Comunicatore G16 – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente del comunicatore Trikdis G16: collegamento al bus dati o alla porta seriale della centrale d'allarme, programmazione della centrale, SIM e configurazione in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-g16

Indice

1. Panoramica

- 1.1 A cosa serve, come funziona
- 1.2 Centrali d'allarme compatibili
- 1.3 Versioni
- 1.4 Caratteristiche principali
- 1.5 Le parti del comunicatore
- 1.6 Morsetti
- 1.7 Segnalazioni dei LED
- 1.8 Dati tecnici

2. Messa in servizio rapida con TrikdisConfig

- 2.1 Preparazione
- 2.2 Tipo di centrale e controllo diretto
- 2.3 Collegamento all'app Protegus 2
- 2.4 Collegamento alla centrale di vigilanza

3. Installazione e collegamento

- 3.1 Le fasi dell'installazione
- 3.2 Posizionamento e antenna
- 3.3 Collegamento alla centrale d'allarme
  - 3.3.1 DSC PowerSeries
  - 3.3.2 Paradox
  - 3.3.3 UTC Interlogix (Caddx) NetworX
  - 3.3.4 Texecom Premier / Premier Elite
  - 3.3.5 Crow Runner
  - 3.3.6 Pyronix
  - 3.3.7 Honeywell Ademco Vista
  - 3.3.8 InnerRange Inception e Integriti
- 3.4 Collegamento della zona a chiave
- 3.5 Collegamento degli ingressi
- 3.6 Collegamento di un'uscita con relè
- 3.7 Collegamento dell'espansore iO-8
- 3.8 Collegamento dei moduli W485 ed E485
- 3.9 Accensione e prima verifica
- A TRIKDIS átjelző elindítása

4. Programmazione della centrale d'allarme

- 4.1 DSC
- 4.2 Paradox
- 4.3 Texecom
- 4.4 UTC Interlogix (Caddx)
- 4.5 Crow e Pyronix
- 4.6 Honeywell Ademco Vista
- 4.7 InnerRange Inception e Integriti

5. Controllo a distanza con l'app Protegus 2

- 5.1 Aggiunta del dispositivo
- A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Controllo diretto con il codice tastiera
5.3 Inserimento con zona a chiave
5.4 Inserimento e disinserimento dall'app
5.5 Controllo con messaggi SMS

6. TrikdisConfig – le impostazioni in dettaglio

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

7. Programmazione a distanza

8. Verifica del funzionamento del comunicatore

9. Aggiornamento del firmware

10. Risoluzione dei problemi e domande frequenti

11. Norme di sicurezza

Vedi anche

1. Panoramica

Il G16 è il **comunicatore cellulare a collegamento diretto** di Trikdis: non si collega all'uscita della linea telefonica della centrale d'allarme, ma al **bus della tastiera o alla porta seriale** della centrale. Legge gli eventi direttamente dalla centrale – insieme al numero di zona, di area e di utente – e li trasmette tramite connessione dati mobile al ricevitore della centrale di vigilanza e al cloud Protegus, nell'app dell'utente. Funziona con le centrali DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell e Crow supportate; con i modelli **controllabili direttamente** l'utente inserisce e disinserisce dall'app Protegus 2 con il proprio codice tastiera, senza una zona a chiave separata. L'app Protegus 2 può essere usata con tutte le centrali d'allarme supportate dal G16, indipendentemente dal produttore. Per centrali di altre marche che hanno solo un'uscita per linea telefonica è indicato il comunicatore G16T (TIP/RING).

1.1 A cosa serve, come funziona

- **Legge direttamente la centrale.** Sul bus della centrale ogni evento arriva subito al comunicatore, con la numerazione propria della centrale; non occorre configurare il combinatore della centrale e non c'è nessuna composizione Contact ID.
- **Trasmette alla centrale di vigilanza.** Invia gli eventi via IP al ricevitore software o hardware Trikdis (protocollo TRK) – che funzionano con qualsiasi software di vigilanza – oppure a qualsiasi ricevitore universale (SIA DC-09 2007/2012, SUR-GARD TL150). Al ricevitore SUR-GARD trasmette i codici Contact ID provenienti dalla centrale convertiti in codici SIA. Per impostazione predefinita verifica la connessione ogni 30 secondi (o all'intervallo che imposti tu) e in caso di guasto passa al canale di riserva.
- **Avvisa l'utente.** L'app Protegus 2 mostra quanto accaduto con notifiche push – con un suono distinto adatto all'evento – e nell'elenco eventi; dall'app l'utente può inserire e disinserire e comandare i dispositivi collegati (illuminazione, cancello, ventilazione, riscaldamento, irrigazione ecc.). Può essere avvisato anche via SMS e con chiamata telefonica.
- **Insieme o separatamente** lavora con la centrale di vigilanza e con l'utente: può essere usato solo con Protegus 2 (senza centrale di vigilanza), solo con la centrale di vigilanza oppure con entrambi. Se sono impostati entrambi, invia l'evento prima alla centrale di vigilanza, poi all'utente.
- **Riserva SMS.** Avvisa la centrale di vigilanza anche via SMS se la connessione dati non funziona nella rete dell'operatore; può inviare in parallelo a due ricevitori, ciascuno con un proprio canale di riserva.
- **Ha ingressi e uscite propri.** Tre morsetti I/O a doppia funzione possono essere usati come ingresso (rivelatore, tamper) o come uscita comandabile (zona a chiave, relè); le uscite si comandano dall'app Protegus 2 e con un comando SMS. Sul bus RS485 della versione 4G può comunicare con un espansore iO-8 per altri 8 I/O e, con un modulo W485 o E485, anche tramite connessione WiFi o Internet cablata – in tal caso la rete mobile è la via di riserva.

La struttura del sistema è mostrata nella figura seguente: il bus della centrale d'allarme si collega al G16, il G16 raggiunge Internet tramite la rete mobile, da lì il ricevitore della centrale di vigilanza e il cloud Protegus, e l'utente vede il sistema nell'app Protegus 2.

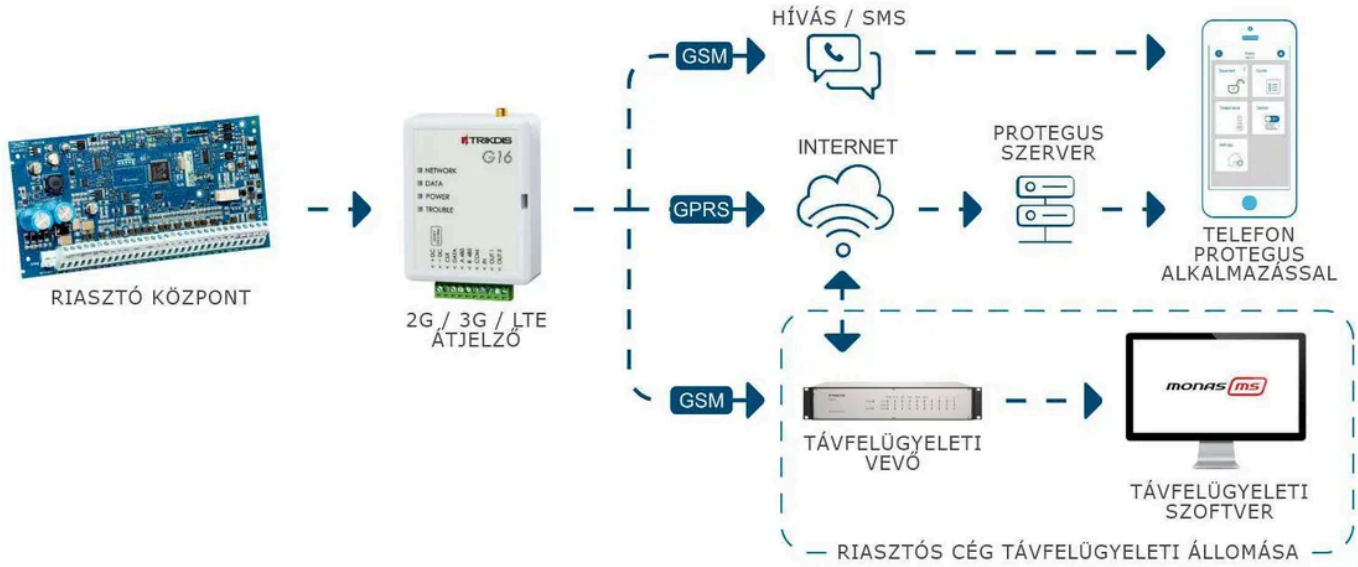


Figura 1. Il posto del G16 nel sistema: centrale d'allarme → G16 → rete mobile → ricevitore della centrale di vigilanza e cloud Protegus → app Protegus 2. L'utente può ricevere anche SMS e chiamate (GSM), il ricevitore della centrale di vigilanza riceve SMS come riserva.

- 1 Centrale d'allarme (bus della tastiera o porta seriale)
- 2 Comunicatore G16 (2G / 4G)
- 3 Chiamata e SMS all'utente
- 4 Connessione dati mobile → Internet → cloud Protegus
- 5 Telefono con l'app Protegus 2
- 6 Ricevitore della centrale di vigilanza
- 7 Software di vigilanza (la centrale di vigilanza dell'istituto di vigilanza)

1.2 Centrali d'allarme compatibili

Il G16 può essere collegato alle centrali seguenti. Con i modelli **controllabili direttamente** l'inserimento e il disinserimento avvengono dall'app con il codice tastiera; con gli altri tramite una zona a chiave (paragrafo 3.4). Per il controllo diretto delle centrali Paradox il firmware della centrale deve essere almeno **V.4**; sui modelli Paradox più recenti (SP+, MG5050+, EVOHD+) la porta seriale è bloccata di fabbrica e deve essere sbloccata prima dell'uso.

Centrali controllabili direttamente – il comunicatore riceve gli eventi tramite il bus dati o la porta seriale, e l'inserimento / disinserimento funziona senza ulteriore cablaggio:

Produttore	Collegamento	Modelli
Paradox	porta seriale	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* con firmware superiore alla 7.50)
DSC	bus dati	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	bus dati	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	porta seriale	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	bus dati	Ademco Vista-15, Vista-20, Vista-48

Sulle centrali Paradox più recenti contrassegnate con * la porta seriale è bloccata di fabbrica; il dispositivo esterno comunica con la centrale solo dopo lo sblocco.

Soros port feloldás útmutató

Centrali controllabili tramite zona a chiave – il comunicatore riceve gli eventi tramite il bus dati o la porta seriale; per il controllo servono il collegamento e la programmazione di una zona a chiave (punto 3.4):

Produttore	Collegamento	Modelli
Paradox	porta seriale	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	bus dati	PC1404, PC5020
Texecom	porta seriale	Premier 412, 816, 832, 832+
Inner Range	bus dati	Inception, Integriti
Crow	bus dati	Runner 4/8, 8/16

L'elenco cambia di tanto in tanto; lo stato più aggiornato si trova nel motore di ricerca della compatibilità. Oltre a queste, può essere usato anche con le centrali **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 e MATRIX 816**, **DSC PC5015** e **Paradox DIGIPLEX EVO96 e NE96**. Con le centrali **DSC PowerSeries NEO** il G16 non funziona: il produttore non consente dispositivi esterni sul bus NEO, vedi DSC Power Series NEO e comunicatori Trikdis: compatibilità e soluzioni.

1.3 Versioni

Questo manuale è stato scritto per la **versione hardware 4** del G16, ma **vale anche per la versione hardware 3**: il collegamento, la configurazione e il funzionamento delle due versioni sono in gran parte identici. Il manuale vale allo stesso modo per le versioni con modem 2G, 3G e 4G. Le differenze sono riassunte nella tabella seguente; dove il testo indica un dato della versione 4, per la versione 3 tieni conto di questa tabella.

	Hardware 3 (v3)	Hardware 4 (v4)
Modelli (in TrikdisConfig)	ad es. G16_3210 (2G); sono state prodotte anche versioni con modem 3G e 4G	G16_G410 (2G), G16_54E0 (4G)
Ingressi/uscite	1 ingresso di tipo selezionabile (IN) + 2 uscite a collettore aperto (OUT1, OUT2, max. 0,15 A)	3 morsetti I/O a doppia funzione (I/O 1, I/O 2, I/O 3), ciascuno utilizzabile come ingresso o come uscita a collettore aperto (max. 0,15 A)
Configurazione degli ingressi/uscite	pagina System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	pagina **IN/OUT** (paragrafo 6.6)
Assorbimento	100 mA; durante la trasmissione fino a 250 mA	60–100 mA; durante la trasmissione fino a 500 mA
Bus RS485 (iO-8, W485, E485)	solo sulle versioni 3G e 4G	solo sulla versione 4G (G16_54E0)

La versione hardware 4 è prodotta con due modem:

Modello	Modem	Frequenze	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	no

Modello	Modem	Frequenze	RS485 (iO-8, W485, E485)
G16_54E0	4G (LTE)	bande LTE a seconda della regione	sì

La versione hardware si trova nella barra di stato di TrikdisConfig (**HW**) e sull'etichetta sul retro del dispositivo. L'annuncio della versione 4 è in un articolo a parte: Arriva la versione hardware v4 dei comunicatori GSM G16 e G16T.

1.4 Caratteristiche principali

Collegamento con la centrale d'allarme

- Si collega con al massimo 4 fili (+DC, −DC, CLK, DATA) al bus della tastiera (DSC, Caddx, Crow, Pyronix, Honeywell) o alla porta seriale (Paradox, Texecom, InnerRange) della centrale; per la porta seriale è disponibile un cavo originale (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Trasmette ogni evento della centrale con le informazioni complete (codice, area, zona o utente); segnala l'interruzione del collegamento (LED TROUBLE, evento COMMUNICATION).
- Le centrali controllabili direttamente possono essere inserite e disinserite dall'app con il codice tastiera; Protegus 2 mostra anche lo stato delle zone.

Comunicazione con la centrale di vigilanza

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

Funzioni per l'utente

- App mobile e web Protegus 2: notifiche, elenco eventi, inserimento e disinserimento, comando delle uscite.
- Comando e configurazione di base anche con comandi SMS.
- Notifica anche via SMS e con chiamata telefonica, fino a 4 numeri di telefono.
- Diritti utente a più livelli nell'app (amministratore, installatore, utente).

Installazione e configurazione

- Le impostazioni possono essere salvate su file e caricate in un altro comunicatore.
- Due livelli di accesso: amministratore e installatore.
- Configurabile e aggiornabile a distanza con il software TrikdisConfig.

1.5 Le parti del comunicatore

Il G16 ha il circuito stampato in una scatola di plastica bianca; il coperchio frontale è rimovibile, la morsettiera è estraibile. Nell'immagine seguente è visibile la versione 4G; la versione 2G non ha il LED BAND né i morsetti A 485 / B 485.

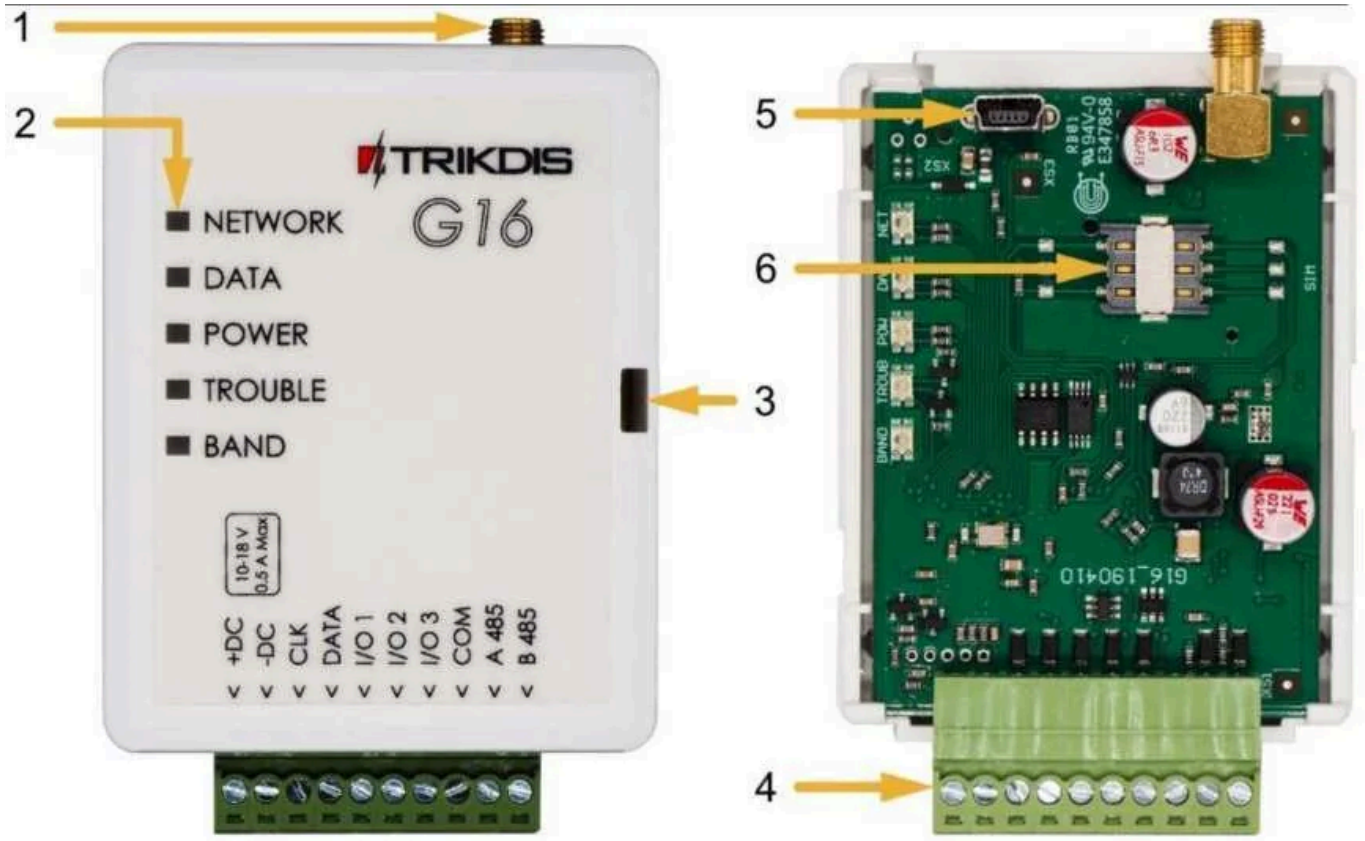


Figura 2. Le parti del G16 (versione 4G) dal davanti e con la scatola aperta.

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

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

1.6 Morsetti

Morsetto	Funzione
+DC	Alimentazione, +10–18 V DC
–DC	Alimentazione, negativo
CLK	Linea di clock / seriale del bus della centrale
DATA	Linea dati del bus della centrale
I/O 1	Ingresso/uscita 1 (impostazione di fabbrica: non usato)
I/O 2	Ingresso/uscita 2 (impostazione di fabbrica: ingresso, NO)
I/O 3	Ingresso/uscita 3 (impostazione di fabbrica: uscita)
COM	Punto comune (negativo) per ingressi e uscite
A 485	Filo A del bus RS485 (solo versione 4G)
B 485	Filo B del bus RS485 (solo versione 4G)

La serigrafia della morsettiera è riportata anche sul coperchio frontale, quindi durante il collegamento non serve togliere il coperchio. A quale morsetto della centrale vanno CLK e DATA dipende dal produttore – gli schemi di collegamento sono nel paragrafo 3.3.

