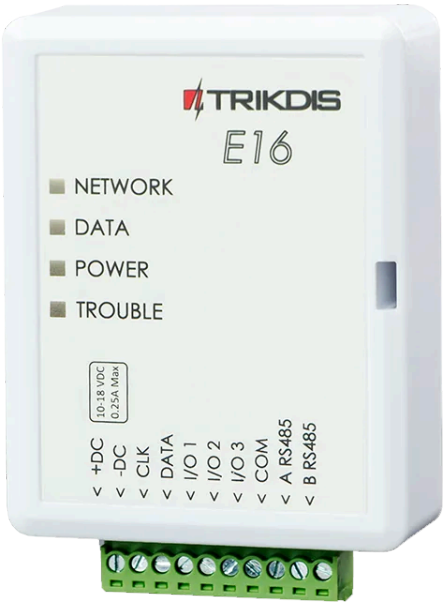
Comunicatore E16 – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente del comunicatore Ethernet Trikdis E16: collegamento al bus dati o alla porta seriale della centrale d'allarme, programmazione della centrale, configurazione di rete in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-e16

Indice

1. Panoramica

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

2. Messa in servizio rapida con TrikdisConfig

2.1 Preparativi
2.2 Modello 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 Fasi dell'installazione
3.2 Posizionamento e rete
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 chiave
3.5 Collegamento degli ingressi
3.6 Collegamento di un'uscita con relè
3.7 Collegamento dell'espansione iO-8
3.8 Collegamento del cavo Ethernet
3.9 Accensione e primo controllo
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 della tastiera

5.3 Inserimento con zona chiave
5.4 Inserimento e disinserimento dall'app

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 Ethernet settings
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

L'E16 è il **comunicatore Ethernet a collegamento diretto** di Trikdis: non si collega all'uscita della linea telefonica della centrale d'allarme, ma al **bus tastiere o alla porta seriale** della centrale. Legge gli eventi direttamente dalla centrale – insieme al numero di zona, di area e di utente – e li inoltra, tramite la rete locale e la connessione Internet cablata, al ricevitore della centrale di vigilanza e al cloud Protegus, cioè all'app dell'utente. Funziona con le centrali DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell e Crow supportate; con i modelli **a controllo diretto** l'utente inserisce e disinserisce dall'app Protegus 2 con il proprio codice della tastiera, senza una zona chiave separata. Per le centrali di altre marche che hanno solo l'uscita della linea telefonica è indicato il comunicatore Ethernet E16T (TIP/RING); dove non c'è Internet cablato, il comunicatore per rete mobile G16.

1.1 A cosa serve e come funziona

- **Legge direttamente la centrale.** Sul bus della centrale ogni evento arriva subito al comunicatore, con la numerazione propria della centrale; non serve configurare il combinatore della centrale e non c'è nemmeno la composizione Contact ID.
- **Trasmette alla centrale di vigilanza.** Invia gli eventi, tramite connessione IP, al ricevitore software o hardware Trikdis (protocollo TRK; i ricevitori Trikdis collaborano con qualsiasi software di vigilanza) oppure a qualsiasi ricevitore universale (SIA DC-09 2007/2012, SUR-GARD TL150). Con un ricevitore SUR-GARD il comunicatore converte in codici SIA i codici Contact ID ricevuti dalla centrale; la tabella di conversione si trova nell'allegato della documentazione in inglese del produttore. Per impostazione predefinita verifica la connessione ogni 30 secondi (l'intervallo è modificabile, paragrafo 6.3) e in caso di guasto passa al canale di riserva; con il canale parallelo gli eventi possono essere inviati contemporaneamente anche a due ricevitori.
- **Avvisa l'utente.** L'app Protegus 2 mostra ciò che è successo con notifiche push, con un segnale acustico dedicato e nell'elenco degli eventi; dall'app l'utente può inserire e disinserire e comandare i dispositivi collegati (illuminazione, cancello, riscaldamento, ventilazione, impianto di irrigazione ecc.). Protegus 2 funziona con le centrali di tutti i produttori supportati dall'E16.
- Funziona **insieme o separatamente** per la centrale di vigilanza e per l'utente: si può usare solo con Protegus 2 (senza centrale di vigilanza), solo con la centrale di vigilanza oppure con entrambe. Se sono configurate entrambe, l'evento viene inviato prima alla centrale di vigilanza e poi all'utente.
- **Non servono scheda SIM né abbonamento mobile.** Il dispositivo usa la connessione Internet già presente nel sito: si collega al router o allo switch con un cavo Ethernet, di fabbrica ottiene l'indirizzo tramite DHCP e stabilisce solo connessioni in uscita, quindi sul router non bisogna aprire porte.
- **Ha ingressi e uscite propri.** Tre morsetti I/O a doppia funzione possono essere usati come ingressi (rivelatore, manomissione) o come uscite comandabili (zona chiave, relè). Con l'espansione iO-8 collegata al bus RS485 si possono aggiungere al sistema altri 8 I/O.

