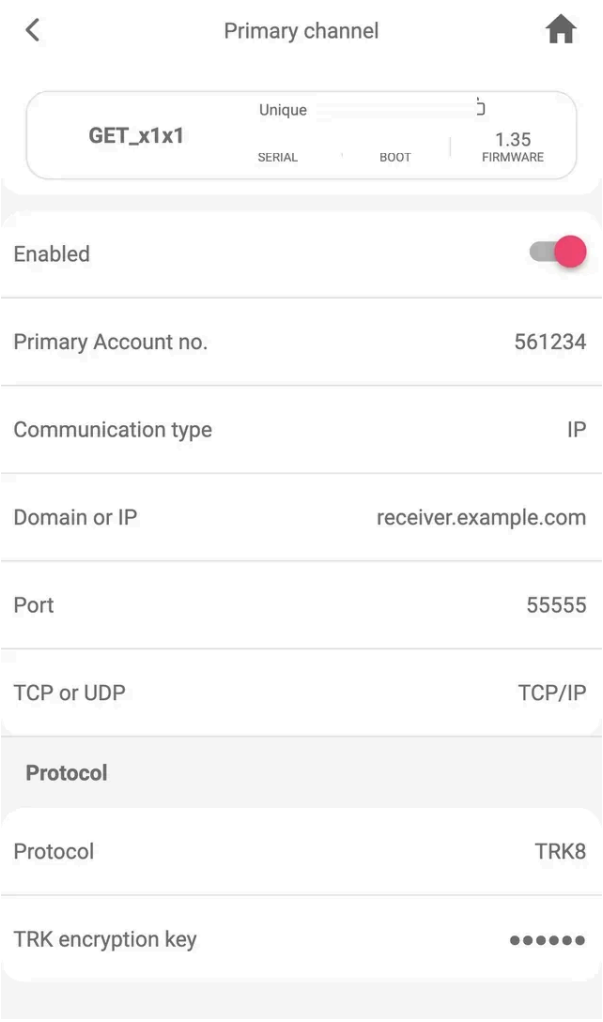


Figura 53. Protegus 2 – Primary channel su hardware x1x1: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 e la TRK encryption key.

In TrikdisConfig: la scheda **CMS settings** della pagina **CMS reporting**.

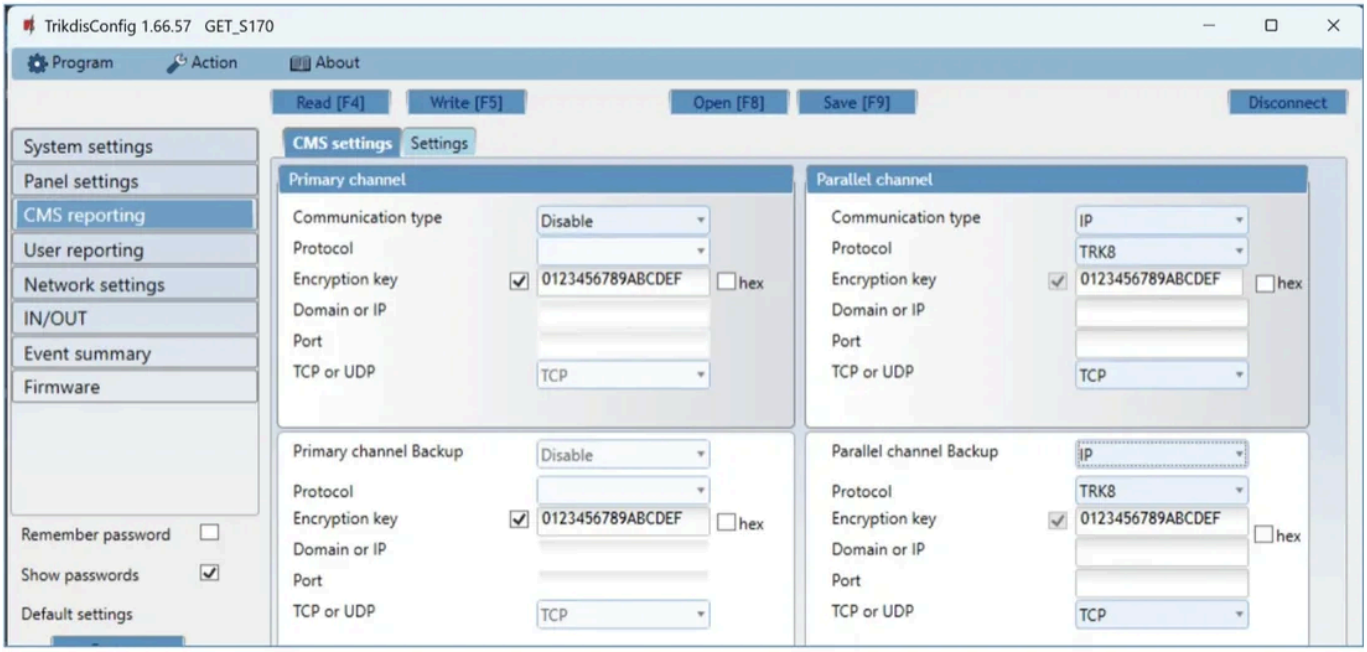


Figura 54. TrikdisConfig – CMS reporting, scheda CMS settings: canale primario e relativo canale di riserva, canale parallelo e relativo canale di riserva (nella figura il canale parallelo con impostazione IP / TRK8 / TCP).

Primary channel – canale primario

- **Communication type** – il tipo 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** (TRK encryption key; con i protocolli DC-09 **Enable encryption key** e **DC-09 encryption key**, con l'interruttore **HEX** per una chiave esadecimale) – la chiave di cifratura dei messaggi; deve essere la stessa nel comunicatore e nel ricevitore. Nell'app la TRK encryption key ha al massimo 6 caratteri, la DC-09 encryption key al massimo 16 (in HEX 32).
- **Domain or IP**, **Port** – il nome di dominio o l'indirizzo IP del ricevitore e la sua porta di rete.
- **TCP or UDP** – il protocollo di trasmissione.

Primary channel Backup – canale di riserva. Se attivato, prende in carico la comunicazione quando il canale primario non funziona; le sue impostazioni sono uguali a quelle sopra.

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

6.4.2 Test, PING e ordine delle connessioni

Nell'app: Advanced settings → Reporting to CMS → Settings (test, PING, tempi del canale di riserva, numero di ricevitore e di linea) e **Reporting to CMS → CMS settings → Reporting mode** (l'ordine dei percorsi di connessione). Nell'app accanto a ogni intervallo c'è un interruttore: **Enable test** per il Test period, **Enable ping** per l'IP ping period e **Test enabled** per il Communication path test; nella pagina Reporting mode i tipi di connessione compaiono con i nomi **LAN**, **SIM** (la SIM1) e **SIM2**.