1.7 Segnalazioni dei LED

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

NETWORK – connessione di rete

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

DATA – traffico dati

Segnalazione	Significato
spento	Nessun messaggio in attesa di invio
verde fisso	Ci sono messaggi in memoria in attesa di invio
verde lampeggiante	Invio o ricezione dati in corso (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 corretta
giallo fisso	Tensione di alimentazione non adeguata (al massimo 11,5 V)
verde fisso, giallo lampeggiante	Pronto per la programmazione (cavo USB collegato)
giallo fisso (durante la programmazione)	Nessuna connessione con il computer

TROUBLE – guasto

Segnalazione	Significato
spento	Nessun guasto
1 lampeggio rosso	Nessuna scheda SIM
2 lampeggi rossi	Errore PIN della SIM (codice PIN errato)
3 lampeggi rossi	Errore di programmazione (manca l'APN)
4 lampeggi rossi	Non riesce a registrarsi sulla rete mobile (errore di registrazione)
5 lampeggi rossi	Non riesce a connettersi alla rete dati (GPRS/UMTS/LTE)
6 lampeggi rossi	Nessuna connessione con il ricevitore della centrale di vigilanza e/o con il server Protegus (la causa può essere anche un guasto della connessione Internet)
7 lampeggi rossi	Interrotto il collegamento con la centrale d'allarme (collegamento bus o seriale)
rosso lampeggiante (durante la programmazione)	Errore di memoria
rosso fisso (durante la programmazione)	Firmware danneggiato

BAND – tipo di rete (solo versione 4G)

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

1.8 Dati tecnici

Parametro	Valore
Collegamento con la centrale d'allarme	bus della tastiera o porta seriale, a seconda del tipo di centrale (al massimo 4 fili: +DC, −DC, CLK, DATA; sul bus Caddx e Pyronix il CLK non è usato)
Ingressi/uscite	3 I/O a doppia funzione (I/O 1, I/O 2, I/O 3): come ingresso NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistenza di fine linea da 2,2 kΩ); come uscita a collettore aperto (OC), max. 0,15 A / 30 V DC
Espansione	sul bus RS485 (solo versione 4G): espansore iO-8 (+8 I/O) e altri espansori della serie iO; modulo WiFi W485, modulo Ethernet E485
Modem 2G	850 / 900 / 1800 / 1900 MHz
Modem 4G	bande LTE a seconda della regione
Tensione di alimentazione	10–18 V DC
Assorbimento	60–100 mA nominale; fino a 500 mA durante la trasmissione
Protocolli di trasmissione	TRK, DC-09_2007, DC-09_2012, TL150
Memoria eventi	60 messaggi

Parametro	Valore
Crittografia	AES-128
Programmazione	TrikdisConfig (Windows) tramite cavo USB Mini-B o a distanza; comandi SMS
Ambiente di funzionamento	−10 … +50 °C, umidità relativa max. 80 % (a +20 °C)
Dimensioni	92 × 65 × 26 mm
Peso	80 g

2. Messa in servizio rapida con TrikdisConfig

Tutte le impostazioni del G16 si eseguono con il programma per Windows **TrikdisConfig** – tramite cavo USB o a distanza. In questo capitolo descriviamo la via più breve: configuri il dispositivo sulla scrivania, prima del collegamento, e poi sul posto devi solo collegarlo. La spiegazione dettagliata delle impostazioni si trova nel capitolo 6.

2.1 Preparazione

Cosa ti servirà

Cavo USB Mini-B · cavo con almeno 4 conduttori per il bus della centrale – per la porta seriale Paradox cavo **CRP2** o **CRP2B**, per la porta seriale Texecom cavo **CRP4** · cacciavite piatto da 2,5 mm · antenna mobile con guadagno adeguato (dove la copertura è debole, un'antenna con guadagno maggiore) · scheda nano SIM attiva con servizio dati mobile (la richiesta del PIN può essere disattivata) · il manuale per l'installatore della centrale d'allarme. Gli accessori necessari vanno ordinati separatamente presso il distributore.

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 coperchio frontale del G16. Inserisci un cacciavite piatto nell'apertura sul bordo superiore del coperchio e, facendo leva verso il basso, sgancia delicatamente il coperchio frontale. La figura seguente mostra l'apertura e la posizione della presa USB.

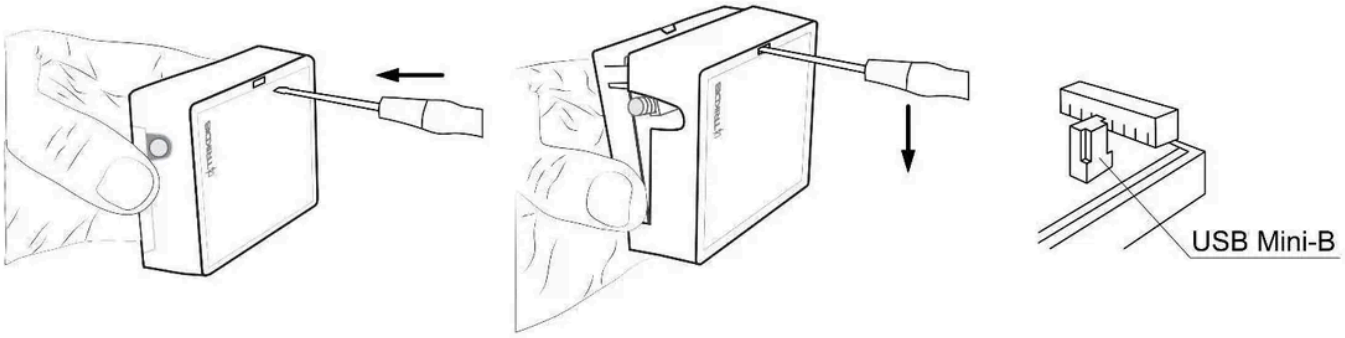


Figura 3. Sgancio del coperchio frontale con un cacciavite piatto (a sinistra, al centro) e posizione della presa USB Mini-B sul circuito stampato (a destra).

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

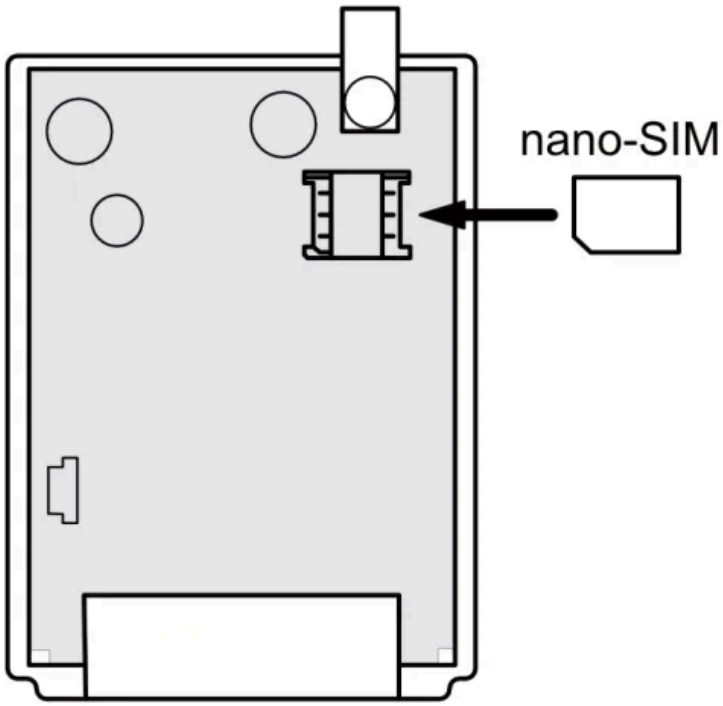


Figura 4. La posizione della scheda nano SIM sul circuito stampato.

4. Collega il G16 al computer con un cavo USB Mini-B. La porta USB fornisce alimentazione sufficiente per la programmazione, non serve un alimentatore separato.

Avvertenza

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

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

`654321`).

2.2 Tipo di centrale e controllo diretto

Qualunque modalità di funzionamento usi, per prima cosa indica nella pagina **System settings** a quale centrale verrà collegato il comunicatore.

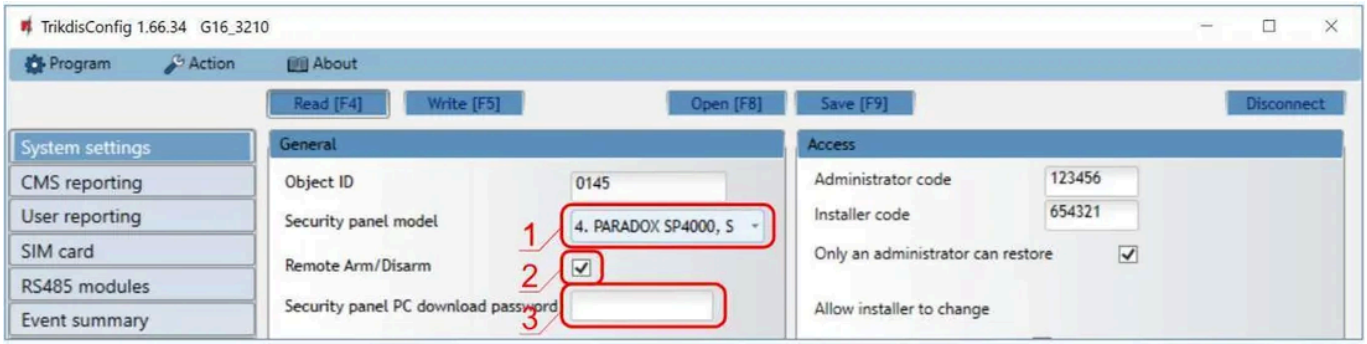


Figura 5. TrikdisConfig – pagina System settings, gruppo General.

- 1 **Security panel model** – il tipo della centrale d'allarme collegata, dall'elenco; da questo dipende come il comunicatore legge il bus.
- 2 **Remote Arm/Disarm** – spunta questa casella se l'utente vuole inserire e disinserire la centrale dall'app Protegus 2 con il proprio codice tastiera. Appare solo con i modelli controllabili direttamente; con le altre centrali l'inserimento si può realizzare con una zona a chiave (paragrafo 3.4) – in tal caso lasciala vuota.
- 3 **Security panel PC download password** – con le centrali Paradox e Texecom, la password PC o UDL della centrale (4 caratteri); deve coincidere con quella impostata nella centrale. Il campo appare dopo aver spuntato Remote Arm/Disarm.

Con diverse centrali serve un'impostazione anche nella centrale stessa: con le centrali Caddx, Honeywell e InnerRange già per la lettura degli eventi (abilitazione del bus o della porta seriale), con le centrali Paradox e Texecom per il controllo diretto (password PC o UDL) – il capitolo 4 lo descrive per produttore, insieme alla modifica della password.

2.3 Collegamento all'app Protegus 2

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



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

- 4 **Enable connection** – spuntala: abilita la connessione con il cloud Protegus.
- 5 **Protegus Cloud access code** – cambia la password di fabbrica `123456`. È quella che dovrai inserire nell'app quando crei il sistema; **dopo la creazione del sistema non può più essere modificata.**

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

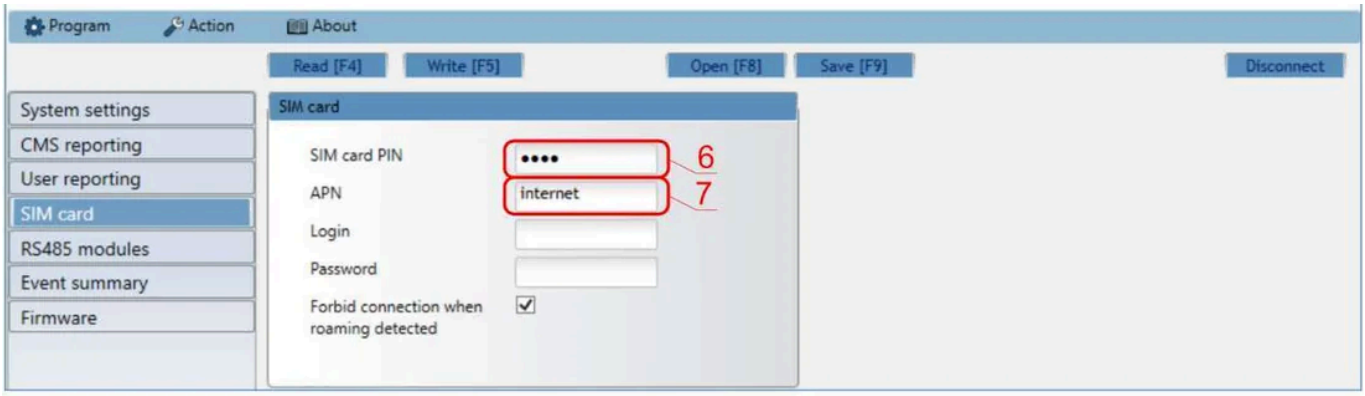


Figura 7. TrikdisConfig – pagina SIM card.

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

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

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

2.4 Collegamento alla centrale di vigilanza

Se il dispositivo trasmette anche a un ricevitore della centrale di vigilanza, nella pagina **System settings** inserisci anche l'identificativo dell'impianto.

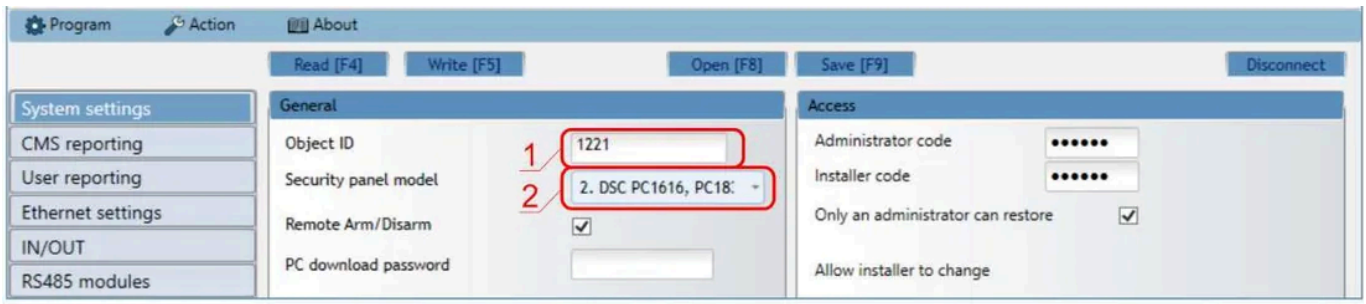


Figura 8. TrikdisConfig – pagina System settings, gruppo General.

- 1 **Object ID** – l'identificativo dell'impianto ricevuto dalla centrale di vigilanza (4 caratteri esadecimali, 0–9, A–F). `FFFE` e `FFFF` non possono essere usati.
- 2 **Security panel model** – il tipo della centrale d'allarme collegata (se non l'hai ancora impostato nel paragrafo 2.2).

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

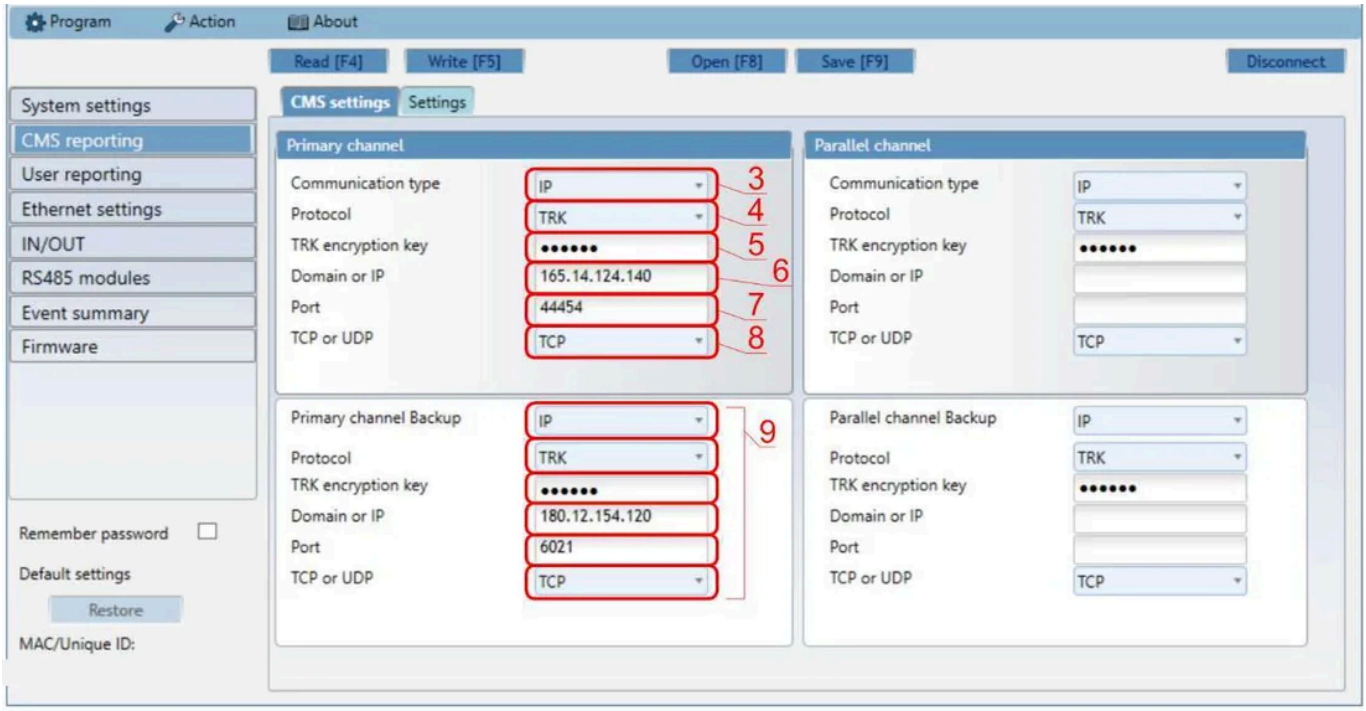


Figura 9. TrikdisConfig – CMS reporting, scheda CMS settings.

- 3 **Communication type** – scegli la connessione **IP** (l'SMS non è consigliato come canale primario).
- 4 **Protocol** – **TRK** per un ricevitore Trikdis, **DC-09_2007** o **DC-09_2012** per un ricevitore universale, **TL150** per un ricevitore SUR-GARD.
- 5 **TRK encryption key** – la chiave di crittografia di 6 cifre impostata nel ricevitore.
- 6 **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- 7 **Port** – il numero di porta del ricevitore.
- 8 **TCP or UDP** – il protocollo di trasmissione; si adegua all'impostazione del ricevitore.
- 9 **Primary channel Backup** – canale di riserva in caso di guasto del primario; compilalo allo stesso modo, è consigliato impostarlo.

È consigliato impostare anche il **Parallel channel** (canale parallelo) e il relativo canale di riserva, se gli eventi devono arrivare a due ricevitori; nel campo **Backup SMS reporting number** – anche questo è consigliato – puoi scrivere il numero di telefono del ricevitore SMS Trikdis: il dispositivo, subito dopo il primo avvio, invia qui un SMS e in seguito trasmette via SMS quando nessuno dei canali IP funziona.

Infine, nella pagina **SIM card**, inserisci i dati della scheda, se non l'hai già fatto nel paragrafo 2.3.