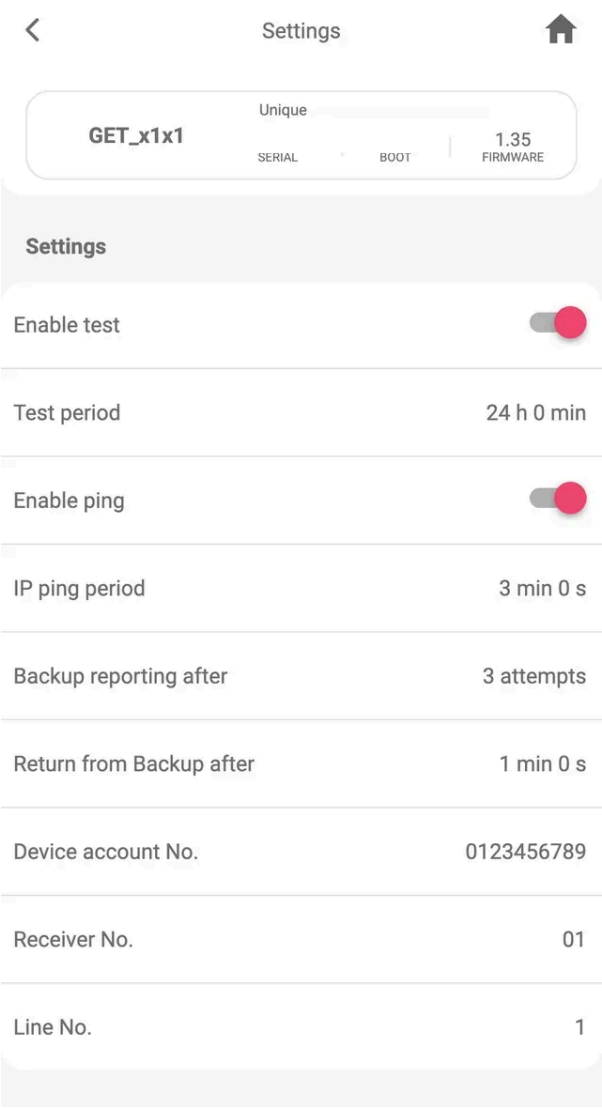


Figura 55. Protegus 2 – Reporting to CMS → Settings su hardware x1x1: Enable test e Test period, Enable ping e IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.

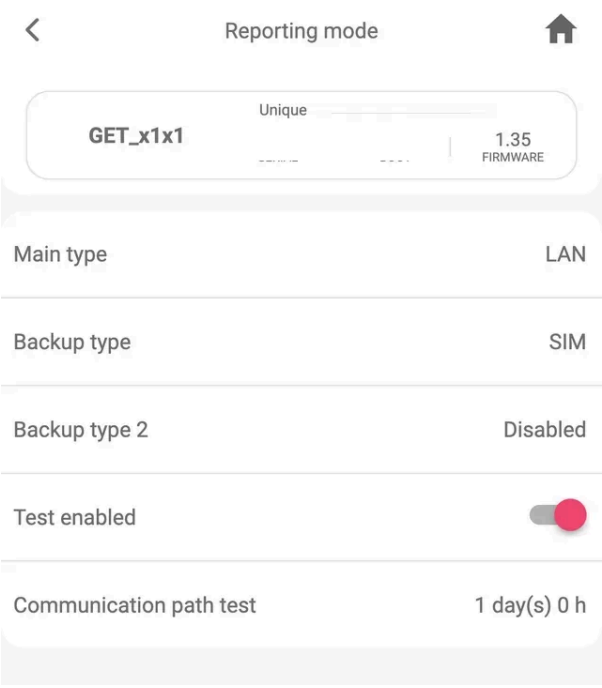


Figura 56. Protegus 2 – CMS settings → Reporting mode: Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled e Communication path test.

In TrikdisConfig: la scheda **Settings** della pagina **CMS reporting**.

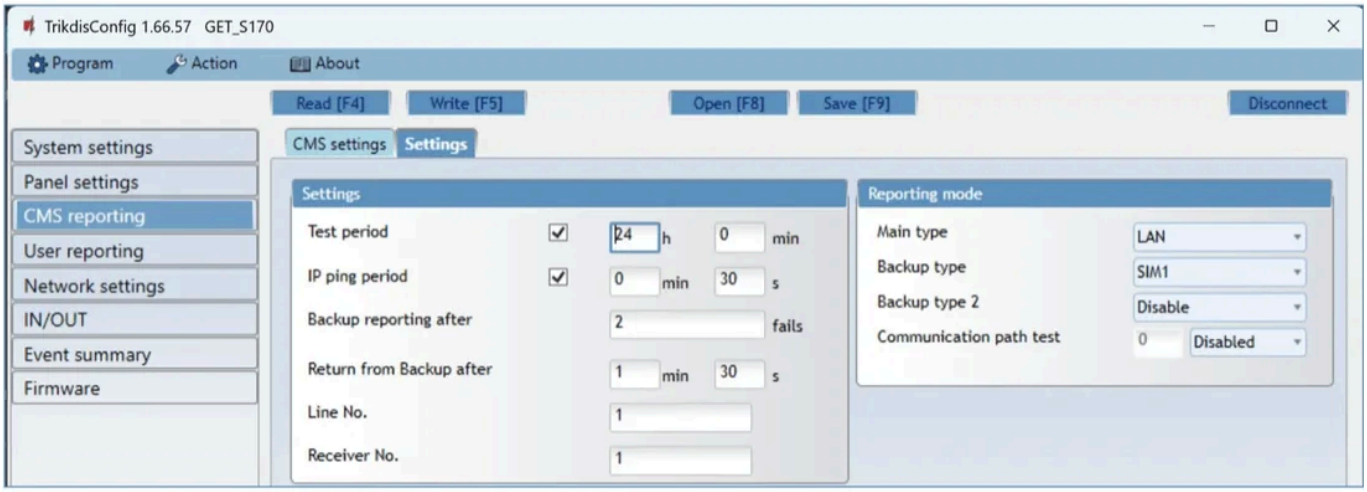


Figura 57. TrikdisConfig – CMS reporting, scheda Settings: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; nel gruppo Reporting mode Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **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 GET si trovano anche i campi **Line No.** (numero di linea del ricevitore) e **Receiver No.** (numero del ricevitore); sul GET non c'è un campo separato «Object ID in DC-09».

Gruppo Reporting mode – qui indichi su quale percorso il comunicatore deve comunicare con i canali verso la centrale di vigilanza e con Protegus 2. I tipi di connessione si indicano in ordine: se la connessione indicata in **Main type** non si stabilisce, il comunicatore passa a quella del **Backup type**, e così via; se il messaggio è stato inviato con successo sul percorso di riserva, trascorso il tempo impostato (Return from backup after) riprova il percorso principale.

- **Main type** – il tipo della connessione principale con il ricevitore e con Protegus 2: **LAN**, **SIM1** o **SIM2**.
- **Backup type** – il tipo della connessione di riserva (LAN, SIM1, SIM2).
- **Backup type 2** – il tipo della seconda connessione di riserva (LAN, SIM1, SIM2).
- **Communication path test** – a quali intervalli il comunicatore prova i tipi di connessione scelti (LAN, SIM1, SIM2).

6.5 User reporting (Protegus Cloud)

Con il servizio Protegus 2 l'utente sorveglia e comanda a distanza il comunicatore e il sistema a esso collegato; dettagli: web.protegus.app. Nell'app: **Advanced settings** → **User reporting** → **Cloud**; in TrikdisConfig la scheda **PROTEGUS Cloud** della pagina **User reporting**.