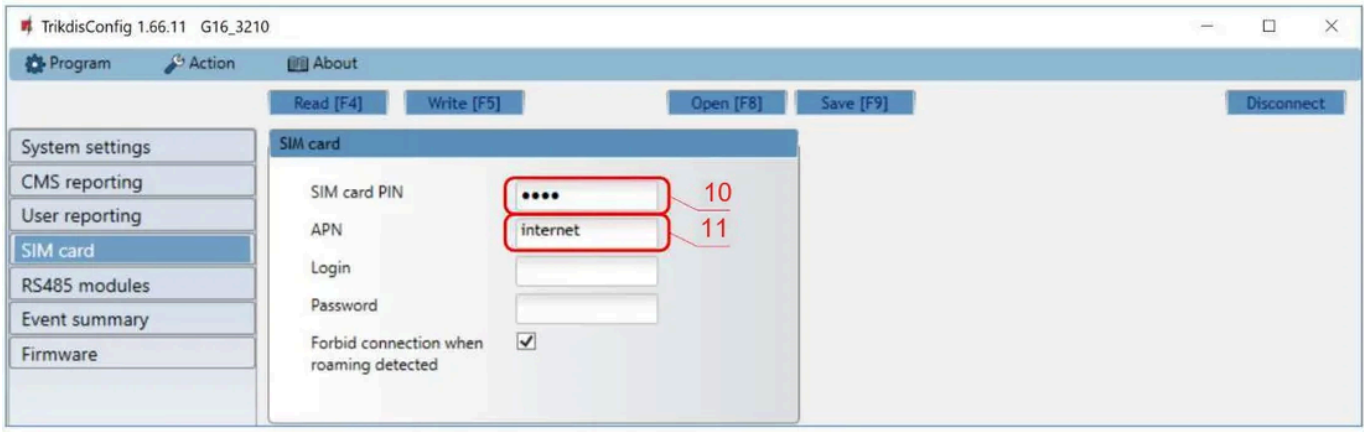


Figura 10. TrikdisConfig – pagina SIM card.

- 10 **SIM card PIN** – il codice PIN della scheda.
- 11 **APN** – il punto di accesso dell'operatore (vedi il paragrafo 2.3).

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

Alla fine delle impostazioni premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB. Il dispositivo è così pronto per il collegamento.

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

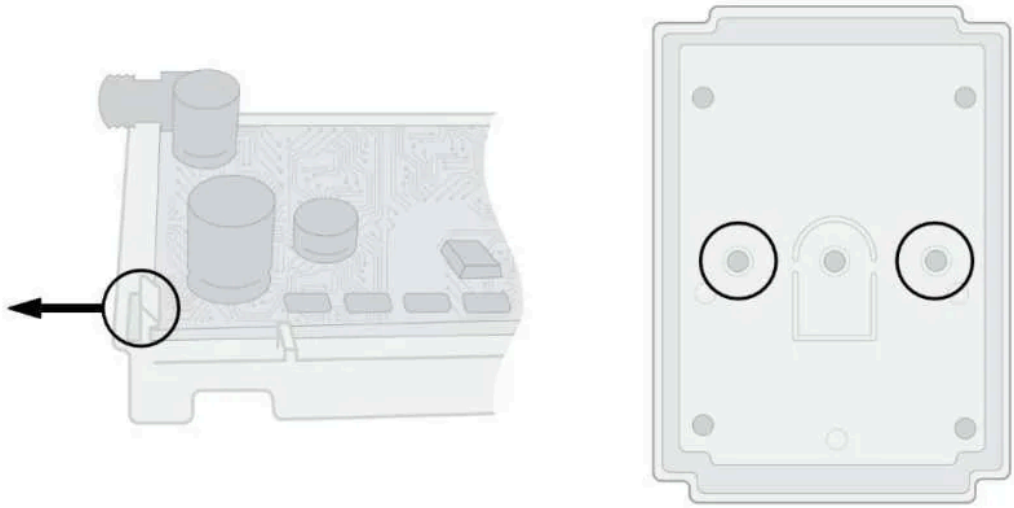


Figura 11. Estrazione del circuito stampato: apertura del fermo nell'angolo (a sinistra) e fori di fissaggio del fondo (a destra, cerchiati).

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

3.2 Posizionamento e antenna

- Installa il comunicatore in un luogo **asciutto, al chiuso**, possibilmente vicino alla scatola della centrale d'allarme, così il cavo del bus resta corto.
- **In una scatola metallica** il segnale mobile si attenua molto. Se il comunicatore va dentro l'involucro metallico della centrale, porta l'antenna fuori dalla scatola oppure usa un'antenna con cavo più lungo.

- Prima del fissaggio definitivo **verifica il livello del segnale**: il numero di lampeggi gialli del LED NETWORK deve essere almeno 5 in 2G e almeno 3 in 4G (vedi il paragrafo 1.7). Se sono meno, cerca un posto migliore oppure passa a un'antenna più sensibile, collocabile più lontano.
- Tieni l'antenna e il comunicatore lontani dal trasformatore della centrale e dai cavi di rete.



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

3.3 Collegamento alla centrale d'allarme

Il G16 si collega alla centrale con **al massimo quattro fili** (sul bus Caddx e Pyronix il CLK non è usato): sui morsetti **+DC** e **–DC** va l'alimentazione ausiliaria a 12 V (AUX) della centrale, sui morsetti **CLK** e **DATA** i due fili dati del bus della tastiera o della porta seriale della centrale. Quale morsetto della centrale corrisponda a quale dipende dal produttore – collega secondo gli schemi seguenti. Per le centrali con porta seriale (Paradox, Texecom) è disponibile un cavo originale, un capo del quale si inserisce nel connettore della centrale e l'altro si collega alla morsettiera del G16.

Il G16 durante la trasmissione può assorbire fino a 500 mA. Verifica che l'uscita AUX della centrale lo sopporti insieme agli altri dispositivi collegati. Poiché l'alimentazione la fornisce la centrale, in caso di blackout la batteria della centrale alimenta anche il comunicatore. La maggior parte delle centrali non viene danneggiata dai fili invertiti di un dispositivo collegato al bus, ma l'inversione di **+DC e –DC** può distruggere il comunicatore – prima del collegamento verifica la polarità.

Dopo il collegamento, nel campo **System settings** → **Security panel model** di TrikdisConfig devi selezionare il tipo della centrale collegata (paragrafo 2.2); con alcuni produttori serve un'impostazione anche nella centrale (capitolo 4).

3.3.1 DSC PowerSeries

I quattro morsetti del Keybus: **RED** → +DC, **BLK** → –DC, **YEL** → CLK, **GRN** → DATA.

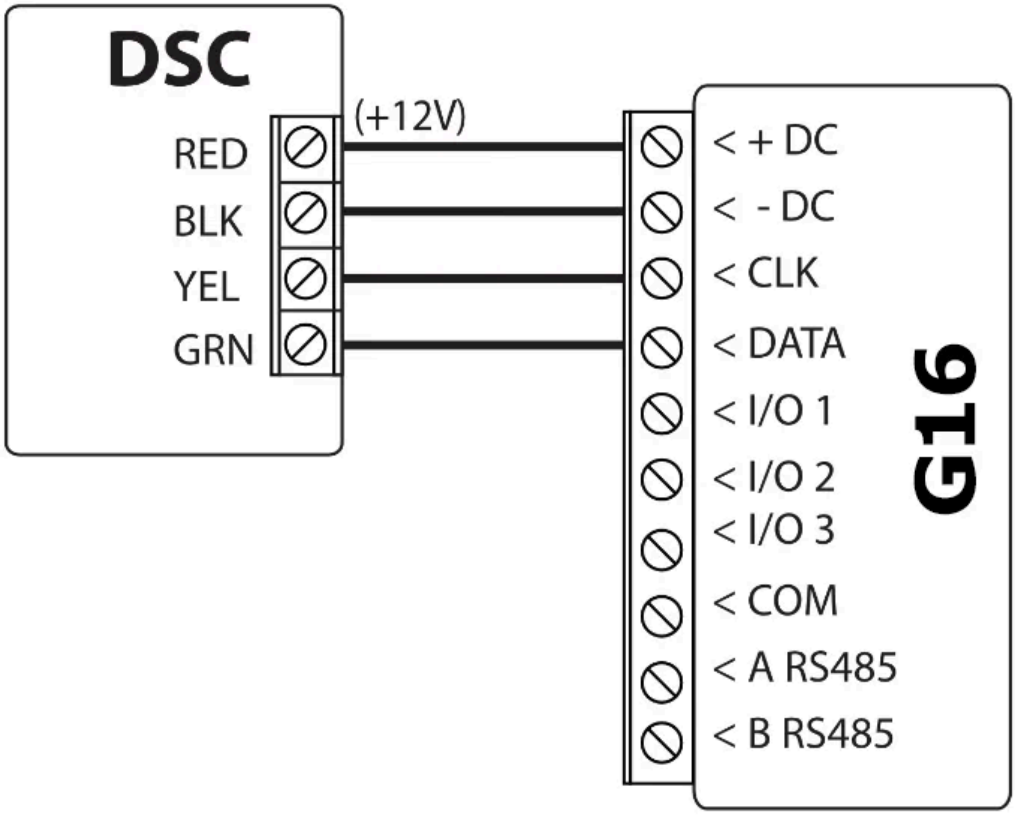


Figura 12. Collegamento al Keybus (bus della tastiera, "Keypad bus") di una centrale DSC PowerSeries: RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Il comunicatore si collega alla **porta seriale** (SERIAL) delle centrali Paradox con il cavo originale **CRP2** o **CRP2B**; il capo del cavo lato centrale si inserisce nel connettore seriale, l'altro capo lo colleghi alla morsettiera del G16. I 4 pin del connettore: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. I colori dei conduttori dei due cavi sono diversi – lo schema mostra la disposizione dei colori di entrambi i cavi. La marcatura del connettore seriale Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

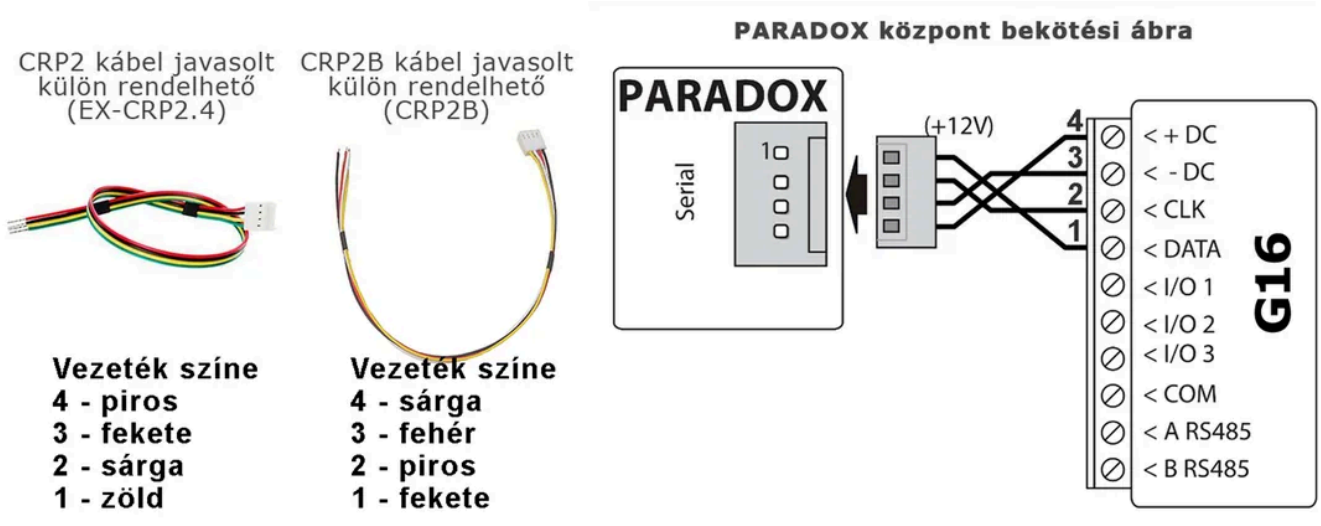


Figura 13. Collegamento alla porta seriale di una centrale Paradox con cavo CRP2 (EX-CRP2.4) o CRP2B. CRP2: 4 rosso → +DC, 3 nero → −DC, 2 giallo → CLK, 1 verde → DATA. CRP2B: 4 giallo → +DC, 3 bianco → −DC, 2 rosso → CLK, 1 nero → DATA.

Sulle centrali Paradox più recenti la porta seriale può essere bloccata di fabbrica – la procedura di sblocco è nel paragrafo 4.2 e nell'articolo Sblocco della porta seriale bloccata nelle centrali d'allarme Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

I tre morsetti del bus della tastiera: **POS** → +DC, **COM** → −DC, **DATA** → DATA. Il morsetto **CLK** non è usato.

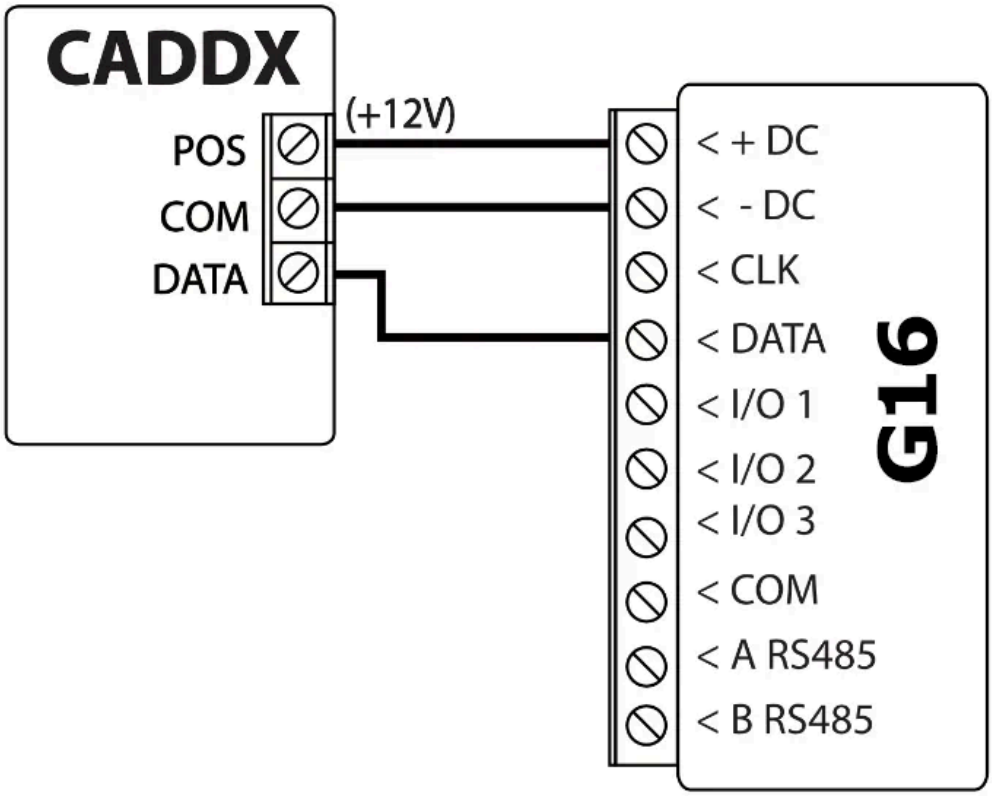


Figura 14. Collegamento al bus della tastiera (“Keypad bus”) di una centrale Caddx NetworX: POS → +DC (+12 V), COM → −DC, DATA → DATA; il CLK resta libero.

3.3.4 Texecom Premier / Premier Elite

Il comunicatore si collega alla porta seriale della centrale con il cavo originale **CRP4**: **rosso (R)** → +DC, **nero (B)** → −DC, **blu (BL)** → CLK, **bianco (W)** → DATA.

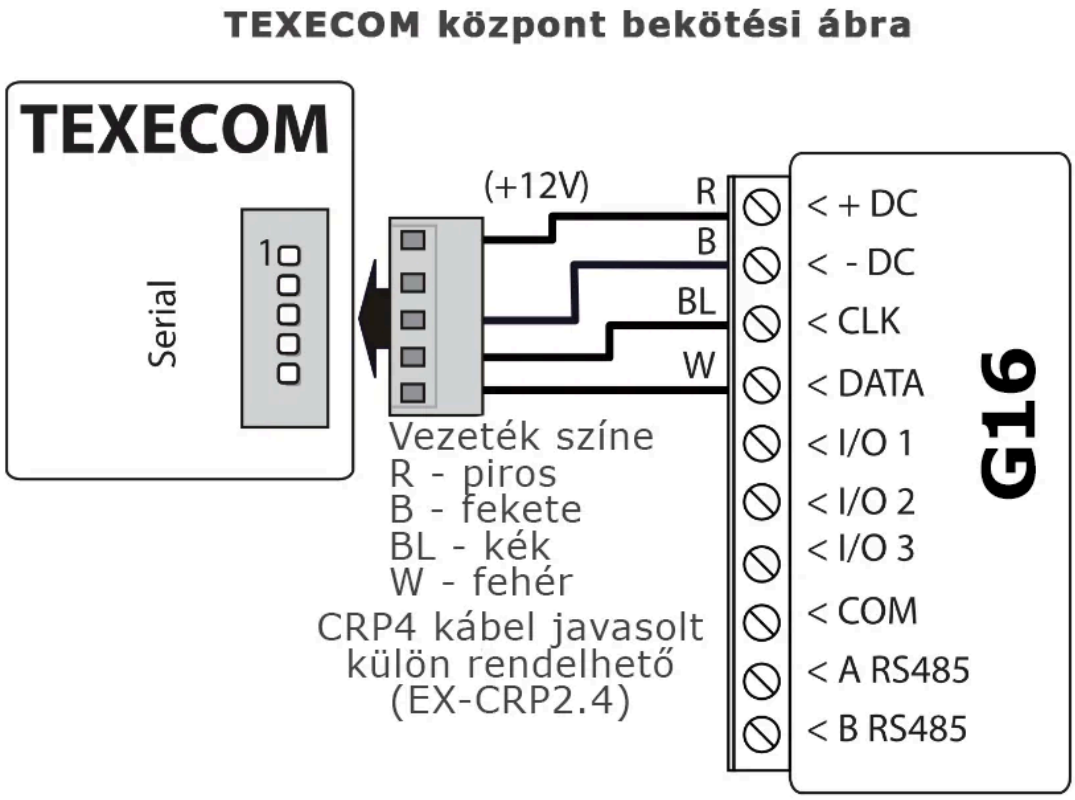


Figura 15. Collegamento alla porta seriale di una centrale Texecom con cavo CRP4: rosso → +DC, nero → −DC, blu → CLK, bianco → DATA.

3.3.5 Crow Runner

Il bus della tastiera delle Crow Runner 4/8 e Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

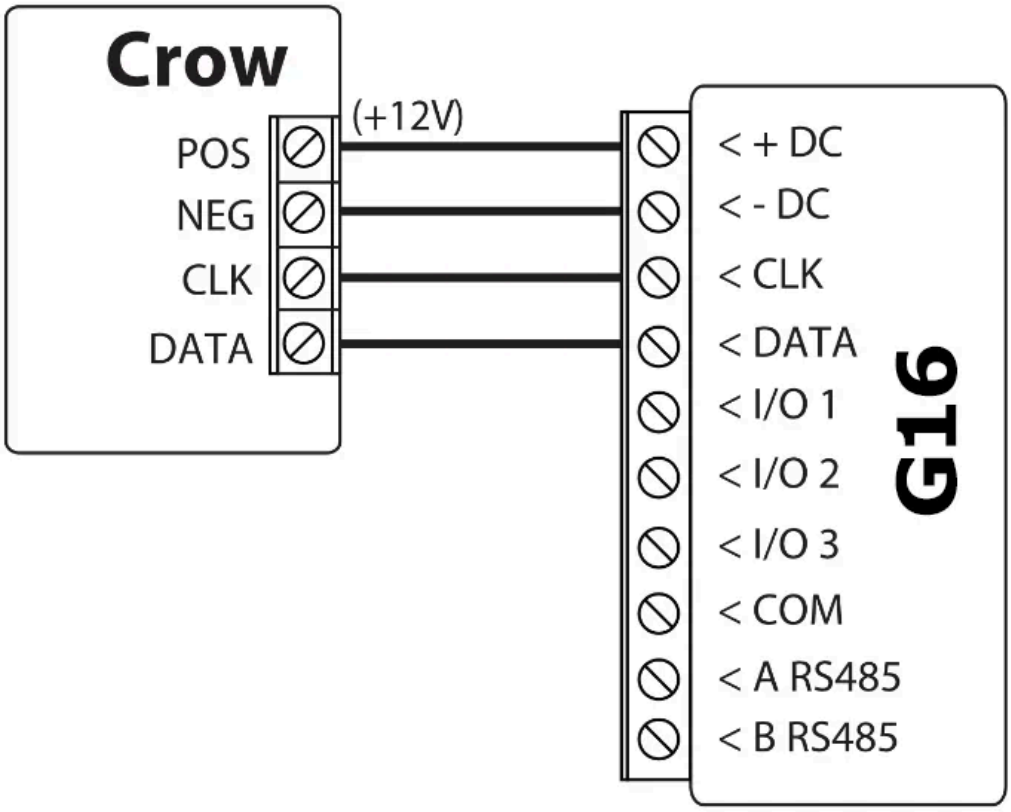


Figura 16. Collegamento al bus della tastiera ("Keypad bus") di una centrale Crow Runner 4/8 e Runner 8/16: POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Il bus della tastiera delle centrali Pyronix: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. Il morsetto **CLK** non è usato. Dopo il collegamento e la configurazione del comunicatore, togli l'alimentazione alla centrale e riavviala, affinché accetti il comunicatore (paragrafo 4.5).

3.3.7 Honeywell Ademco Vista

I morsetti numerati del bus della tastiera delle centrali Vista-15, Vista-20 e Vista-48: **5** (AUX +) → +DC, **4** (AUX −) → −DC, **7** (uscita dati, giallo) → CLK, **6** (ingresso dati, verde) → DATA.

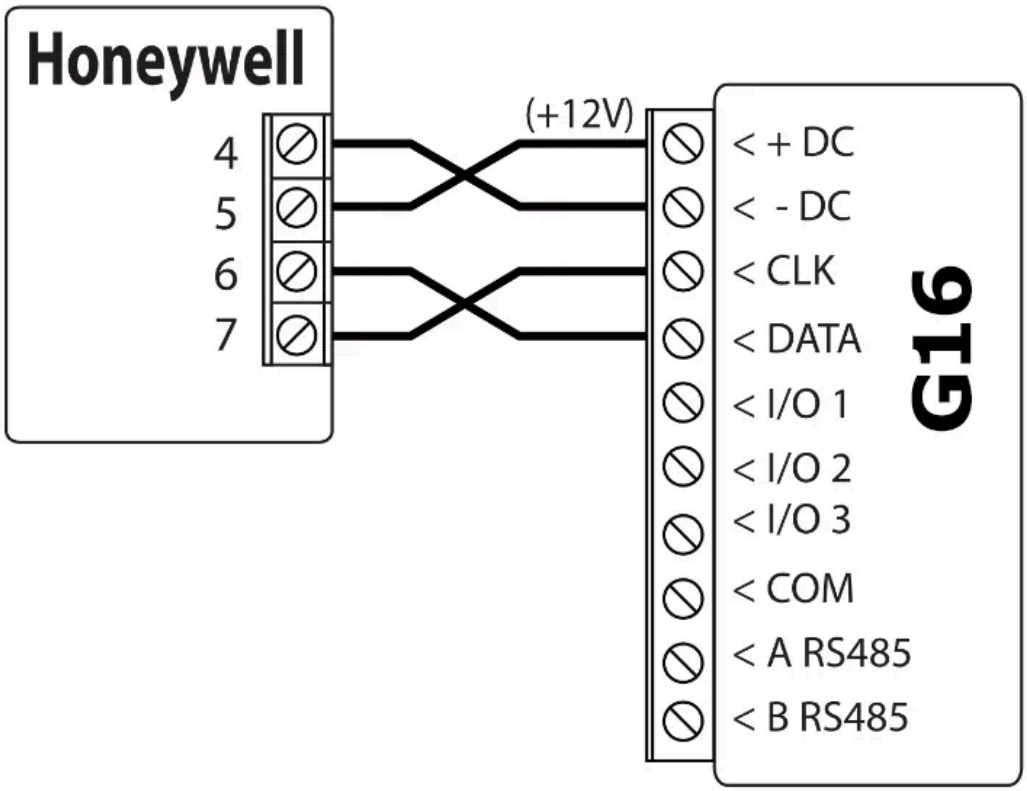


Figura 17. Collegamento al bus della tastiera (“Keypad bus”) di una centrale Honeywell Vista-20 / Vista-48: 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception e Integriti

Il comunicatore riceve l'alimentazione dai morsetti di alimentazione della centrale **Inception** (**VOUT +** → +DC, **0V** → −DC), mentre il collegamento dati si realizza dalla porta USB della centrale, con il cavo InnerRange 993030USB: **nero** → 0V (−DC), **verde** → CLK, **bianco** → DATA. Nella centrale deve essere abilitato l'uso della porta seriale (paragrafo 4.7).

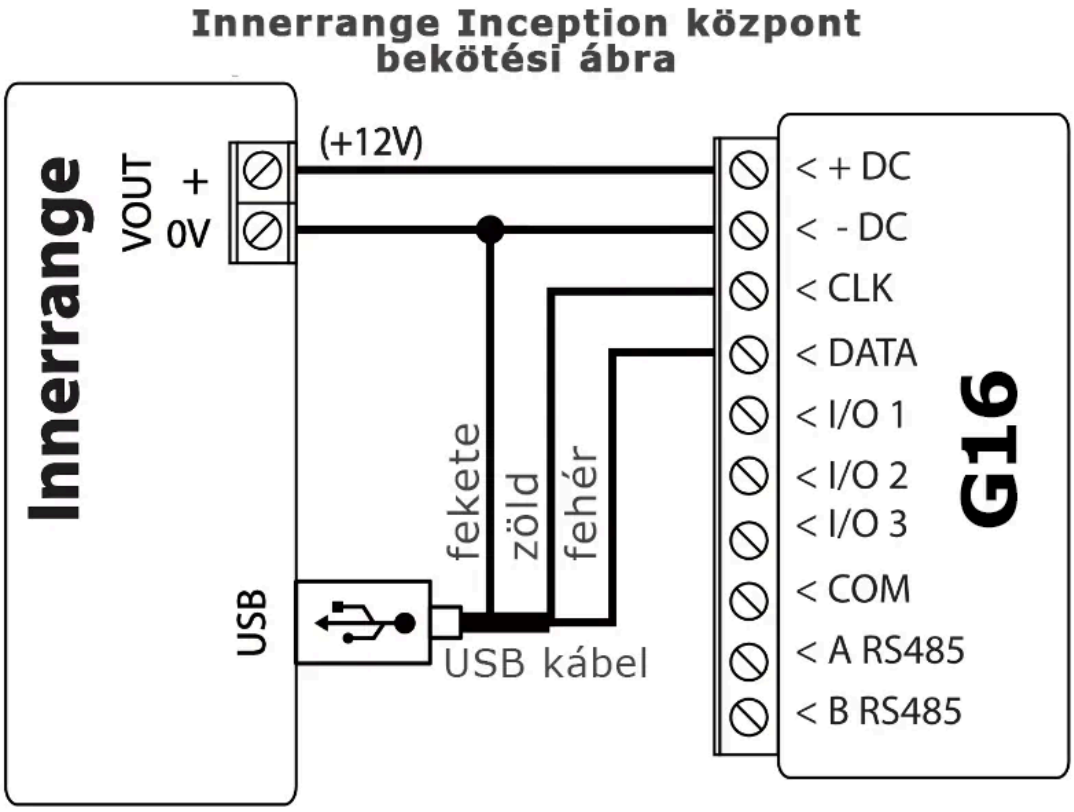


Figura 18. Collegamento a una centrale InnerRange Inception: alimentazione dai morsetti VOUT + e 0V, dati dalla porta USB con il cavo 993030USB (nero → 0V, verde → CLK, bianco → DATA).

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

3.4 Collegamento della zona a chiave

Se la centrale non rientra tra i modelli controllabili direttamente, oppure non vuoi usare il controllo diretto, l'inserimento e il disinserimento a distanza si possono realizzare con una **zona a chiave**: imposti uno dei morsetti I/O del comunicatore come **uscita** (pagina IN/OUT, paragrafo 6.6) e lo colleghi a una zona a chiave della centrale. All'attivazione l'uscita porta la zona a COM (negativo); collega la resistenza di fine linea della zona in base al tipo di zona della centrale. Poiché il G16 ha tre morsetti I/O, si possono gestire fino a tre aree con uscite separate.

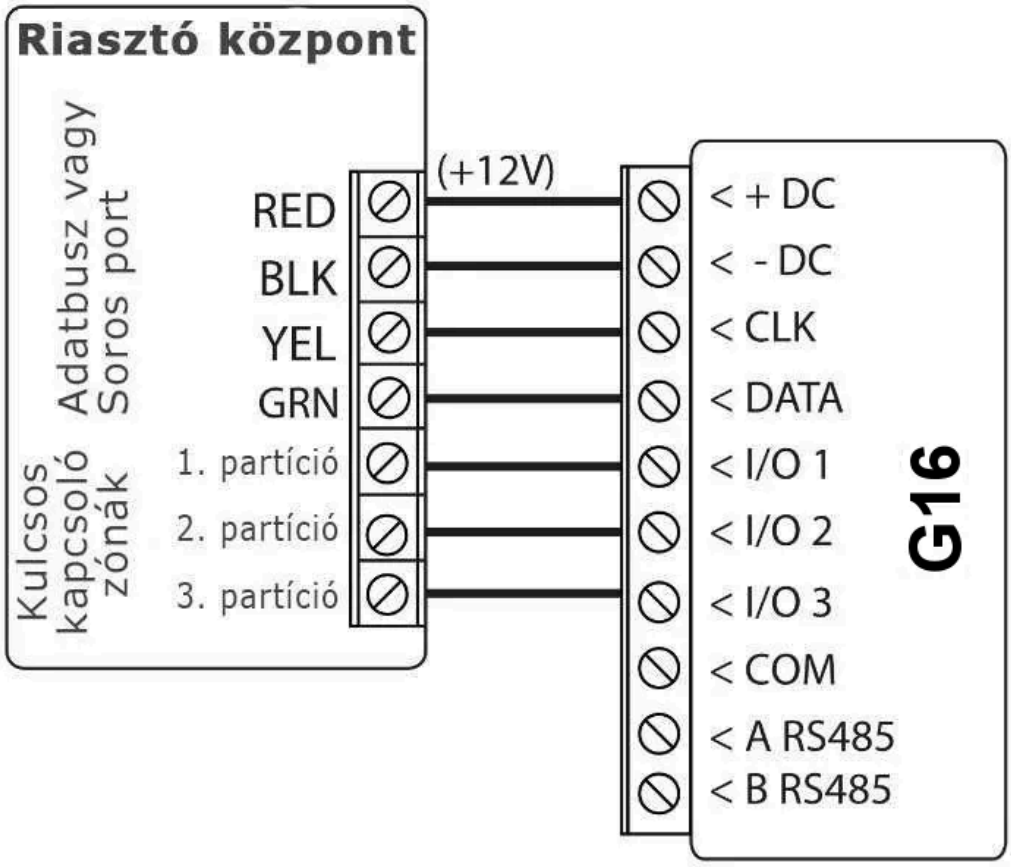


Figura 19. Inserimento e disinserimento con zona a chiave: il comunicatore legge gli eventi dal bus della centrale, mentre le uscite I/O 1–3 comandano la zona a chiave delle aree 1–3 della centrale.

- Nella pagina **System settings** di TrikdisConfig il **Remote Arm/Disarm** deve restare **vuoto** – le due cose non possono essere usate contemporaneamente.
- La zona a chiave può essere impulsiva o bistabile; nell'app Protegus 2 va impostata la stessa modalità (paragrafo 5.3).
- Sulla **versione hardware 3** le due uscite (OUT1, OUT2) possono gestire due aree; il campo **System settings** → **Output OUT1 & OUT2 mode** deve essere su **Remote control** (impostazione di fabbrica).

Sui dettagli e sulle insidie dell'inserimento con zona a chiave c'è un articolo a parte: Inserimento a distanza con zona a chiave dall'app Protegus 2.

3.5 Collegamento degli ingressi

I morsetti I/O del comunicatore, come ingressi, possono essere usati anche per ricevere altri rivelatori (ad es. interruttore tamper, pulsante antipanico, termostato), indipendentemente dalla centrale d'allarme. L'ingresso va collegato tra l'I/O scelto e il morsetto COM.

Gli ingressi accettano i seguenti tipi di circuito: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La resistenza di fine linea è **2,2 kΩ**. Con la terminazione singola (EOL) sia il cortocircuito sia l'interruzione contano come allarme; la doppia terminazione (DEOL), con due resistenze, riconosce separatamente l'allarme e il sabotaggio (cortocircuito o interruzione). L'impostazione di fabbrica è NO (normalmente aperto); il tipo di ingresso si imposta nella pagina **IN/OUT** di TrikdisConfig, in base al collegamento.

Tipo	Stato di riposo	Allarme	Sabotaggio
NC	chiuso	aperto	–

Tipo	Stato di riposo	Allarme	Sabotaggio
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 d'ingresso: tipi NO, NC, NC/EOL, NO/EOL, NO/DEOL e NC/DEOL con resistenza di fine linea da 2,2 kΩ; nei tipi DEOL è collegato anche il circuito tamper.

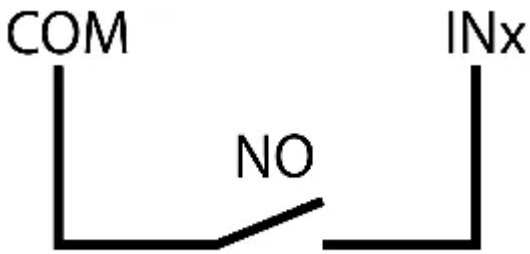


Figura 20. NO – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

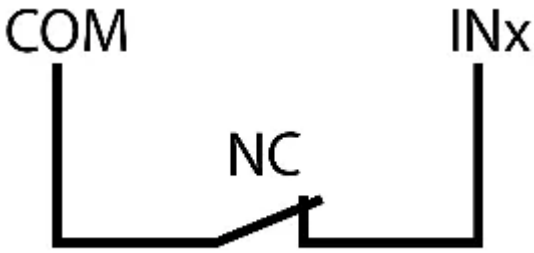


Figura 21. NC – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

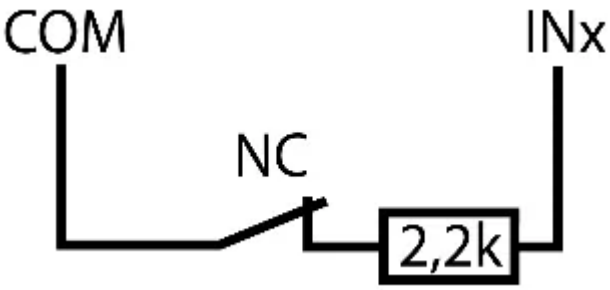


Figura 22. NC/EOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

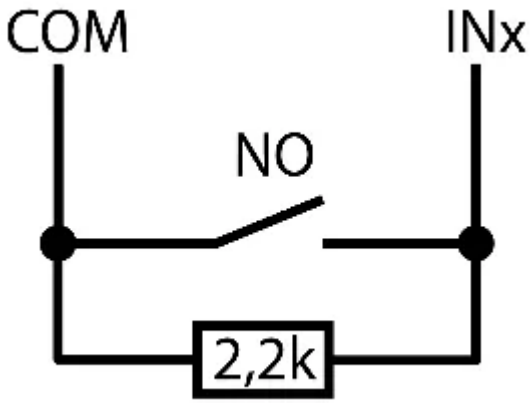


Figura 23. NO/EOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

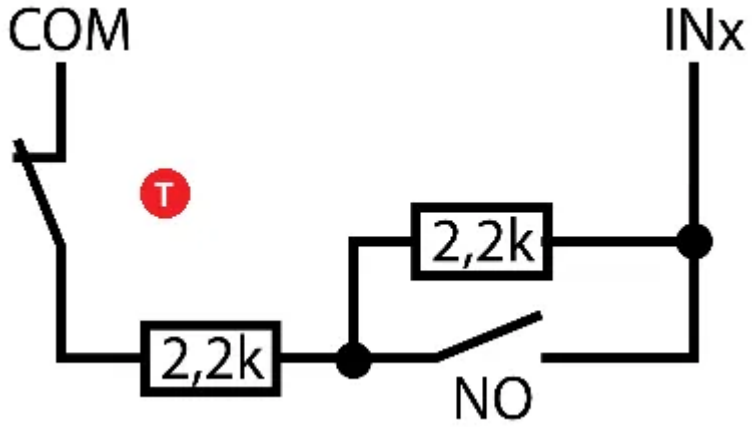


Figura 24. NO/DEOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento tamper: cortocircuito o interruzione – tamper, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

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

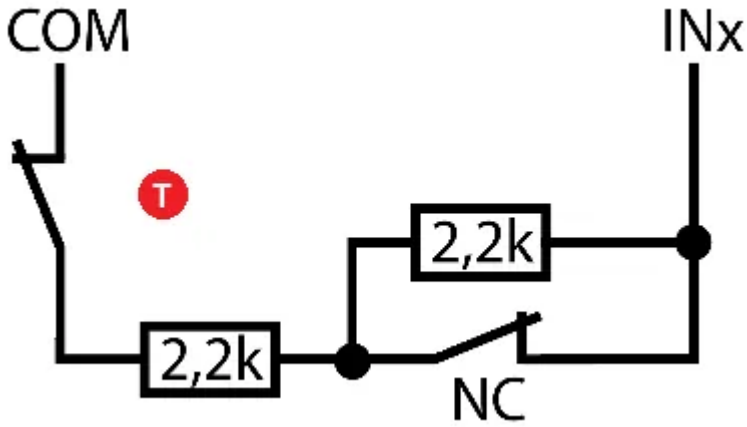


Figura 25. NC/DEOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento tamper: cortocircuito o interruzione – tamper, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

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

Sulla **versione hardware 3** c'è un solo ingresso (IN); il suo tipo si imposta nel campo **System settings → Input IN type**.

3.6 Collegamento di un'uscita con relè

Come uscite, i morsetti I/O sono uscite a collettore aperto (OC): nello stato attivo portano a negativo il carico collegato, con al massimo 0,15 A, fino a 30 V DC. Un utilizzatore più grande o un dispositivo a tensione di rete va comandato **tramite un relè**: un capo della bobina del relè va su +DC, l'altro sul morsetto I/O. Con i contatti del relè si possono accendere e spegnere diversi dispositivi elettrici. Per questo il morsetto I/O va impostato come uscita (**OUT**) nella pagina **IN/OUT** di TrikdisConfig (paragrafo 6.6).

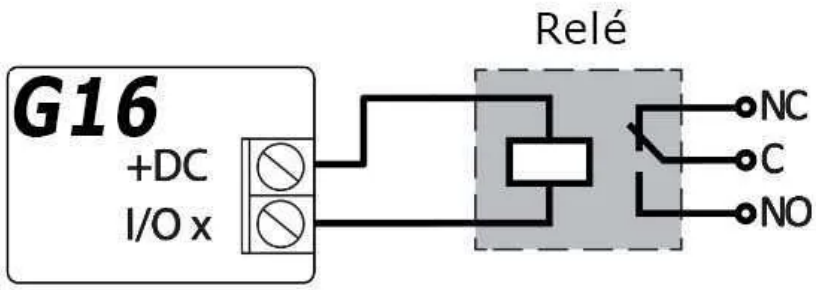


Figura 26. Collegamento di un relè all'uscita del comunicatore: la bobina va tra il morsetto +DC e il morsetto I/O x, i contatti (NC, C, NO) comandano l'utilizzatore.