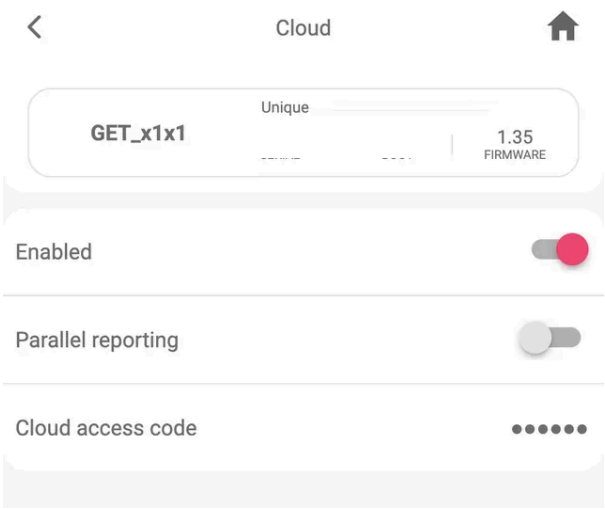


Figura 58. Protegus 2 – User reporting → Cloud: Enabled, Parallel reporting, Cloud access code.

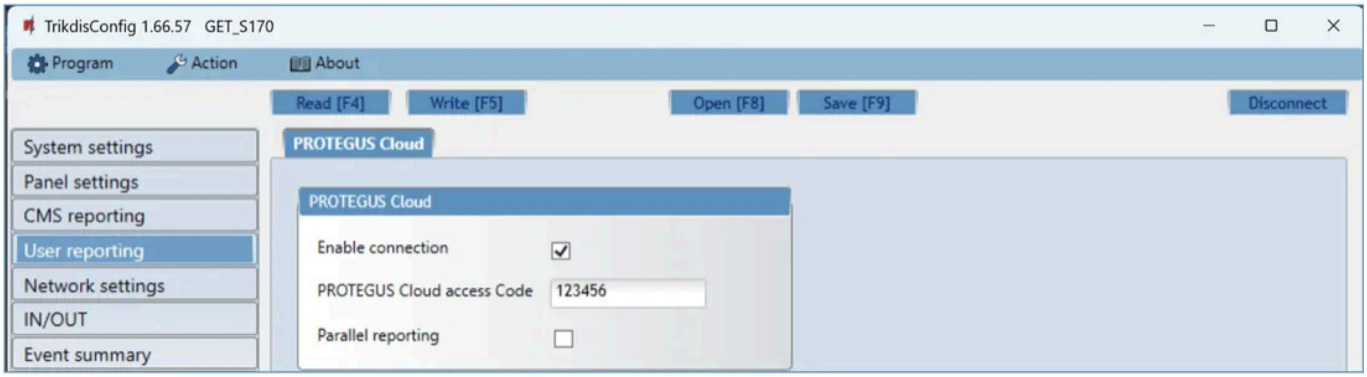


Figura 59. TrikdisConfig – User reporting, scheda PROTEGUS Cloud: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – abilita il servizio Protegus 2: il dispositivo scambia dati con l'app Protegus 2 e TrikdisConfig lo raggiunge anche a distanza.
- **PROTEGUS Cloud access Code** (Cloud access code) – codice a 6 cifre per la connessione a Protegus 2 (di fabbrica `123456`). Se lo cambi in TrikdisConfig, devi cambiarlo anche nell'app Protegus 2.
- **Parallel reporting** (nell'app è visibile solo se il firmware lo supporta) – con la spunta i messaggi vanno contemporaneamente sul canale primario (alla centrale di vigilanza) e a Protegus 2; Protegus 2 e gli utenti ricevono il messaggio solo dopo che è stato inviato alla centrale di vigilanza.

6.6 Network settings

6.6.1 LAN (Ethernet)

Queste impostazioni vanno indicate se il comunicatore è collegato alla rete locale cablata (LAN). Nell'app: **Advanced settings** → **Network settings** → **LAN**; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** e **DNS2** si possono modificare solo con **Use DHCP** disattivato. In TrikdisConfig la scheda **LAN** della pagina **Network settings**, gruppo **Ethernet settings**.

Che cosa deve offrire la rete? È il comunicatore stesso ad avviare la connessione in uscita verso il ricevitore della centrale di vigilanza e verso il cloud Protegus, quindi sul router **non serve aprire né inoltrare porte**, e non servono nemmeno un indirizzo IP pubblico fisso o un DNS dinamico. Ciò che serve:

- una porta Ethernet libera sul router o sullo switch;
- DHCP (impostazione di fabbrica), oppure indirizzo IP fisso, subnet mask, gateway e DNS forniti dall'amministratore di rete;
- il traffico in uscita consentito verso l'indirizzo e la porta del ricevitore (TCP o UDP, secondo l'impostazione del ricevitore) e verso il cloud Protegus.

Su una rete filtrata – aziendale, di un ente – concordalo prima con l'amministratore di rete: sui router domestici di norma tutte le connessioni in uscita sono consentite, mentre su una rete protetta da firewall può servire una regola apposita.

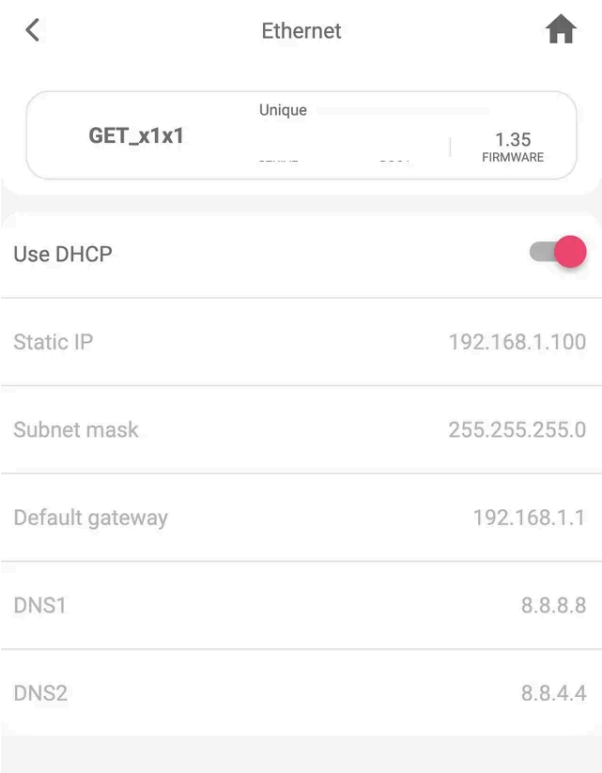


Figura 60. Protegus 2 – Network settings → LAN: Use DHCP attivato; i campi Static IP, Subnet mask, Default gateway, DNS1 e DNS2 in questo caso sono grigi.



Figura 61. TrikdisConfig – Network settings, scheda LAN, gruppo Ethernet settings: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

- **Use DHCP** – con la spunta il comunicatore si registra automaticamente sulla rete (riceve l'indirizzo dal server DHCP del router). Se la registrazione automatica non riesce, gli indirizzi vanno inseriti manualmente:
- **Static IP** – l'indirizzo IP fisso del comunicatore con l'impostazione manuale.
- **Subnet mask** – la subnet mask con l'impostazione manuale.
- **Default gateway** – l'indirizzo del gateway (router) con l'impostazione manuale.
- **DNS1, DNS2** – server dei nomi (DNS, Domain Name System: fornisce l'indirizzo IP corrispondente a un nome di dominio); servono se nel campo **Domain or IP** del canale hai indicato il ricevitore 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 fornitore di Internet.

6.6.2 SIM1 e SIM2

Queste impostazioni vanno indicate separatamente per ogni scheda SIM inserita; le impostazioni degli slot SIM1 e SIM2 sono identiche.

Prima dell'uso assicurati che la scheda SIM sia attiva e funzionante e che sulla scheda sia abilitato anche il servizio dati mobile.

Nell'app: **Advanced settings** → **Network settings** → **SIM** (la SIM1) o **SIM2**. In TrikdisConfig la scheda **SIM1** o **SIM2** della pagina **Network settings**, gruppo **SIM card**.

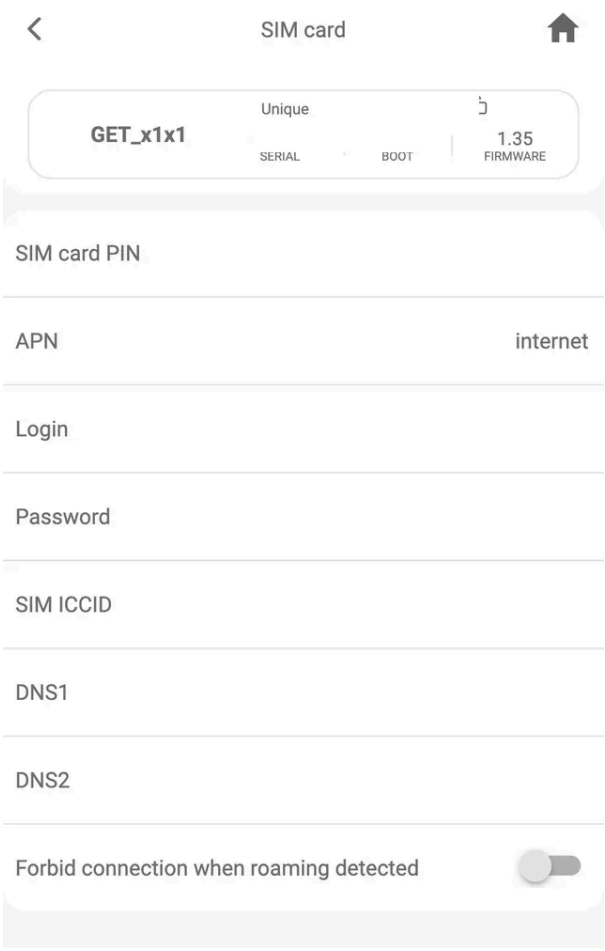


Figura 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 e l'interruttore Forbid connection when roaming detected.

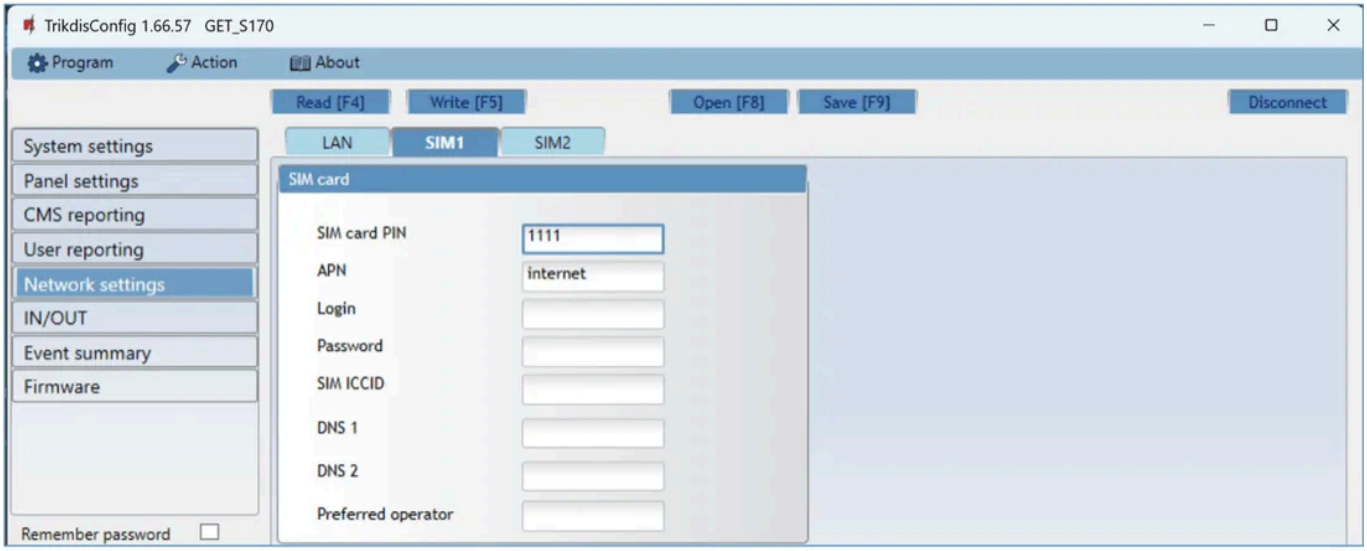


Figura 63. TrikdisConfig – Network settings, scheda SIM1, gruppo SIM card: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (la scheda SIM2 è uguale).

- **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 può restare il valore di fabbrica del campo.
- **APN** – il punto di accesso dell'operatore (Access Point Name); senza di esso il dispositivo non si collega a Internet. Il valore si trova sul sito dell'operatore della scheda SIM; `internet` è di uso generale e funziona sulla rete di molti operatori. Gli APN noti degli operatori sono elencati nell'articolo sugli APN (per le schede IoT / M2M l'operatore fornisce un APN a parte, vedi il paragrafo 2.3).
- **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.
- **DNS1, DNS2** – server dei nomi; servono se nel campo **Domain or IP** del canale hai indicato il ricevitore con un nome di dominio. Il valore predefinito è il DNS pubblico di Google; 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 collega solo alla rete dell'operatore scelto. Si trova **solo in TrikdisConfig**.

Nella pagina SIM dell'app, al posto di Preferred operator, c'è l'interruttore **Forbid connection when roaming detected**: se attivato, il comunicatore non si connette quando rileva il roaming. Su hardware **M15**, con firmware **1.17** o successivo, nella pagina SIM compaiono anche le impostazioni **Generation** e **Bands**: con queste puoi limitare quale tecnologia di rete mobile e quali bande di frequenza usa il comunicatore.

6.7 IN/OUT

Qui indichi il ruolo dei due morsetti I/O a doppia funzione del comunicatore: **Disabled** (non usato), **IN** (ingresso) o **OUT** (uscita; sul GET è l'impostazione di fabbrica). Per un ingresso bisogna indicare anche, nel campo **Type**, il tipo di circuito collegato (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Agli ingressi si possono collegare altri sensori: quando il sensore viene violato, il comunicatore invia un proprio evento, con il codice Contact ID (SIA) assegnato all'ingresso, alla centrale di vigilanza e a Protegus 2.