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

3.7 Collegamento dell'espansore iO-8

Se servono più ingressi o uscite, sul bus RS485 della **versione 4G** si possono collegare fino a quattro espansori **iO-8**; ciascuno aggiunge 8 I/O a doppia funzione. Collega i morsetti A 485 e B 485 ai morsetti A e B del modulo, e prendi l'alimentazione del modulo dall'uscita AUX a 12 V della centrale. Il modo di collegamento è descritto anche nel manuale dell'iO-8. Il modulo va aggiunto nella pagina **RS485 modules** di TrikdisConfig (paragrafo 6.7); gli eventi degli ingressi vanno alla centrale di vigilanza e in Protegus 2, le uscite si comandano dall'app.

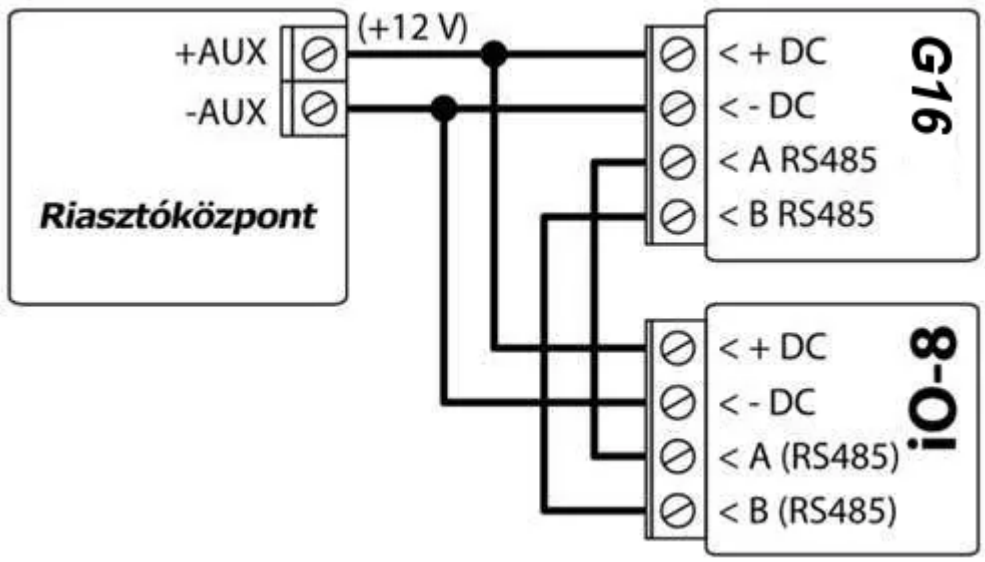


Figura 27. Collegamento dell'espansore iO-8 al bus RS485 del G16 (A 485 → A, B 485 → B); entrambi i dispositivi sono alimentati dall'uscita AUX della centrale d'allarme (+12 V).

Il G16 con modem 2G (G16_G410) non ha il bus RS485, quindi non è possibile collegarvi i moduli iO-8, W485 ed E485.

3.8 Collegamento dei moduli W485 ed E485

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

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

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

Finché la connessione WiFi o Ethernet è attiva, il G16 comunica tramite essa e non usa la connessione dati mobile; se la connessione si interrompe, passa alla connessione dati mobile e, al ripristino della connessione, torna al modulo. Per il funzionamento del modulo **nel G16 deve esserci una scheda SIM**.

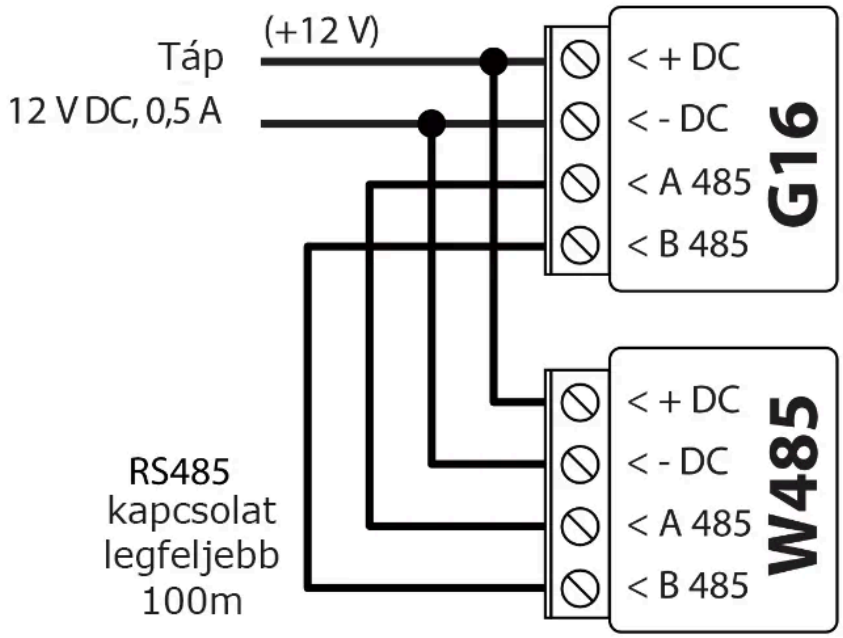


Figura 28. Collegamento del modulo WiFi W485 al G16 tramite bus RS485. I due dispositivi sono alimentati da un'alimentazione comune a 12 V DC (di almeno 0,5 A) (l'ingresso di alimentazione del modulo è 9–28 V DC); il cavo RS485 può essere lungo al massimo 100 m.

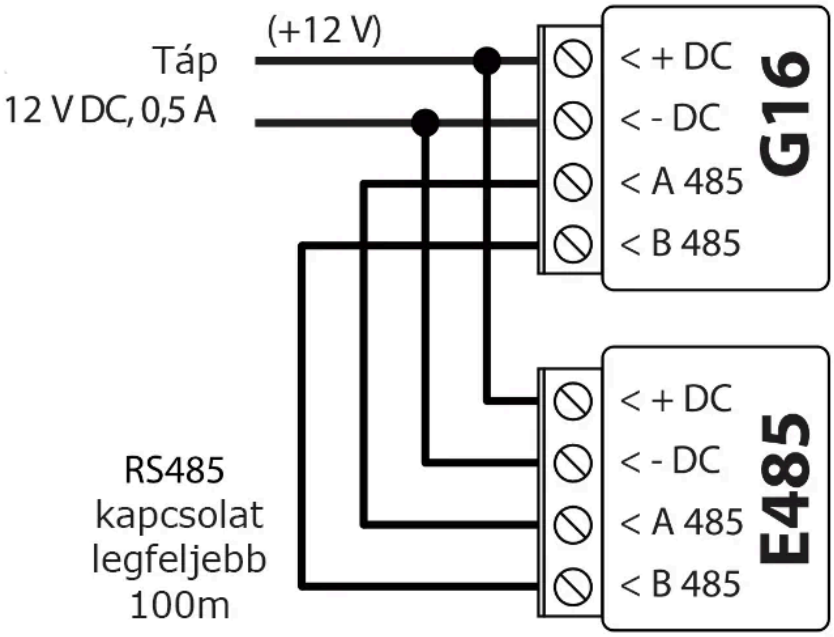


Figura 29. Collegamento del modulo Ethernet E485 al G16 tramite bus RS485. I due dispositivi sono alimentati da un'alimentazione comune a 12 V DC (di almeno 0,5 A) (l'ingresso di alimentazione del modulo è 9–28 V DC); il cavo RS485 può essere lungo al massimo 100 m.

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

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

3.9 Accensione e prima verifica

A TRIKDIS átjelző elindítása

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

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

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

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

- **POWER** verde fisso – l'alimentazione è corretta;
- **NETWORK** verde fisso e giallo lampeggiante – connesso alla rete; il numero di lampeggi è il livello del segnale (in 2G 5, in 4G 3 indicano un buon segnale);
- **TROUBLE** spento.

Se il LED NETWORK dà meno lampeggi gialli, il livello del segnale non è sufficiente: cerca un altro posto per il comunicatore oppure usa un'antenna più sensibile (paragrafo 3.2). Ogni segnalazione dei LED diversa da questa indica un guasto – identificalo con le tabelle del paragrafo 1.7. Se il TROUBLE lampeggia, il numero di lampeggi indica la causa (paragrafo 1.7). **7 lampeggi** indicano la mancanza di collegamento con la centrale: verifica i fili CLK e DATA, il tipo di centrale selezionato e – dove serve – la programmazione della centrale (capitolo 4). Se nessun LED è acceso, verifica l'alimentazione e il cablaggio.

4. Programmazione della centrale d'allarme

Questo capitolo descrive, per produttore, cosa occorre impostare nella centrale d'allarme affinché il G16 legga gli eventi e – dove possibile – controlli la centrale a distanza. Con la maggior parte delle centrali per la lettura degli eventi non serve programmare nulla; per il **controllo diretto** spunta l'opzione **Remote Arm/Disarm** nella pagina **System settings** di TrikdisConfig e, con le centrali Paradox e Texecom, inserisci anche la password PC o UDL della centrale nel campo **Security panel PC download password** (paragrafi 2.2 e 6.2).

Se controlli la centrale non direttamente, ma tramite una zona a chiave (paragrafo 3.4), il **Remote Arm/Disarm** deve restare vuoto, e questo capitolo riguarda solo le impostazioni necessarie per la lettura degli eventi.

4.1 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.

4.2 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.

4.3 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]**.

4.4 UTC Interlogix (Caddx)

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

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

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

Locazione (location)	Segmento	Impostazione
108	3	12345678

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

4.5 Crow e Pyronix

Le centrali **Crow Runner 4/8** e **Runner 8/16** non richiedono alcuna impostazione particolare.

Nemmeno le centrali **Pyronix** richiedono programmazione, ma dopo la configurazione e il collegamento del comunicatore **togli l'alimentazione alla centrale** (rete e batteria) e riavviala: la centrale accetta il comunicatore collegato al suo bus all'avvio.

4.6 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]**.

4.7 InnerRange Inception e Integriti

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.

Inception e Integriti trasmettono gli eventi al comunicatore; per l'inserimento e il disinserimento serve una zona a chiave (paragrafi 1.2 e 3.4).

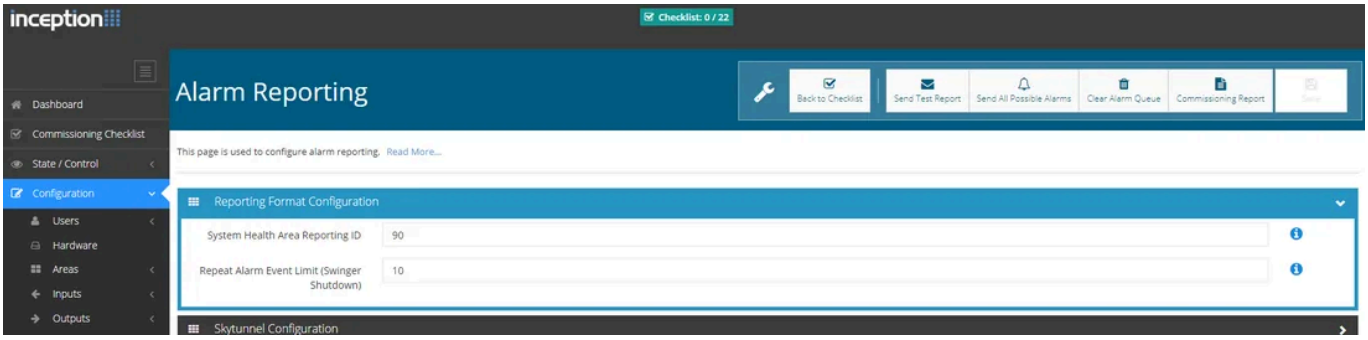


Figura 30. Interfaccia web dell'Inception – Configuration → General → Alarm Reporting.



Figura 31. Inception – 3rd Party Device Configuration.

- 1 **Enable 3rd Party Device Reporting** – spuntato.
- 2 **3rd Party Device Type** – Trikdis.
- 3 **Serial Port** – Serial Port 1 (Plugged In, In Use By 3rd Party Device).

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. Con il G16 l'inserimento può avvenire in due modi: con le centrali **controllabili direttamente** l'utente usa il proprio **codice tastiera**, con le centrali collegate tramite zona a chiave si usa l'**uscita** del comunicatore.

5.1 Aggiunta del dispositivo

Prima di aggiungere il dispositivo verifica:

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

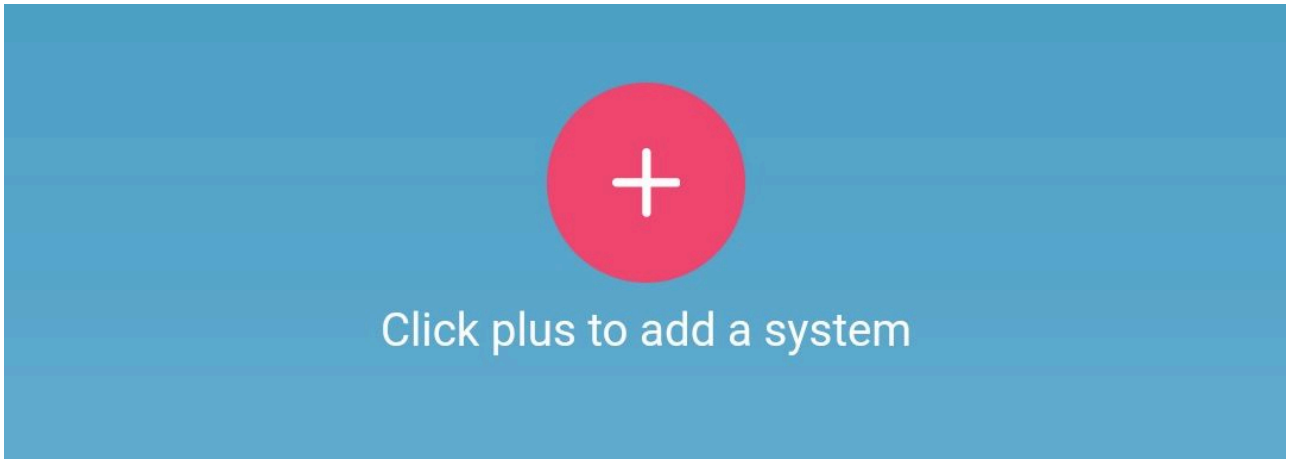
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è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

A rendszer létrehozása a Protegus 2 alkalmazásban

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



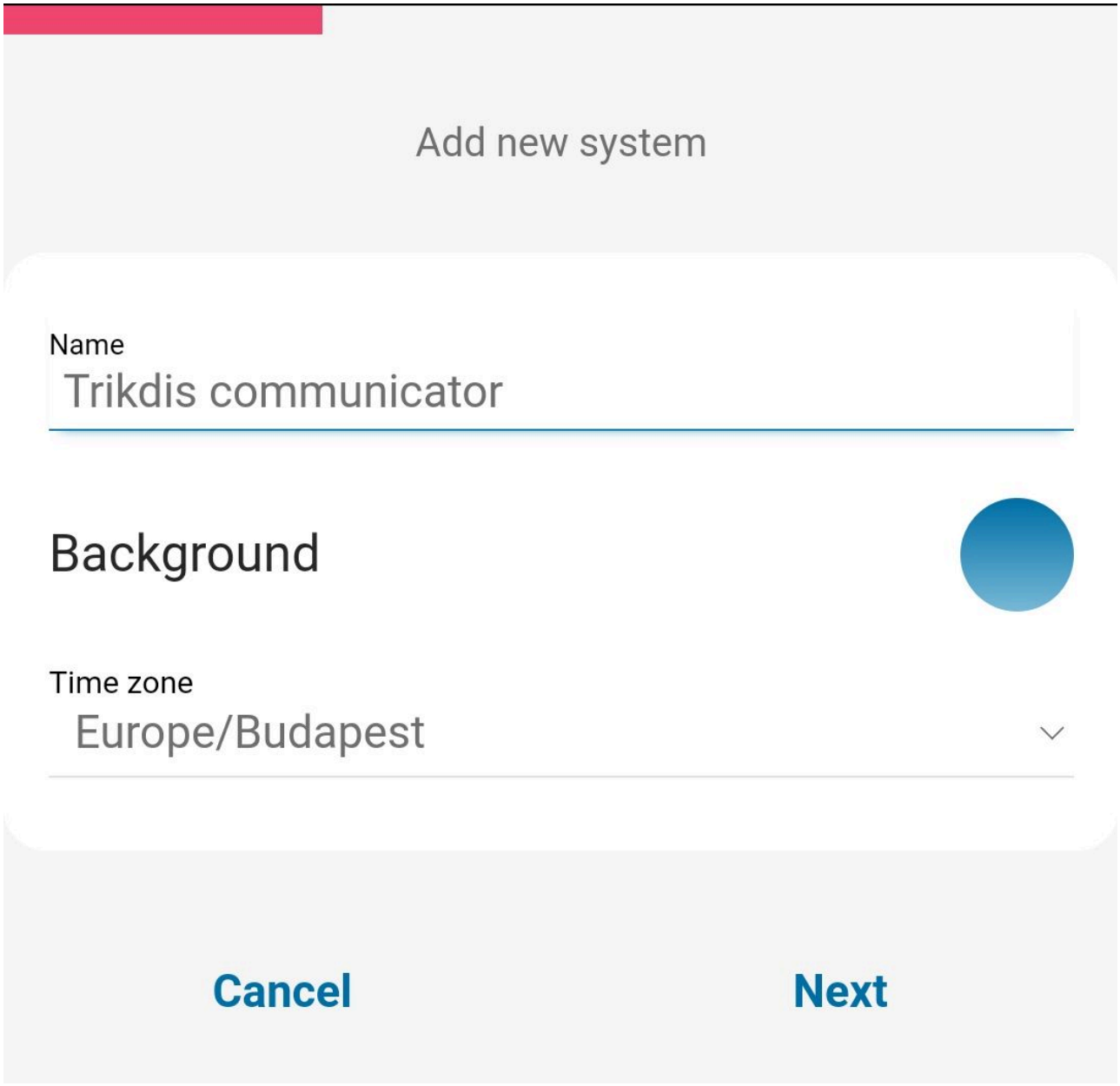
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