Nell'app: **Advanced settings** → **IN/OUT**, poi il morsetto **1** o **2**: la **Function** (Disabled, IN, OUT) e, per un ingresso, il **Type**; nelle parti **Alarm** e **Tamper** i messaggi di evento e di ripristino inviati quando l'ingresso viene violato. In TrikdisConfig la pagina **IN/OUT**.

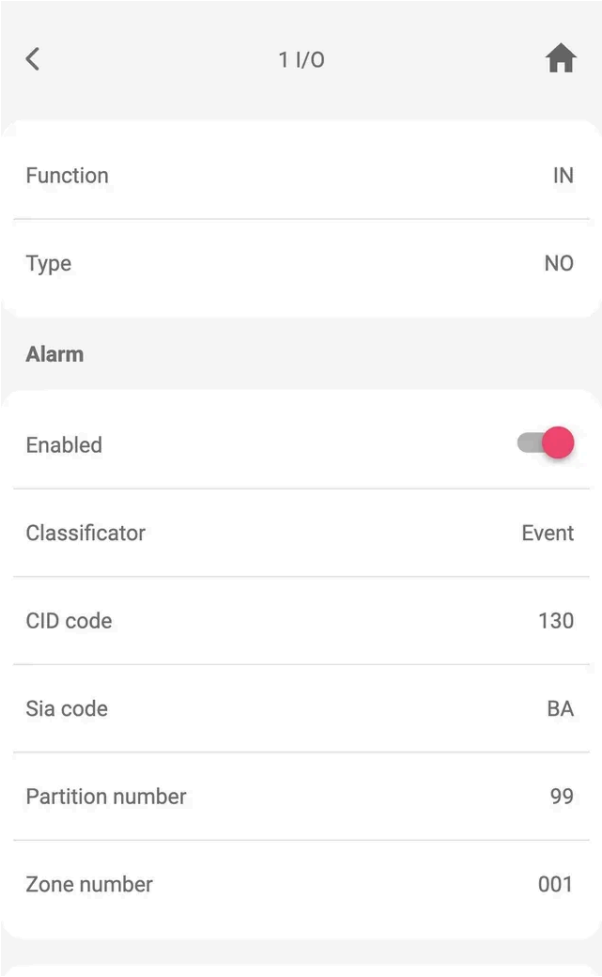


Figura 64. Protegus 2 – IN/OUT, morsetto 1: Function IN, Type NO; l'evento Alarm Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.

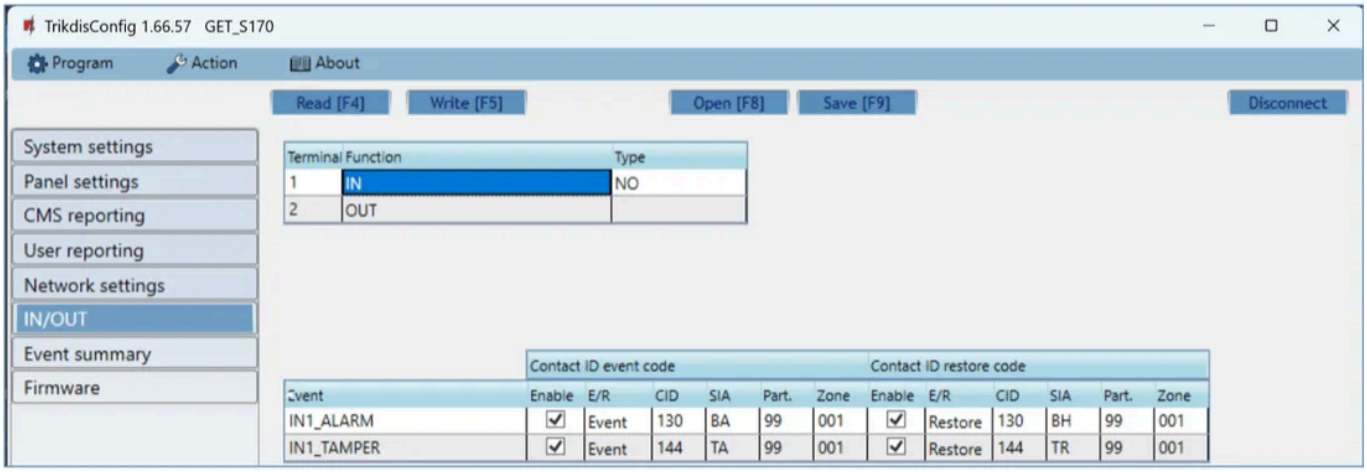


Figura 65. TrikdisConfig – pagina IN/OUT: il morsetto 1 è un ingresso (IN, NO), il 2 un'uscita (OUT); sotto, gli eventi di allarme e di manomissione dell'ingresso 1 con codice CID e SIA.

Quando il sensore collegato all'ingresso viene violato, il comunicatore invia un allarme (**INx_ALARM**, Contact ID 130, SIA BA; ripristino BH); quando viene violato il circuito tamper, invia un evento di manomissione (**INx_TAMPER**, 144, SIA TA; ripristino TR); nella tabella compaiono gli eventi di ogni morsetto impostato come ingresso. Le colonne della tabella:

- **Enable** (Enabled) – abilita l'invio del messaggio alla centrale di vigilanza e a Protegus 2.

- **E/R** (Classificator) – il tipo di messaggio: Event (evento) o Restore (ripristino).
- **CID** (CID code) – il codice Contact ID (modificabile, oppure può restare quello di fabbrica); quando l'ingresso viene violato, il messaggio va a Protegus 2 e alla centrale di vigilanza con questo codice.
- **SIA** (Sia code) – il codice SIA (modificabile, oppure può restare quello di fabbrica).
- **Part.** (Partition number) – il numero dell'area nel messaggio (sia per l'evento sia per il ripristino).
- **Zone** (Zone number) – il numero della zona nel messaggio.

6.8 Event summary (System events)

Qui puoi abilitare, disabilitare e modificare i messaggi interni propri del dispositivo. Un messaggio disabilitato qui non viene inviato, indipendentemente da qualsiasi altra impostazione. Nell'app: **Advanced settings** → **System events**, i messaggi sono negli elenchi **Event** e **Restore**; per modificarli scegli il messaggio. In TrikdisConfig la pagina **Event summary**.

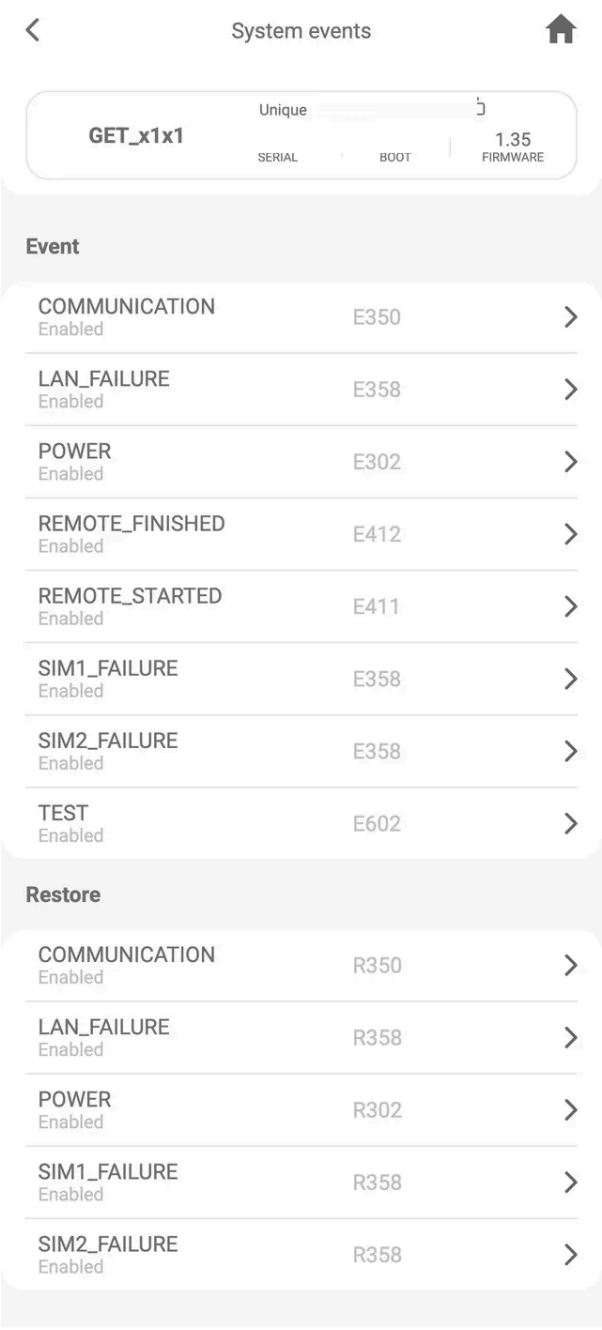


Figura 66. Protegus 2 – System events: l'elenco Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) e l'elenco Restore.

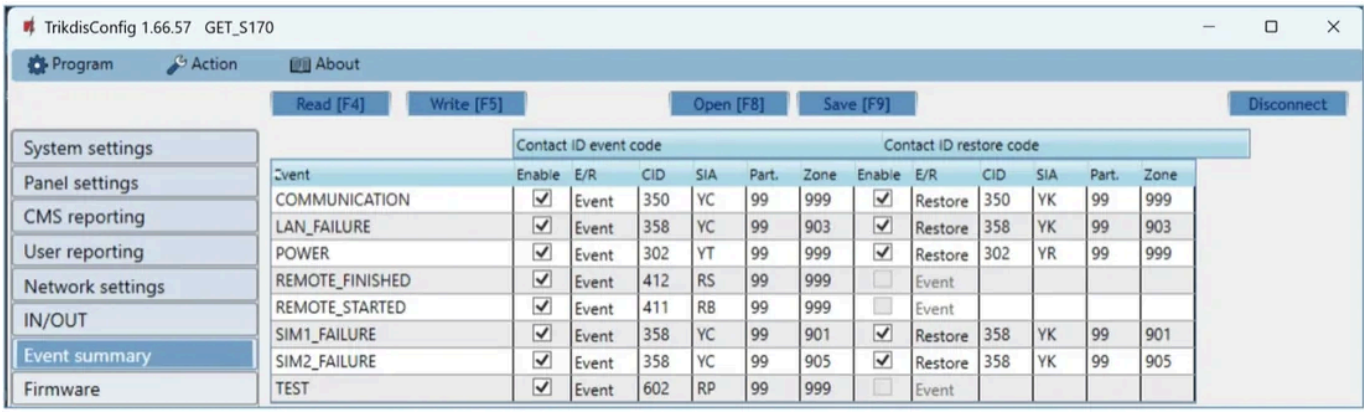


Figura 67. TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo con codice CID e SIA, con l'area 99.

I messaggi interni del GET (tra parentesi il codice Contact ID di fabbrica e la zona):

- **COMMUNICATION** (350, zona 999) – guasto della connessione tra centrale e comunicatore; il ripristino è un messaggio a parte.
- **LAN_FAILURE** (358, zona 903) – guasto della connessione di rete cablata (LAN); il ripristino è un messaggio a parte.
- **POWER** (302, zona 999) – tensione di alimentazione bassa; il ripristino è un messaggio a parte.
- **REMOTE_FINISHED** (412) – fine della programmazione a distanza con TrikdisConfig (disconnessione).
- **REMOTE_STARTED** (411) – connessione a distanza per la programmazione del GET con TrikdisConfig.
- **SIM1_FAILURE** (358, zona 901) – guasto della connessione alla rete mobile sulla SIM1; il ripristino è un messaggio a parte.
- **SIM2_FAILURE** (358, zona 905) – guasto della connessione alla rete mobile sulla SIM2; il ripristino è un messaggio a parte.
- **TEST** (602) – rapporto di prova periodico.

L'attivazione e l'intervallo del messaggio periodico TEST si impostano nel campo **Test period** (paragrafo 6.4.2).

- **Enable** (Enabled) – con la spunta l'invio del messaggio è abilitato.
- Per ogni messaggio si possono modificare il codice Contact ID (SIA) e il numero di zona e di area.

6.9 Ripristino delle impostazioni di fabbrica

Dall'app Protegus 2 le impostazioni di fabbrica **non** si possono ripristinare: serve il pulsante **Restore** di TrikdisConfig o il pulsante **RESET** del dispositivo.

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 68. TrikdisConfig – il pulsante Restore del gruppo Default settings.

Le impostazioni di fabbrica si possono ripristinare 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.

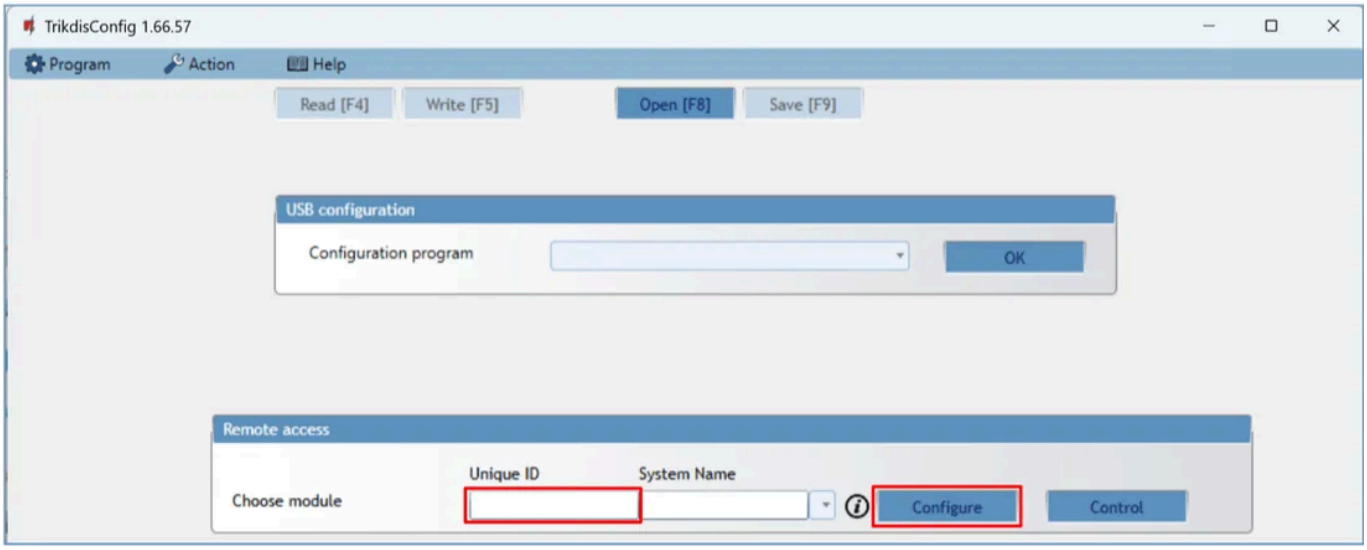


Figura 69. TrikdisConfig – il gruppo Remote access: il campo Unique ID, l'elenco System name e il pulsante Configure.