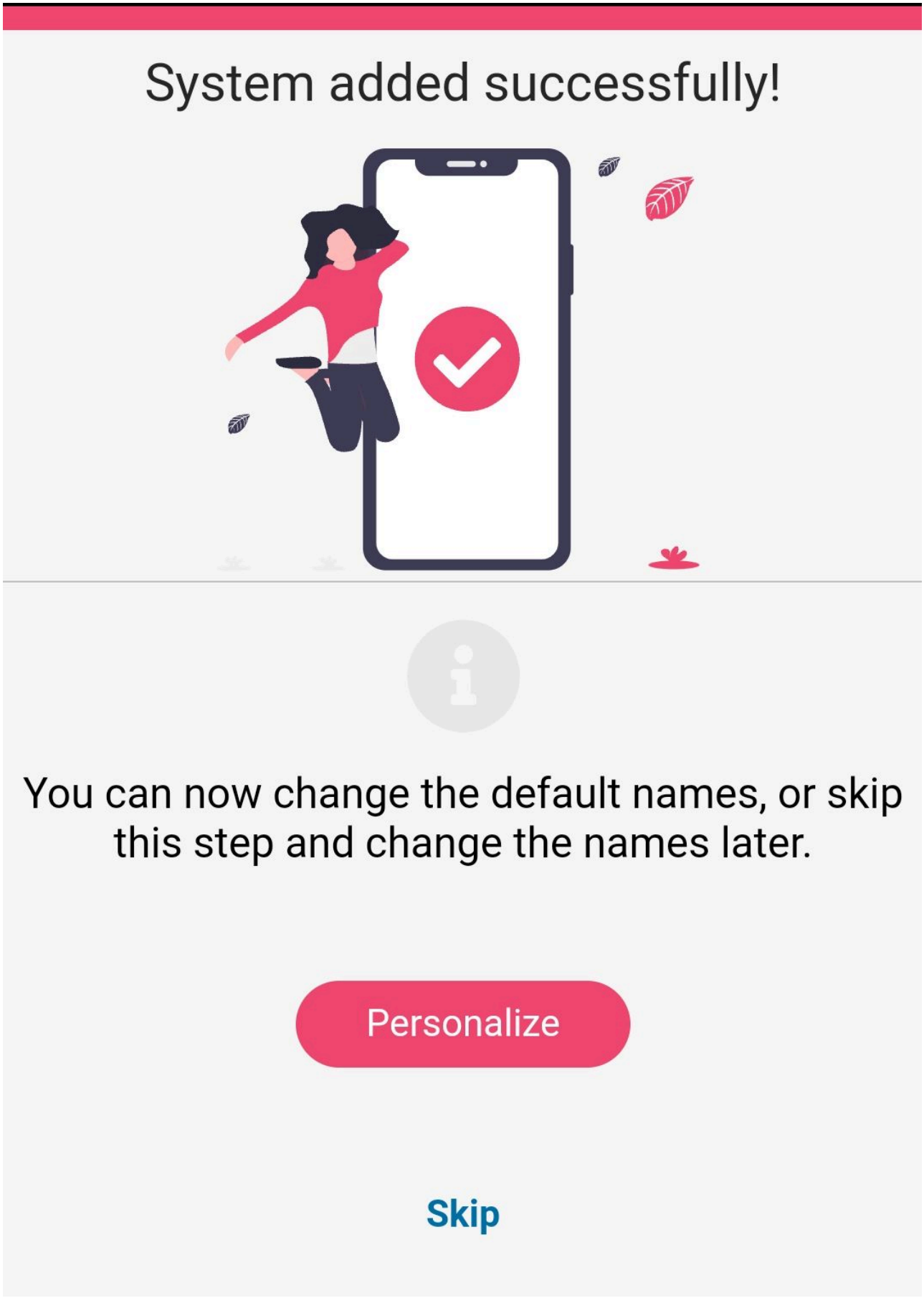
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



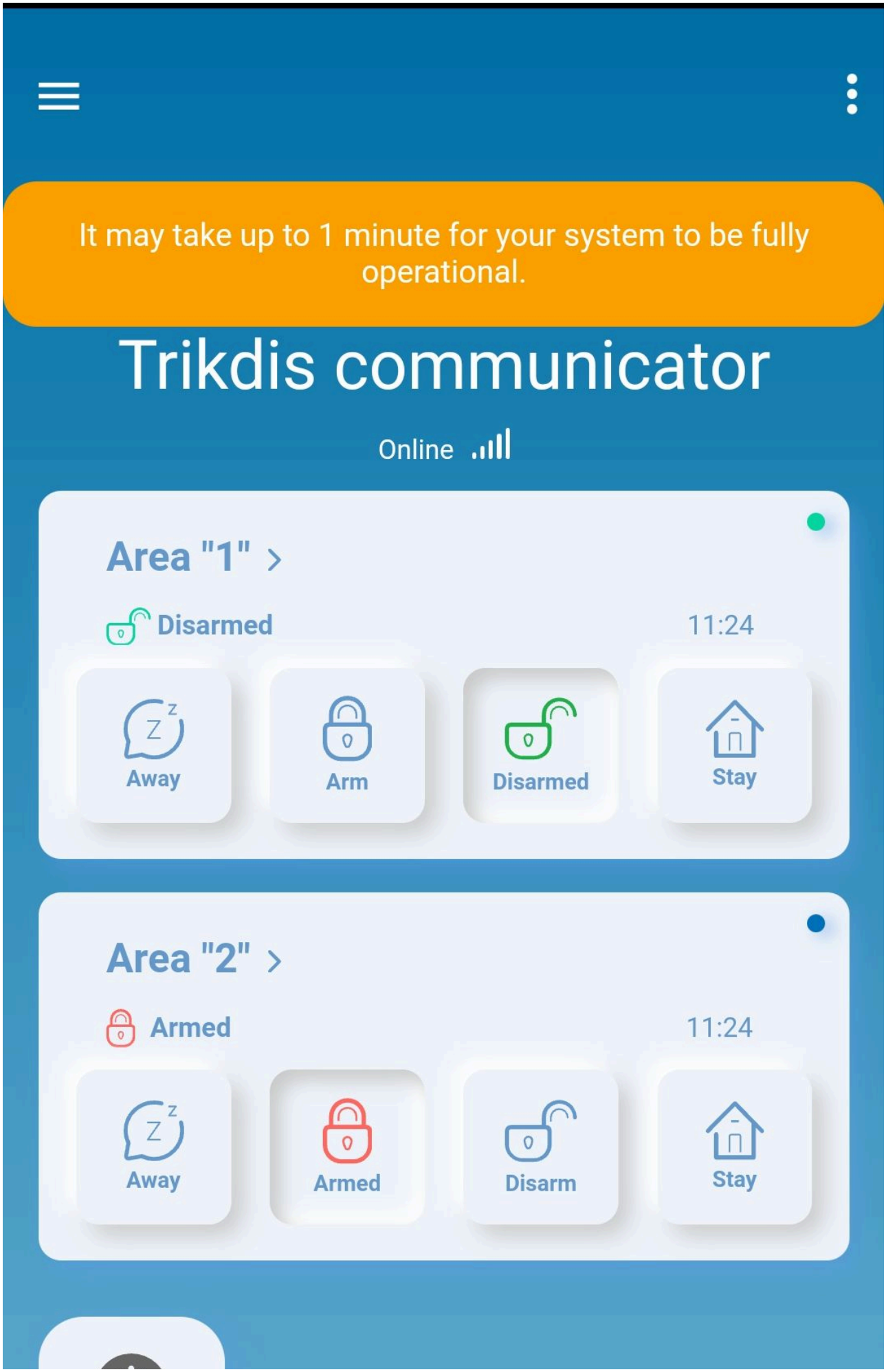
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



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

5.2 Controllo diretto con il codice tastiera

Se la centrale rientra tra i modelli controllabili direttamente (paragrafo 1.2) e nella pagina **System settings** di TrikdisConfig è spuntato **Remote Arm/Disarm**, Protegus 2 mostra le aree della centrale con lo stato letto dal bus e, per inserire / disinserire, l'utente inserisce nell'app **il codice tastiera della centrale** – lo stesso che usa sulla tastiera. Non servono un'uscita separata né una zona a chiave.

- Per questo, a seconda del produttore, serve un'impostazione nella centrale (Paradox: password PC, Texecom: password UDL; con le centrali Caddx, Honeywell e InnerRange l'abilitazione del bus o della porta seriale serve già per la lettura degli eventi) – vedi il capitolo 4.
- Il codice tastiera viene verificato dalla centrale, e anche il registro eventi della centrale registra l'utente, non il comunicatore.
- Con le centrali Paradox il codice dell'utente **non può essere il codice master**; dopo aver modificato il codice riavvia il comunicatore (paragrafo 4.2).
- Con le centrali DSC PowerSeries l'app mostra anche lo stato delle zone ed è possibile anche l'esclusione delle zone – dettagli nell'articolo sul controllo diretto DSC.

Alla creazione del sistema Protegus 2 chiede se l'inserimento è comandato dall'uscita del comunicatore. Con il controllo diretto **non** assegnare un'uscita all'area (**Control with Protegus2** disattivato): l'area è gestita dalla centrale, lo stato arriva dal bus.

5.3 Inserimento con zona a chiave

Se la centrale non è controllabile direttamente, oppure non vuoi usarla così, colleghi una delle uscite del comunicatore alla zona a chiave della centrale (paragrafo 3.4), in TrikdisConfig il **Remote Arm/Disarm** resta vuoto e in Protegus 2 assegni l'uscita all'area.

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

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

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

1. Seleziona (o aggiungi) l'area che vuoi controllare. Il numero dell'area deve coincidere con quello che la centrale invia negli eventi (l'area 1 con l'1, la 2 con il 2).

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

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

5.4 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.

Con il controllo diretto l'app chiede il codice tastiera della centrale; con l'inserimento tramite zona a chiave – se attivata – la password di Protegus 2.

5.5 Controllo con messaggi SMS

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

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

Con la password **amministratore** si possono usare tutti i comandi, con la password **installatore** i comandi INFO, RESET e OUTPUTx. `x` è il numero dell'uscita: il morsetto I/O impostato come uscita (1, 2 o 3) che vuoi commutare.

Comando	Dati	Che cosa fa	Esempio
`INFO`	–	Richiede informazioni sul dispositivo: tipo, IMEI, numero di serie, versione firmware	`123456 INFO`
`RESET`	–	Riavvia il dispositivo	`123456 RESET`
`OUTPUTx`	`ON`	Attiva l'uscita x	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Disattiva l'uscita x	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Genera un impulso sull'uscita x; `tttt` = la durata dell'impulso in secondi, con quattro cifre	`123456 OUTPUT2 PULSE=0002`
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Abilita o disabilita la connessione a Protegus	`123456 CONNECT PROTEGUS=ON`

Comando	Dati	Che cosa fa	Esempio
`CONNECT`	`IP=indirizzo:porta`	Indirizzo IP e porta del canale primario	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=chiave`	La chiave di crittografia TRK	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=nome`	L'APN della scheda SIM	`123456 CONNECT APN=internet`
`CONNECT`	`USER=nome`	Nome utente APN (se richiesto dall'operatore)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=password`	Password APN (se richiesta dall'operatore)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Selezione del tipo di centrale d'allarme con il numero d'ordine nell'elenco **Security panel model** di TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=nnnn` / `DIR=OFF`	La password di 4 cifre del controllo diretto (la password PC o UDL della centrale); `DIR=OFF` lo disattiva	`123456 CONNECT DIR=1122`

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

6. TrikdisConfig – le impostazioni in dettaglio

Nella finestra di TrikdisConfig si vedono a sinistra l'elenco delle pagine (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), in alto la barra dei pulsanti (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), in basso la barra di stato. Questo capitolo passa in rassegna le impostazioni del G16 pagina per pagina.

6.1 La barra di stato

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

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

Etichetta	Significato
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.

Nel campo **Device**, con il G16, deve comparire la sigla del modello G16 (ad esempio G16_G410 o G16_54E0). Dopo la lettura il programma mostra le impostazioni memorizzate nel G16; impostale secondo le descrizioni delle pagine riportate qui sotto.



Figura 32. La barra di stato di TrikdisConfig con un G16 letto: identificativo, stato, modello, numero di serie, versioni, modalità di connessione e livello di accesso.

6.2 System settings

La pagina è composta da due gruppi: nel gruppo **General** imposti il funzionamento di base del dispositivo e il suo collegamento con la centrale d'allarme, nel gruppo **Access** i livelli di accesso.

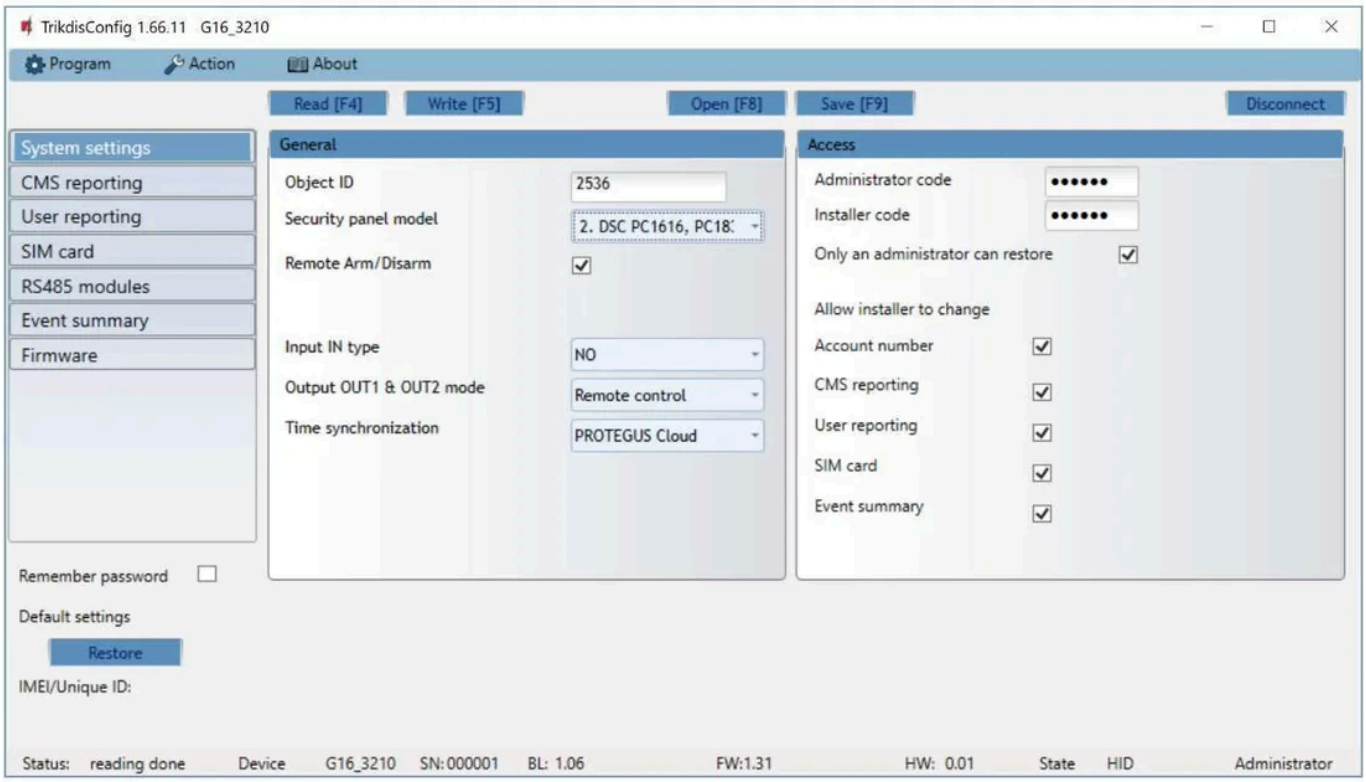


Figura 33. TrikdisConfig – pagina System settings: gruppi General e Access (nell'immagine la versione hardware 3, G16_3210; sulla versione 4 non ci sono i campi Input IN type e Output OUT1 & OUT2 mode, che sono stati spostati nella pagina IN/OUT).

- **Object ID** – l'identificativo dell'impianto ricevuto dalla centrale di vigilanza (4 caratteri esadecimali, 0–9, A–F). Obbligatorio se il dispositivo trasmette anche alla centrale di vigilanza; `FFFE` e `FFFF` non possono essere usati.
- **Security panel model** – il tipo della centrale d'allarme collegata, dall'elenco. Da questo dipende come il comunicatore legge il bus, quindi scegli il tipo esatto della centrale collegata.
- **Remote Arm/Disarm** – se spuntato, il comunicatore controlla direttamente la centrale: l'utente inserisce e disinserisce da Protegus 2 con il proprio codice tastiera. Appare solo con i tipi di centrale controllabili direttamente; a seconda del produttore serve un'impostazione nella centrale (capitolo 4). Con l'inserimento tramite zona a chiave lascialo vuoto.
- **Security panel PC download password** – per il controllo diretto delle centrali Paradox e Texecom, la password PC o UDL della centrale (4 caratteri); deve coincidere con quella impostata nella centrale (paragrafi 4.2 e 4.3).
- **Time set** – la sorgente dell'orologio del dispositivo (predefinito **Cloud application**, il cloud Protegus).
- Sulla **versione hardware 3** qui si trovano anche i campi **Input IN type** (il tipo dell'ingresso: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) e **Output OUT1 & OUT2 mode** (la modalità delle due uscite; per l'inserimento con zona a chiave **Remote control**).

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

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

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

Non lasciare le password di fabbrica nel dispositivo!

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

6.3 CMS reporting

Il comunicatore invia gli eventi alla centrale di vigilanza tramite connessione dati mobile (IP) o via SMS. Gli eventi possono andare su più canali: il canale **primario** e quello **parallelo** funzionano contemporaneamente (a due ricevitori insieme), e a ciascuno appartiene un canale **di riserva**, che entra in funzione se il canale in questione si interrompe. La comunicazione è crittografata e protetta da password; per la ricezione serve un ricevitore Trikdis (ricevitore software IPcom, RL14, RM14) o un ricevitore universale che conosca il protocollo DC-09 / TL150. I ricevitori Trikdis inoltrano gli eventi al software di vigilanza: via IP il ricevitore software **IPcom** (Windows / Linux), il ricevitore IP/SMS **RL14** o il ricevitore multicanale **RM14**; per la ricezione degli SMS l'RL14, l'RM14 o il ricevitore SMS **GM14**.

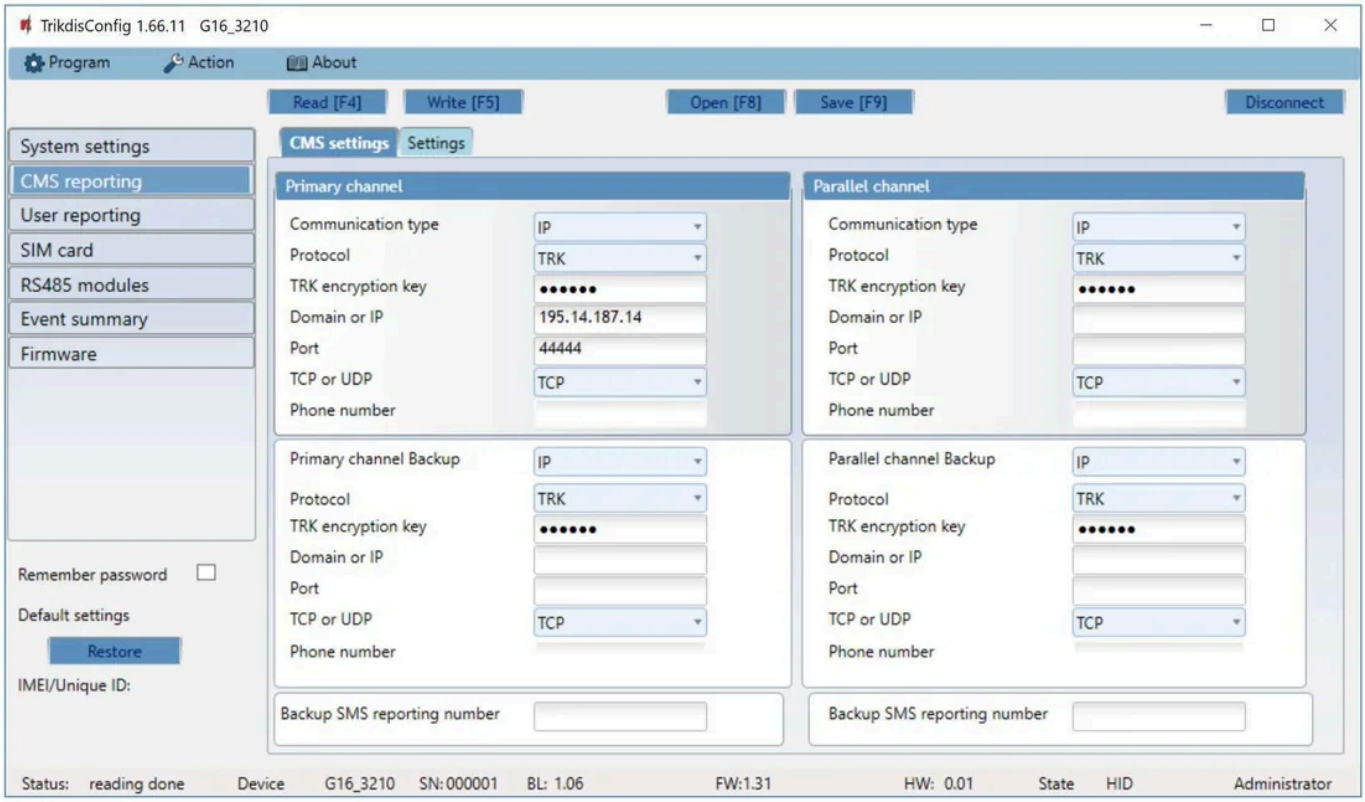


Figura 34. TrikdisConfig – CMS reporting, scheda CMS settings: canale primario, di riserva e parallelo.