L'identificativo univoco del GET è l'**IMEI / Unique ID**; si legge sull'etichetta del dispositivo e sull'adesivo della scatola. L'accesso a distanza funziona solo se la scheda SIM è attiva e il suo codice PIN è inserito oppure la richiesta del PIN è disattivata – **oppure** il comunicatore è collegato con un cavo di rete (LAN) –; nella pagina **User reporting** → **PROTEGUS Cloud** è spuntato **Enable connection** (paragrafo 6.5); il LED **POWER** è verde fisso; il LED **NETWORK LTE** è verde fisso e lampeggia in giallo (con la sola connessione cablata è il LED **NETWORK LAN** a essere verde fisso). L'inizio e la fine della programmazione a distanza vengono segnalati dal comunicatore con i messaggi REMOTE_STARTED e REMOTE_FINISHED (paragrafo 6.8).

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.

Se il comunicatore trasmette sia sulla rete cablata sia sulla rete mobile (paragrafo 6.4.2, Reporting mode), conviene fare la prova su entrambi i percorsi: scollega il cavo LAN, genera un evento e verifica che arrivi alla centrale di vigilanza anche tramite la scheda SIM; poi ricollega il cavo.

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.

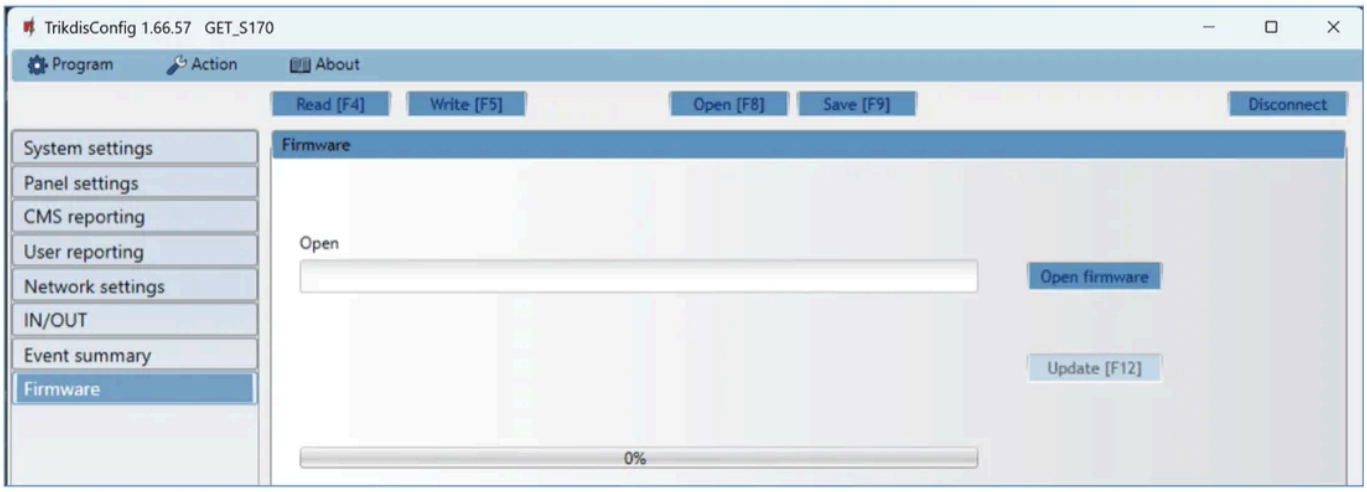


Figura 70. TrikdisConfig – pagina Firmware: pulsante Open firmware, pulsante Update [F12] e indicatore di avanzamento.

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.

Alcune funzioni del GET richiedono una determinata versione del firmware:

- **1.08** o successivo: configurazione dall'app Protegus 2 (Advanced settings, paragrafo 2.2 e capitolo 6);
- **1.17** o successivo, su versione hardware **M15**: le impostazioni **Generation** e **Bands** nella pagina SIM dell'app (paragrafo 6.6.2);
- **1.21** o successivo: il collegamento Keybus + TIP/RING della Paradox SP / SP+ / MG / MG+ (paragrafo 3.3.3);
- **1.31** o successivo, su versione hardware **x1x1**: gli identificativi (Account No., Device account No.) nell'app si trovano tra le impostazioni CMS (paragrafo 6.2).

10. Risoluzione dei problemi e domande frequenti

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

Il LED NETWORK LTE non si accende – nessuna rete mobile

1. Guarda i lampeggi del LED **TROUBLE**: 2 = guasto della scheda SIM1, 3 = guasto della scheda SIM2 (paragrafo 1.6).
2. Verifica che la scheda SIM sia attiva, abbia un servizio dati e sia inserita correttamente nello slot (la SIM1 al centro della scheda, la SIM2 sul bordo sinistro; paragrafo 3.1).
3. Se sulla scheda la richiesta del PIN è attiva, inserisci il PIN nella scheda **Network settings** → **SIM1** (o **SIM2**), oppure disattiva la richiesta del PIN con un telefono.
4. Verifica l'APN (paragrafo 2.3): per le schede IoT / M2M l'operatore fornisce un APN a parte.
5. Controlla l'antenna: è avvitata, non è in un contenitore metallico, il livello del segnale è adeguato (il LED NETWORK LTE lampeggia in giallo almeno 3 volte; paragrafi 1.6 e 3.2).
6. Se il comunicatore trasmette sulla rete cablata, la mancanza della rete mobile di per sé non lo blocca: secondo l'ordine del **Reporting mode** (paragrafo 6.4.2) invia sul percorso successivo disponibile – ma così manca il percorso di riserva, conviene sistemarlo.

Il LED NETWORK LAN non si accende – nessuna rete cablata

1. 1 lampeggio del LED **TROUBLE** indica un guasto nel collegamento fisico della rete cablata: controlla il cavo LAN a entrambe le estremità e che la porta del router o dello switch sia attiva (paragrafo 1.6).
2. Se il cavo è a posto, guarda la scheda **Network settings** → **LAN**: con il DHCP deve essere il router a fornire l'indirizzo; con un indirizzo fisso, Static IP, Subnet mask e Default gateway devono essere adatti alla rete locale (paragrafo 6.6.1).
3. Se hai indicato il ricevitore con un nome di dominio, anche gli indirizzi DNS devono funzionare nella rete (DNS1, DNS2).

La rete c'è, 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. Verifica l'indirizzo del ricevitore, la porta, l'impostazione TCP/UDP, il protocollo e la chiave di cifratura (**CMS reporting** → **CMS settings**, paragrafo 6.4.1); la chiave deve essere la stessa nel comunicatore e nel ricevitore.
2. Guarda l'impostazione del **Reporting mode** (paragrafo 6.4.2): il **Main type** deve essere un percorso effettivamente disponibile nel sito (c'è il cavo LAN, oppure c'è una scheda SIM nello slot indicato), e ci deve essere anche un percorso di riserva.
3. Se il ricevitore è indicato con un nome di dominio, verifica l'impostazione DNS sul percorso su cui il comunicatore trasmette (**Network settings** → **LAN**, oppure **SIM1 / SIM2** → **DNS1, DNS2**).

4. Sulla rete mobile verifica che il piano dati della scheda SIM non blocchi la porta necessaria (alcune schede M2M consentono solo determinati indirizzi); sulla rete cablata il firewall locale deve consentire in uscita la porta del ricevitore.
5. Se la centrale non invia eventi (il LED DATA non si accende), la causa è sul lato della centrale: vedi il punto seguente.

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 verifica 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 attivato, in modalità DTMF, con formato Contact ID e con un numero di telefono impostato (paragrafo 4.2), e il **Communication protocol** deve essere **2. AUTO** (paragrafo 6.3).

Su quale percorso va l'evento: LAN o SIM?

Su quello dato dall'ordine del **Reporting mode** (paragrafo 6.4.2): sul percorso del **Main type**; se questo non funziona, su quello del **Backup type**, poi del **Backup type 2**. Se il messaggio è stato inviato sul percorso di riserva, trascorso il tempo **Return from backup after** il comunicatore riprova il percorso principale, e il **Communication path test** prova periodicamente tutti i percorsi. Anche la connessione di Protegus 2 usa lo stesso percorso. Sulla rete cablata il traffico dati mobile non si consuma.

A cosa servono i due slot SIM?

Con le schede di due operatori diversi anche la rete mobile diventa a doppio percorso: nel Reporting mode SIM1 e SIM2 sono tipi di connessione distinti, ognuno può essere il percorso principale o quello di riserva (paragrafo 6.4.2). Le due schede vanno configurate separatamente (**Network settings** → **SIM1**, **SIM2**: PIN, APN; paragrafo 6.6.2); il guasto della SIM2 è segnalato da 3 lampeggi del LED TROUBLE e dal messaggio SIM2_FAILURE (paragrafi 1.6 e 6.8). Il comunicatore funziona anche con una sola scheda.

DSC: tutti gli allarmi arrivano come allarme generico E130

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). Il collegamento contemporaneo del Keybus e dei morsetti TIP/RING non è disponibile sul GET (è una funzione del GT+). Se la centrale di vigilanza si aspetta il codice corrispondente al tipo di zona (per esempio incendio: E110), collega il GET solo ai morsetti TIP/RING della centrale e programma il combinatore (paragrafi 3.3.9 e 4.2): così vengono inviati i codici Contact ID propri della centrale, ma non c'è il comando diretto – 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+, invece della porta seriale, si può usare anche il collegamento Keybus + TIP/RING (paragrafo 3.3.3), 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 comando diretto **Panel settings → Remote Arm/Disarm** deve essere spuntato e la centrale deve essere configurata 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 comandabile direttamente.
2. Con l'inserimento tramite zona chiave (paragrafo 3.4) il morsetto deve essere **OUT** nella pagina **IN/OUT** (l'impostazione di fabbrica del GET), la zona della centrale deve essere una zona chiave e in Protegus 2 l'uscita deve essere assegnata all'area, con la stessa modalità della centrale (impulsiva 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 pagina **User reporting → PROTEGUS Cloud** deve essere spuntato **Enable connection** (paragrafo 6.5).
2. Durante l'aggiunta bisogna inserire il **PROTEGUS Cloud access Code** impostato nel dispositivo; se hai cambiato il codice in TrikdisConfig, cambialo anche nell'app.
3. Inserisci l'IMEI esattamente, dall'etichetta del dispositivo o dall'adesivo della scatola (oppure scansiona il codice QR).
4. Ci deve essere Internet funzionante almeno su uno dei percorsi: il LED NETWORK LTE è verde e lampeggia in giallo (scheda SIM con servizio dati e APN corretto), oppure il LED NETWORK LAN è verde (cavo LAN). Il LED DATA deve spegnersi dopo un evento.

Non riesco ad accedere a distanza con TrikdisConfig

1. Il dispositivo deve essere online (NETWORK LTE verde, lampeggia in giallo, oppure NETWORK LAN verde) e la connessione Protegus deve essere abilitata (**Enable connection**).
2. **CMS reporting → Settings → IP ping period** non deve essere più lungo di 5 minuti: il PING mantiene la connessione necessaria per l'accesso a distanza.
3. Verifica la password di amministratore o di installatore.

Posso configurare il comunicatore dall'app?

Sì: con firmware 1.08 o successivo la maggior parte delle impostazioni è disponibile nel menu **Settings → Advanced settings** di Protegus 2 (paragrafo 2.2 e capitolo 6). Solo in TrikdisConfig ci sono: il ripristino delle impostazioni di fabbrica (paragrafo 6.9), il **Preferred operator** (paragrafo 6.6.2) e l'aggiornamento manuale del firmware (capitolo 9); l'interruttore **Event** del Serial bus è mostrato dall'app, ma non modificato. Se accedi con il codice installatore, puoi modificare solo i gruppi consentiti dall'amministratore (paragrafo 6.2).

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 6.9): con l'alimentazione accesa, tienilo premuto per 10 secondi. Tutte le impostazioni vengono cancellate. Dall'app il ripristino non si può avviare.

Quanto traffico dati usa il dispositivo?

I messaggi di evento e i PING sono molto piccoli; il traffico dipende soprattutto dal periodo di PING e dalla frequenza dei rapporti di prova. Per un normale sistema domestico il traffico mensile resta di solito sotto i 10 MB. Il valore esatto dipende dalle impostazioni e dall'unità di fatturazione dell'operatore, perciò con una

scheda a dati limitati conviene controllare il traffico del primo mese. Finché il comunicatore trasmette sulla rete cablata, il traffico dati della scheda SIM non si consuma.

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 della manutenzione scollega l'apparecchiatura dall'alimentazione.
- Le modifiche, trasformazioni e riparazioni non autorizzate dal produttore invalidano la garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare l'apparecchio inutilizzabile e i suoi componenti nei rifiuti domestici. Il simbolo del bidone barrato (RAEE) sul dispositivo indica che va conferito 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: guida rapida per l'installatore – i passi del collegamento DSC in breve.
- Comunicatore Trikdis + centrale d'allarme Paradox: guida rapida per l'installatore – i passi del collegamento Paradox in breve.
- DSC PowerSeries NEO e i comunicatori Trikdis: compatibilità e soluzioni – perché la NEO non si può collegare 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 – GET – qui si trova anche la tabella di conversione dei codici Contact ID → SIA (appendice).

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

Prodotti correlati

Trikdis GET Ethernet + 4G comunicatore intelligente

Trikdis CRP2 cavo di collegamento porta seriale per pannelli allarme Paradox

Trikdis ANT04 antenna GSM adesiva con cavo da 2,5m

Trikdis ME301M antenna GSM magnetica con cavo da 2,5m

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-get