Primary channel – canale primario

- **Communication type** – IP o SMS. L'SMS va bene come riserva – funziona anche se non c'è connessione dati mobile –, come canale primario non è consigliato.
- **Protocol** – TRK (ricevitori Trikdis), DC-09_2007 o DC-09_2012 (ricevitori universali), TL150 (SUR-GARD).
- **TRK encryption key** – chiave di crittografia di 6 cifre; deve essere la stessa nel comunicatore e nel ricevitore.
- **Domain or IP**, **Port** – l'indirizzo e la porta del ricevitore.
- **TCP or UDP** – il protocollo di trasmissione.
- **Phone number** – solo con la comunicazione SMS: il numero di telefono del ricevitore SMS Trikdis con il prefisso internazionale (ad es. `CCxxxxxxxxx`, dove CC è il prefisso internazionale).

Primary channel Backup – canale di riserva. Prende in carico la comunicazione se il canale primario non funziona; le sue impostazioni sono le stesse di quelle sopra.

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

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

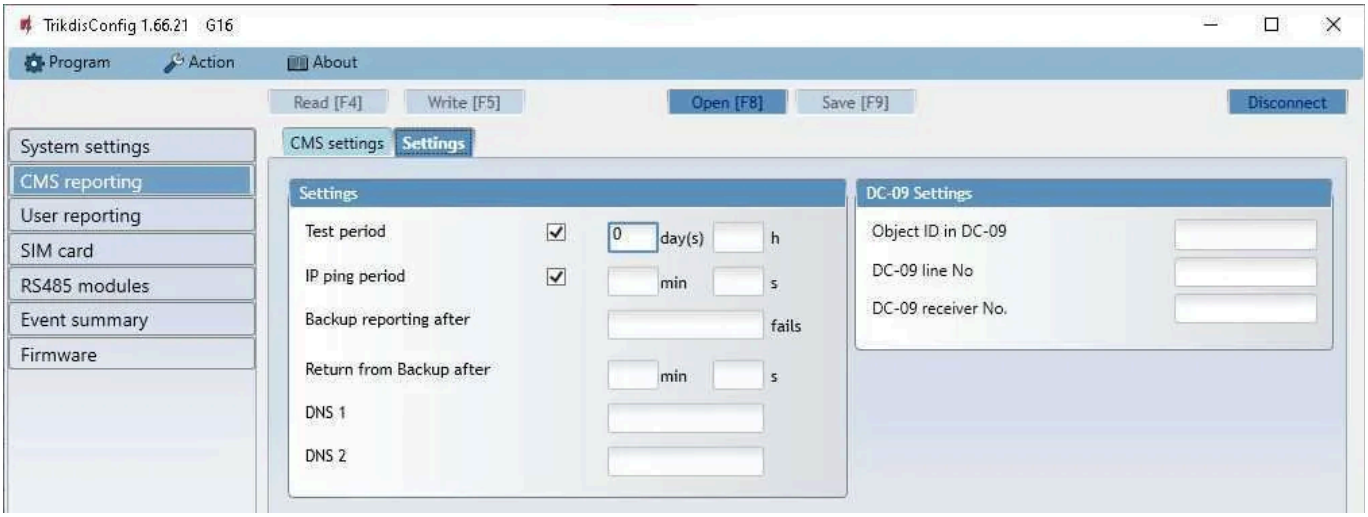


Figura 35. TrikdisConfig – CMS reporting, scheda Settings: rapporto di test, PING, tempi del canale di riserva, DNS e dati DC-09.

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

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

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

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

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

In fondo alla scheda: **DNS 1, DNS 2** – server dei nomi; servono se hai indicato il ricevitore con un nome di dominio e non con un indirizzo IP. Il valore predefinito è il DNS pubblico di Google. Il gruppo **DC-09 settings** è visibile solo se su uno dei canali è impostato il protocollo DC-09.

6.4 User reporting

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

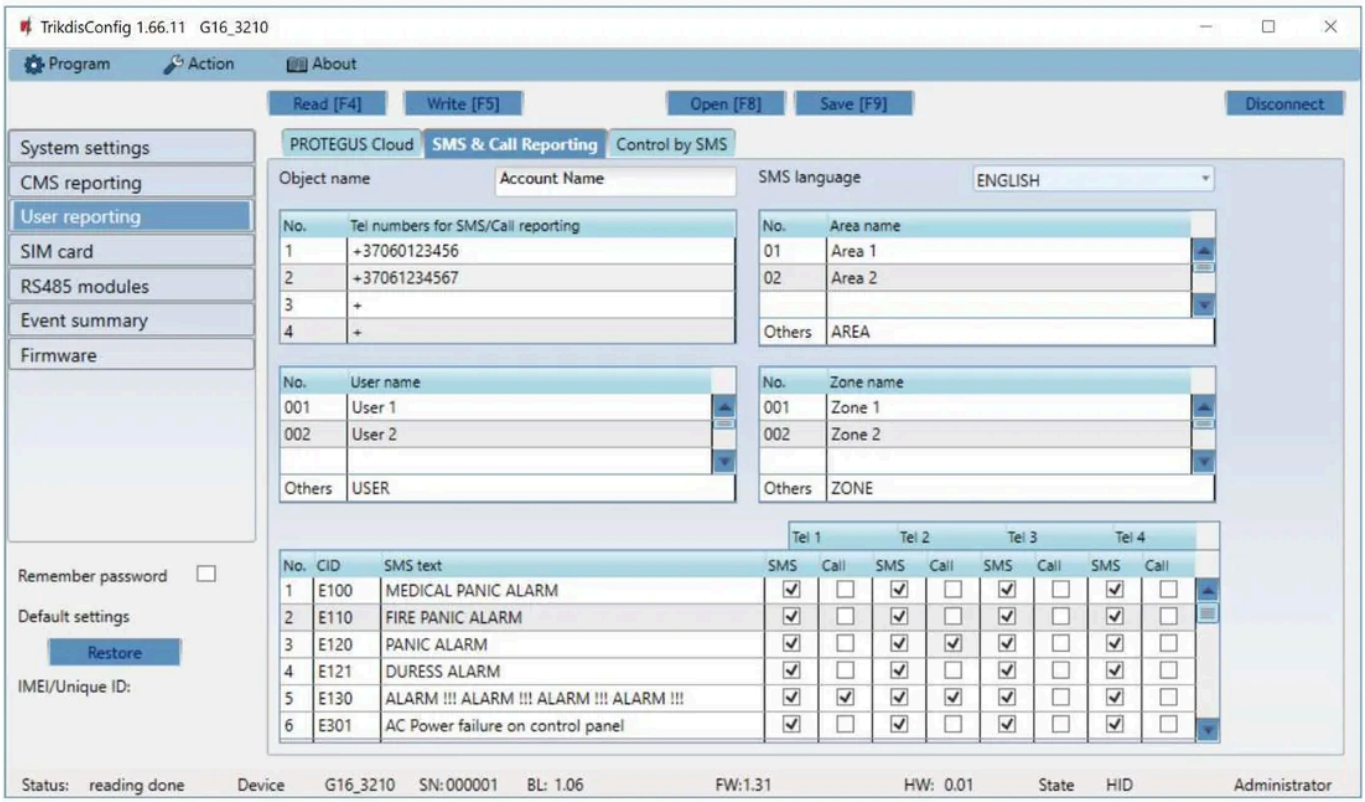


Figura 36. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

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

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

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

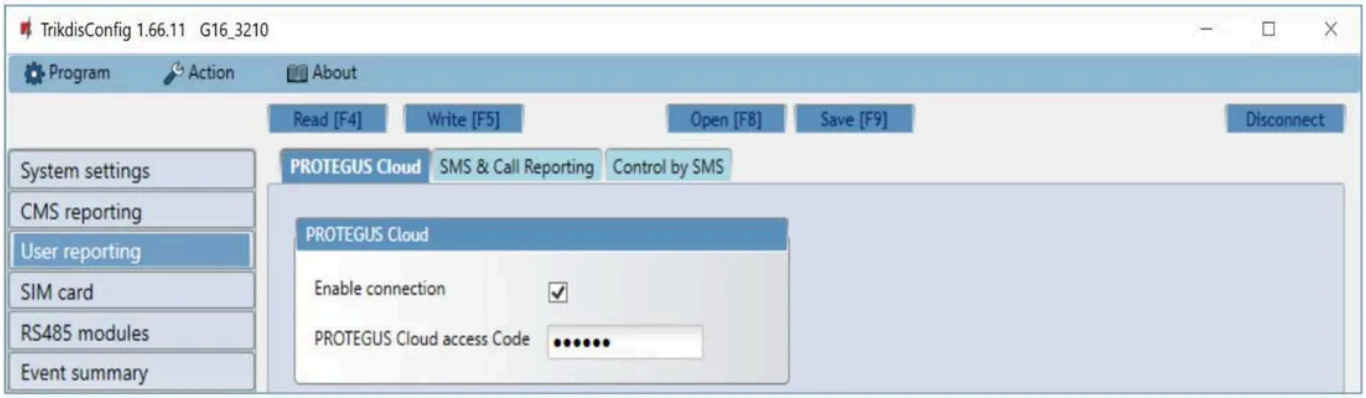


Figura 37. TrikdisConfig – User reporting, scheda SMS & Call Reporting.

- **Object name** – il nome del sistema; compare in ogni SMS.
- **SMS language** – la lingua degli SMS (per i caratteri accentati della lingua).

- **Tel numbers for SMS/Call reporting** – fino a 4 numeri di telefono con il prefisso internazionale (`+CC…`, `00CC…` o `CC…`, dove CC è il prefisso internazionale).
- **Area name, User name, Zone name** – i nomi delle aree, degli utenti e delle zone; il dispositivo li usa nel testo degli SMS. Nella tabella corrispondente scrivi il numero dell'area, dell'utente o della zona e accanto il suo nome. Con una centrale letta dal bus arrivano i numeri di zona e di utente propri della centrale: assegna i nomi a questi.
- **CID event table** – per ogni evento si può impostare quale numero riceva l'SMS o la chiamata; il testo del messaggio e il codice Contact ID possono essere modificati e si può aggiungere anche un nuovo evento.

Nella scheda **Control by SMS** imposti la ricezione dei comandi SMS (i comandi sono descritti nel paragrafo 5.5).



Figura 38. TrikdisConfig – User reporting, scheda Control by SMS.

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

6.5 SIM card

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

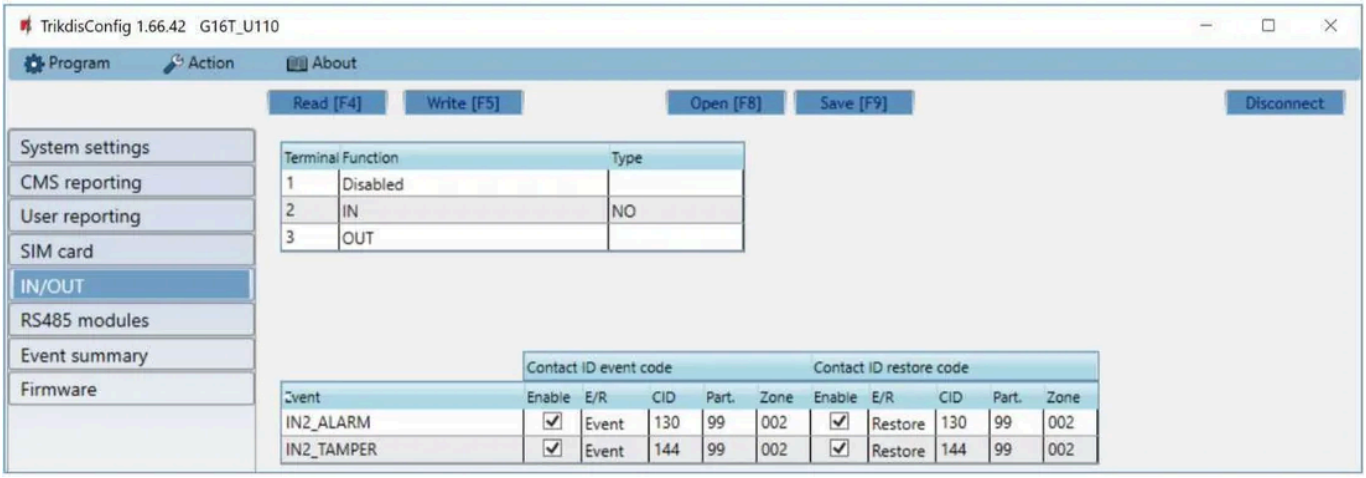


Figura 39. TrikdisConfig – pagina SIM card.

- **SIM card PIN** – il codice PIN della scheda. Puoi disattivare la richiesta del PIN inserendo la scheda in un telefono cellulare e disabilitandola lì. Se la richiesta del PIN è disattivata, può restare il valore di fabbrica del campo.
- **APN** – il punto di accesso dell'operatore (Access Point Name); senza di esso il comunicatore non può connettersi a Internet. Lo trovi anche sul sito dell'operatore; l'APN "internet" è generico e funziona nella 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 dell'APN, se l'operatore li richiede.
- **Forbid connection when roaming detected** – utile vicino a un confine di Stato: impedisce che il dispositivo si connetta alla rete del Paese confinante.

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

6.6 IN/OUT

Qui indichi il ruolo dei tre morsetti I/O a doppia funzione del comunicatore: **Disabled** (non usato), **IN** (ingresso) o **OUT** (uscita). Per un ingresso va indicato anche il tipo (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Impostazione di fabbrica: I/O 1 non usato, I/O 2 ingresso (NO), I/O 3 uscita.



Figura 40. TrikdisConfig – pagina IN/OUT: la funzione dei morsetti I/O e gli eventi degli ingressi.

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

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

Sulla **versione hardware 3** non c'è la pagina IN/OUT: il tipo dell'unico ingresso si imposta nel campo **System settings** → **Input IN type**, la modalità delle due uscite nel campo **Output OUT1 & OUT2 mode**, e gli eventi dell'ingresso (IN_ALARM, IN_TAMPER) nella pagina **Event summary**.

6.7 RS485 modules

Gli espansori iO-8 e i moduli W485 / E485 collegati al bus RS485 vanno aggiunti nella scheda **Modules list**.

Sul G16 con modem 2G (G16_G410) questa pagina non può essere usata: la versione 2G non ha il bus RS485.

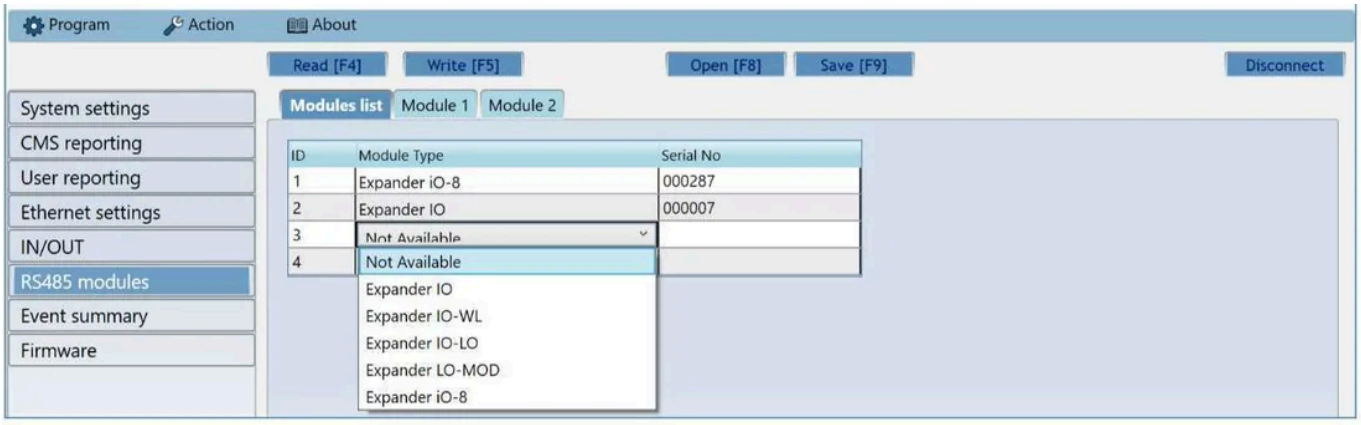


Figura 41. TrikdisConfig – RS485 modules, scheda Modules list: il tipo di modulo (Expander iO-8, W17u/W485, E485) e il numero di serie.

- **Module Type** – il tipo del modulo collegato, dall'elenco (Expander iO-8, W17u/W485, E485).
- **Serial No** – il numero di serie di 6 cifre del modulo (sul modulo e sulla sua scatola, SN).

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

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

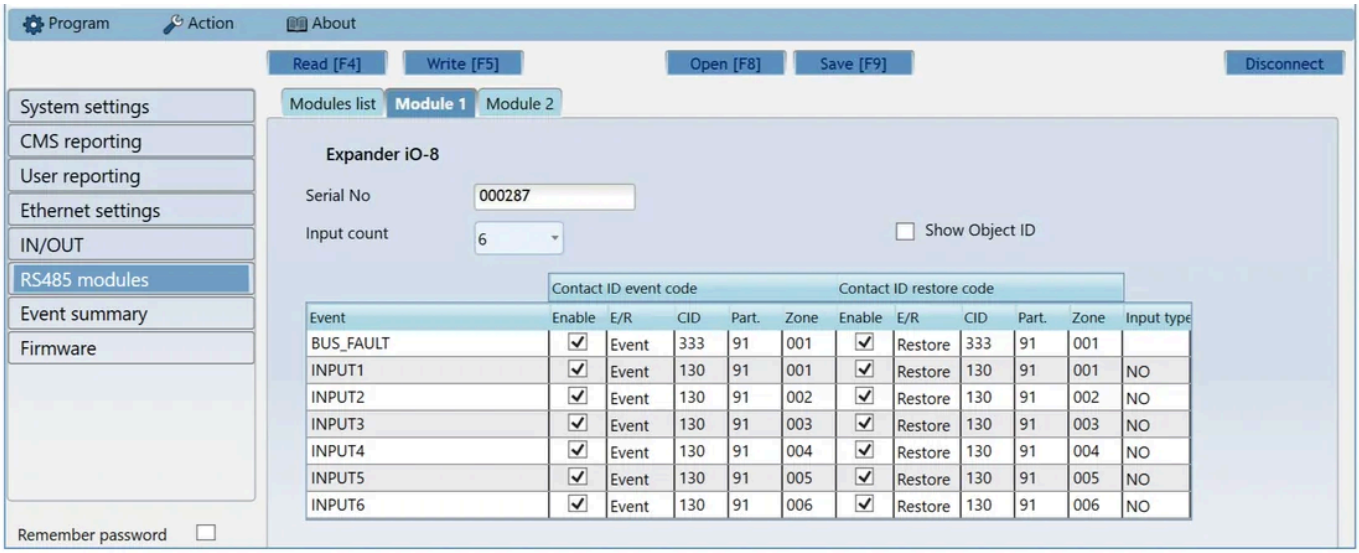


Figura 42. TrikdisConfig – RS485 modules, scheda del modulo iO-8.

- **Input Count** – quanti morsetti devono essere ingressi; gli altri saranno uscite. Il tipo d'ingresso (**Input type**: NO o NC) si indica nella tabella. Il ruolo delle uscite (inserimento / disinserimento con zona a chiave o comando di un dispositivo) lo imposti nell'app Protegus 2.
- Nella tabella puoi assegnare un codice Contact ID al guasto del bus (**BUS_FAULT**, Contact ID 333) e agli eventi di violazione e ripristino degli ingressi (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Alla violazione dell'ingresso il comunicatore invia un evento con il codice impostato al ricevitore della centrale di vigilanza, all'app Protegus 2 e via SMS al numero di telefono dell'utente. Per impostazione predefinita il modulo 1 trasmette con l'area 91, il modulo 4 con l'area 94. Spuntando **Show Object ID** si può indicare per gli ingressi anche un identificativo dell'impianto diverso da quello del comunicatore.

- Se l'utente deve ricevere SMS o chiamate anche per gli ingressi dell'espansore, aggiungi il codice Contact ID assegnato all'ingresso anche alla tabella eventi della scheda **SMS & Call Reporting**.

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



Figura 43. TrikdisConfig – RS485 modules, scheda del modulo W485.

- **DHCP mode** – impostazione di rete automatica (DHCP) o manuale (Static).
- **Static IP**, **Subnet mask**, **Default gateway** – con l'impostazione manuale.
- **Wifi SSID name**, **Wifi SSID password** – il nome e la password della rete WiFi.
- Nella tabella puoi assegnare un codice Contact ID ai guasti del bus RS485 (interruzione e ripristino del collegamento tra il modulo e il G16); l'evento lo ricevono sia la centrale di vigilanza sia Protegus 2.

Modulo Ethernet E485 – le stesse impostazioni di rete senza WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); anche qui nella tabella puoi assegnare al guasto del bus RS485 (interruzione e ripristino del collegamento tra l'E485 e il G16) un codice Contact ID, che ricevono sia la centrale di vigilanza sia Protegus 2.

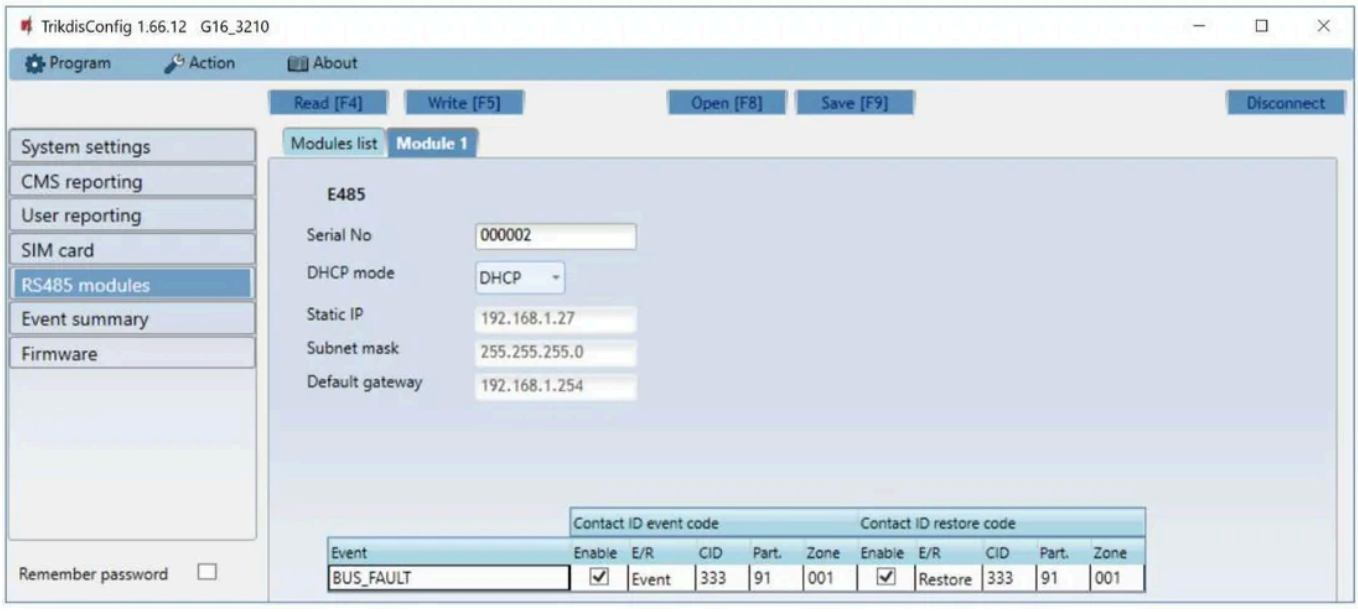


Figura 44. TrikdisConfig – RS485 modules, scheda del modulo E485.

Per il funzionamento del W485 e dell'E485 la connessione del G16 alla centrale di vigilanza e/o a Protegus deve essere impostata (paragrafi 2.3 e 2.4) e nel G16 deve esserci una scheda SIM. Finché la connessione cablata o WiFi è attiva, il comunicatore comunica tramite essa e non usa la connessione dati mobile.

6.8 Event summary

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

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

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

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

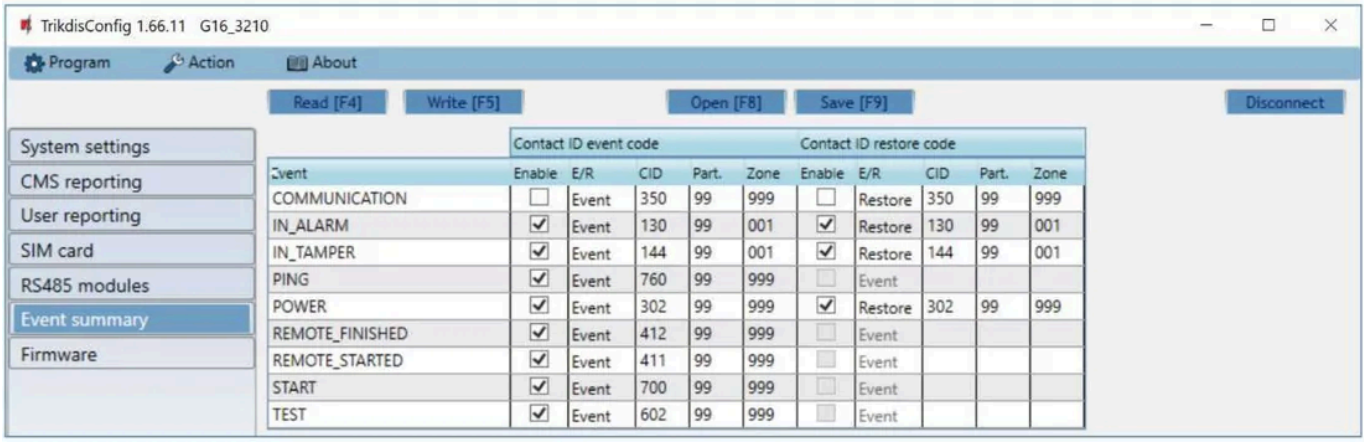


Figura 45. TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo (nell'immagine la versione hardware 3, nella quale qui compaiono anche gli eventi IN_ALARM e IN_TAMPER dell'ingresso e il PING; sulla versione 4 gli eventi degli ingressi sono nella pagina IN/OUT).

6.9 Ripristino delle impostazioni di fabbrica

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

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

7. Programmazione a distanza

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

Per l'accesso da remoto servono:

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

Passaggi:

1. Avvia il software TrikdisConfig.
2. Nella sezione **Remote access**, nel campo **Unique ID**, inserisci l'identificativo univoco del dispositivo (IMEI o MAC).
3. Se vuoi, dai un nome al sistema nel campo **System name** – il programma lo ricorda e la volta successiva puoi sceglierlo dall'elenco a discesa.
4. Premi il pulsante **Configure**.

5. Nella finestra che si apre fai clic sul pulsante **Read [F4]** (lettura) e inserisci la password. Con la spunta **Remember password** il programma la ricorda per questa sessione.
6. Esegui le modifiche, poi inviale al dispositivo con il pulsante **Write [F5]** (scrittura).

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

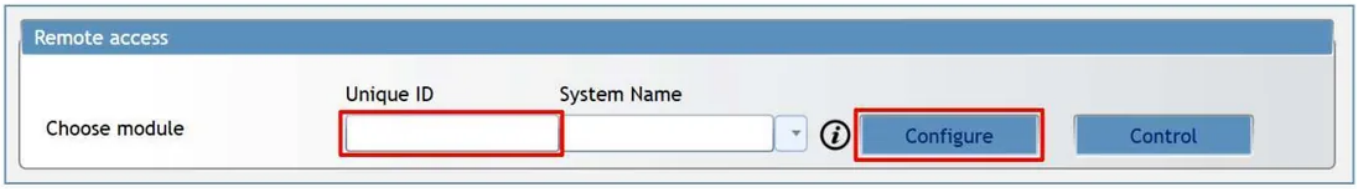


Figura 46. TrikdisConfig – Remote access: l'identificativo del dispositivo, il nome del sistema e il pulsante Configure.

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.

Con una centrale collegata al bus verifica anche che il comunicatore legga davvero dalla centrale: inserisci e disinserisci la centrale dalla tastiera e controlla che nell'elenco eventi di Protegus 2 (e presso la centrale di vigilanza) l'evento compaia con il numero di area e di utente corretto. Con il controllo diretto esegui anche un inserimento di prova dall'app, con il codice tastiera dell'utente.

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.

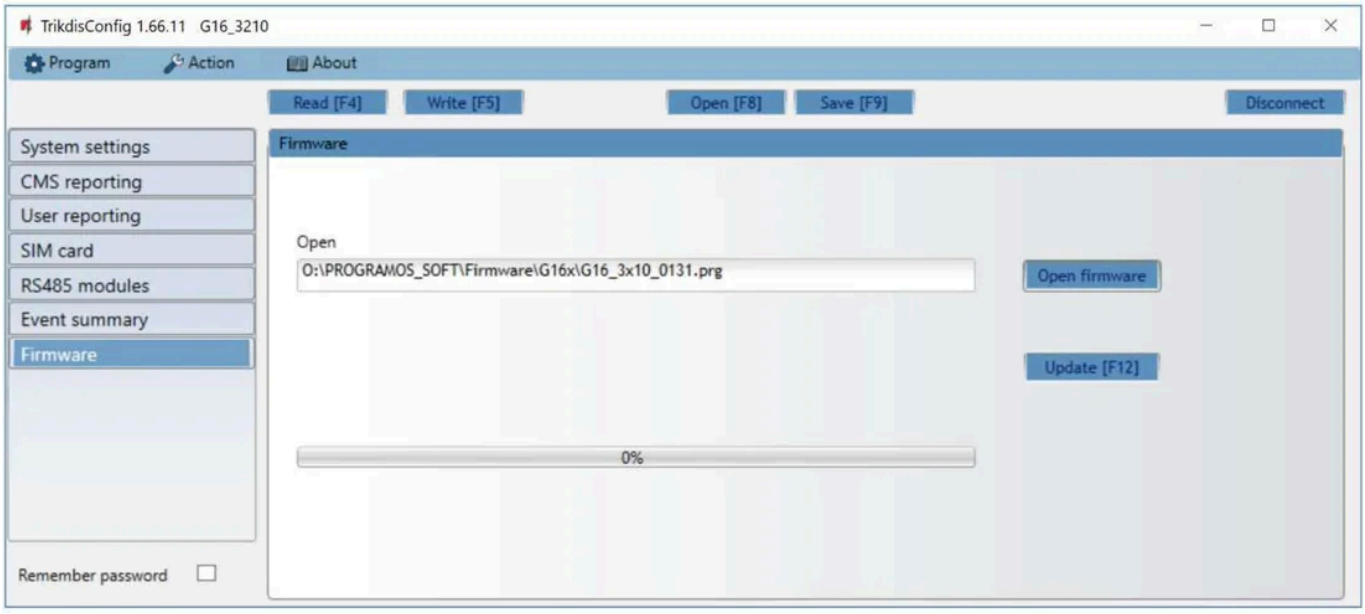


Figura 47. TrikdisConfig – pagina Firmware: Open firmware e Update [F12].

Per l'aggiornamento serve una connessione Internet. Un antivirus, un firewall o impostazioni di rete restrittive possono impedire il download automatico del firmware; in tal caso modifica le impostazioni dell'antivirus (consenti a TrikdisConfig l'accesso a Internet), oppure scarica il file manualmente e aprilo nella pagina Firmware.

10. Risoluzione dei problemi e domande frequenti

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

Il LED NETWORK non si accende – nessuna rete

1. Guarda i lampeggi del LED **TROUBLE**: 1 = nessuna SIM, 2 = PIN errato, 3 = manca l'APN, 4 = non riesce a connettersi alla rete mobile, 5 = non riesce a connettersi alla rete dati.
2. Verifica che la scheda SIM sia attiva, abbia il servizio dati e sia ben inserita nell'alloggiamento.
3. Se sulla scheda la richiesta del PIN è attiva, inserisci il PIN nella pagina **SIM card**, oppure disattiva la richiesta del PIN in un telefono.
4. Verifica l'antenna: è avvitata, non è in una scatola metallica, il livello del segnale è adeguato (paragrafi 1.7 e 3.2).

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

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

1. 6 lampeggi del LED **TROUBLE** indicano che non c'è connessione con il ricevitore: verifica l'indirizzo e la porta del ricevitore, l'impostazione TCP/UDP e la chiave di crittografia (**CMS reporting**).
2. Se il ricevitore è indicato con un nome di dominio, verifica l'impostazione DNS (**CMS reporting** → **Settings**).
3. Verifica che il piano dati della scheda SIM non blocchi la porta necessaria (alcune schede M2M consentono solo indirizzi determinati).

Il LED TROUBLE lampeggia sette volte – il comunicatore non vede la centrale

1. Verifica il collegamento secondo la figura del paragrafo 3.3: l'errore più frequente sono i fili **CLK** e **DATA** invertiti, oppure la linea dati collegata al morsetto sbagliato della centrale.
2. Nel campo **System settings** → **Security panel model** di TrikdisConfig deve essere selezionato il tipo esatto della centrale collegata.
3. Con le centrali Texecom, Caddx, Honeywell e InnerRange serve un'impostazione anche nella centrale (capitolo 4) – senza di essa la centrale non fornisce dati sul bus.
4. Con le centrali Paradox può darsi che la porta seriale sia bloccata di fabbrica – ecco come sbloccarla.
5. Dopo il collegamento togli l'alimentazione alla centrale Pyronix e riavviala, affinché accetti il comunicatore.
6. Con la centrale DSC PowerSeries **NEO** il G16 non funziona (il bus NEO non consente dispositivi esterni) – qui serve un comunicatore per linea telefonica.

Gli eventi arrivano, ma non riesco a inserire dall'app

Con il controllo diretto:

1. Nella pagina **System settings** deve essere spuntato **Remote Arm/Disarm**.
2. Con le centrali Paradox e Texecom la **Security panel PC download password** deve coincidere con la password PC o UDL della centrale (paragrafi 4.2 e 4.3).
3. Con le centrali Paradox il firmware della centrale deve essere almeno **V.4**; il codice dell'utente non deve essere il codice master; dopo aver modificato il codice riavvia il comunicatore.
4. Con le centrali Honeywell Vista deve essere abilitato il 2° indirizzo AUI (paragrafo 4.6).
5. In Protegus 2 all'area **non** deve essere assegnata un'uscita (Control with Protegus2 disattivato).

Con la zona a chiave:

1. Il **Remote Arm/Disarm** deve essere vuoto, il morsetto I/O deve essere **OUT** nella pagina **IN/OUT**.
2. La zona della centrale deve essere di tipo a chiave e in Protegus 2 all'area deve essere assegnata l'uscita corretta, nella modalità impulsiva o bistabile corrispondente alla zona (paragrafo 5.3).

Protegus 2 non vede il dispositivo

1. Nella scheda **User reporting** → **PROTEGUS Cloud** deve essere spuntato **Enable connection**.

2. Alla creazione del sistema va inserito il **Protegus Cloud access code** impostato nel dispositivo; dopo la creazione del sistema non può più essere modificato nel dispositivo.
3. Inserisci l'IMEI esattamente, dalla scatola o dal retro del dispositivo.
4. Il servizio dati della scheda SIM e l'APN devono essere a posto (il LED NETWORK è verde e il LED DATA si spegne dopo un evento).

Non riesco ad accedere a distanza con TrikdisConfig

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

Ho dimenticato la password

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

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

Il G16 con modem 2G (G16_G410) non ha il bus RS485; iO-8, W485 ed E485 si possono collegare solo alla versione 4G (G16_54E0). Per i moduli W485 ed E485 nel G16 deve esserci anche una scheda SIM.

Ho un dispositivo 2G – fino a quando funzionerà?

La dismissione delle reti 2G procede con tempi diversi a seconda dell'operatore; per un funzionamento a lungo termine consigliamo la versione 4G, che è anche espandibile tramite bus RS485.

Quanto traffico dati usa il dispositivo?

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

11. Norme di sicurezza

Figyelem!

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

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

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

- L'installazione e la manutenzione delle apparecchiature di sicurezza possono essere eseguite solo da un installatore qualificato.

- Prima dell'installazione leggi attentamente il manuale; ignorare le istruzioni può causare malfunzionamenti o guasti.
- Prima del collegamento, prima di ogni connessione elettrica e prima della manutenzione scollega l'apparecchiatura dall'alimentazione.
- I guasti derivanti da installazione o uso non corretti, nonché le modifiche e le riparazioni non autorizzate dal produttore, invalidano la garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare il dispositivo guasto e i suoi componenti nei rifiuti domestici.

Vedi anche

- Motore di ricerca della compatibilità – quale comunicatore è adatto a quale centrale d'allarme.
- G16 – controllo diretto per le centrali d'allarme DSC PowerSeries – inserimento con il codice tastiera, stato delle zone, esclusione delle zone.
- DSC Power Series NEO e comunicatori Trikdis: compatibilità e soluzioni – perché il G16 non può essere collegato alla NEO e qual è la soluzione.
- Sblocco della porta seriale bloccata nelle centrali d'allarme Paradox – lo sblocco della porta seriale delle centrali Paradox più recenti.
- Inserimento a distanza con zona a chiave dall'app Protegus 2 – i dettagli e le insidie dell'inserimento con zona a chiave.
- Arriva la versione hardware v4 dei comunicatori GSM G16 e G16T – cosa è cambiato rispetto alla versione 3.
- Impostazione dell'APN – elenco degli operatori mobili europei – l'APN della scheda SIM per operatore.
- Documentazione in inglese: docs.trikdis.com.

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

Prodotti correlati

Trikdis G16 4G GSM comunicatore intelligente

Trikdis G16 2G GSM comunicatore intelligente

Trikdis CRP2 cavo di collegamento porta seriale per pannelli allarme Paradox

CRP2B cavo di collegamento porta seriale per pannelli allarme Paradox

Trikdis CRP4 cavo seriale per pannelli di controllo Texecom

Trikdis iO8 modulo di espansione cablato

Diritti d'autore

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

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

Versione sempre aggiornata di questo manuale: https://trikdis.it/manuale-g16