La struttura del sistema è mostrata nella figura seguente: il bus della centrale d'allarme si collega all'E16, l'E16 raggiunge Internet tramite il router e da lì il cloud Protegus e il ricevitore della centrale di vigilanza, mentre l'utente vede il sistema nell'app Protegus 2.

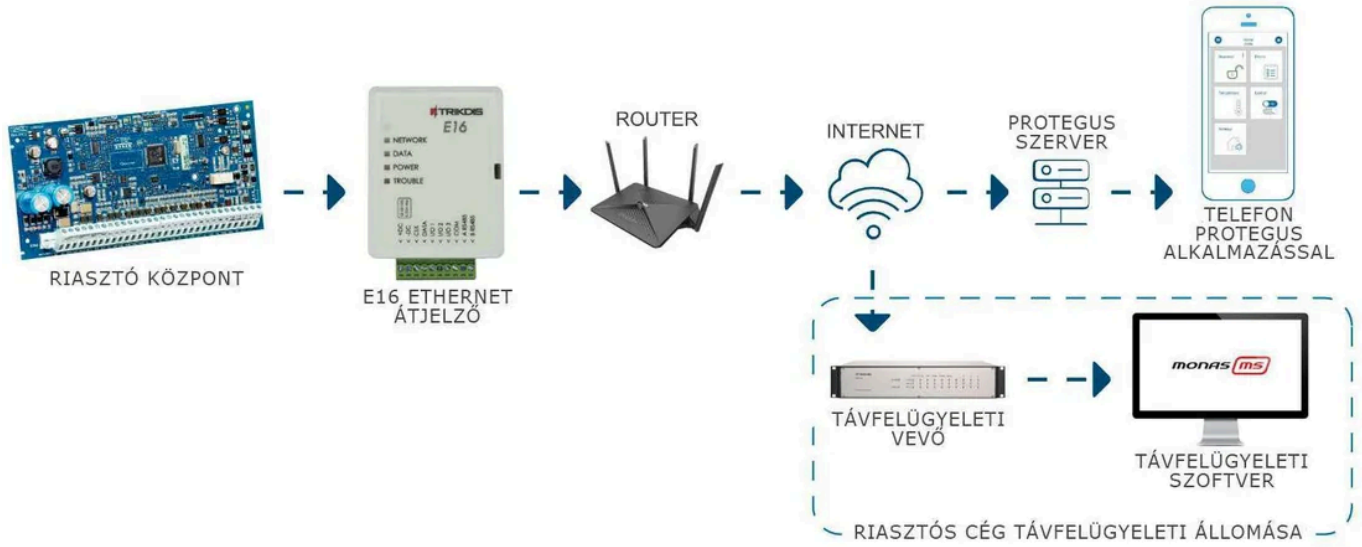


Figura 1. La posizione dell'E16 nel sistema: centrale d'allarme (bus tastiere o porta seriale) → comunicatore Ethernet E16 → router → Internet → cloud Protegus e ricevitore della centrale di vigilanza → il telefono dell'utente con l'app Protegus 2 e il software di vigilanza dell'azienda di sicurezza.

1.2 Centrali d'allarme compatibili

L'E16 può essere collegato alle centrali seguenti. Con i modelli **a controllo diretto** l'inserimento e il disinserimento avvengono dall'app con il codice della tastiera; con gli altri tramite una zona 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 va 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

Oltre a queste, può essere usato anche con le centrali **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 e MATRIX 816** e con le centrali **Paradox DIGIPLEX NE96 ed EVO96**.

L'elenco cambia di tanto in tanto; lo stato più aggiornato si trova nel motore di ricerca della compatibilità. L'E16 non funziona con le centrali **DSC PowerSeries NEO**: al bus della NEO il produttore non consente dispositivi esterni, vedi DSC Power Series NEO e comunicatori Trikdis: compatibilità e soluzioni.

1.3 Caratteristiche principali

Collegamento alla centrale d'allarme

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

Connessione di rete

- Connessione Ethernet (IEEE 802.3, 10Base-T, RJ45) alla rete locale; di fabbrica l'indirizzo è ottenuto tramite DHCP, ma si può impostare anche un indirizzo IP fisso.
- Stabilisce solo connessioni in uscita verso il ricevitore e il cloud Protegus: non bisogna aprire porte e non servono né un indirizzo IP pubblico né una scheda SIM.

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 principale, di riserva e parallelo, ognuno con il proprio ricevitore di riserva; con il canale parallelo gli eventi vanno contemporaneamente a due ricevitori.
- Messaggi cifrati (AES-128); memoria eventi di 60 messaggi.

Funzioni per l'utente

- App mobile e web Protegus 2: notifiche, elenco degli eventi, inserimento e disinserimento, comando delle uscite.
- Diritti utente su più livelli nell'app (amministratore, installatore, utente).

Installazione e configurazione

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

1.4 Le parti del comunicatore

L'E16 ha il circuito stampato in una scatola di plastica bianca; il coperchio frontale è rimovibile e la morsettiera è estraibile. Il connettore Ethernet si trova sul circuito stampato e il cavo entra attraverso l'apertura della scatola.

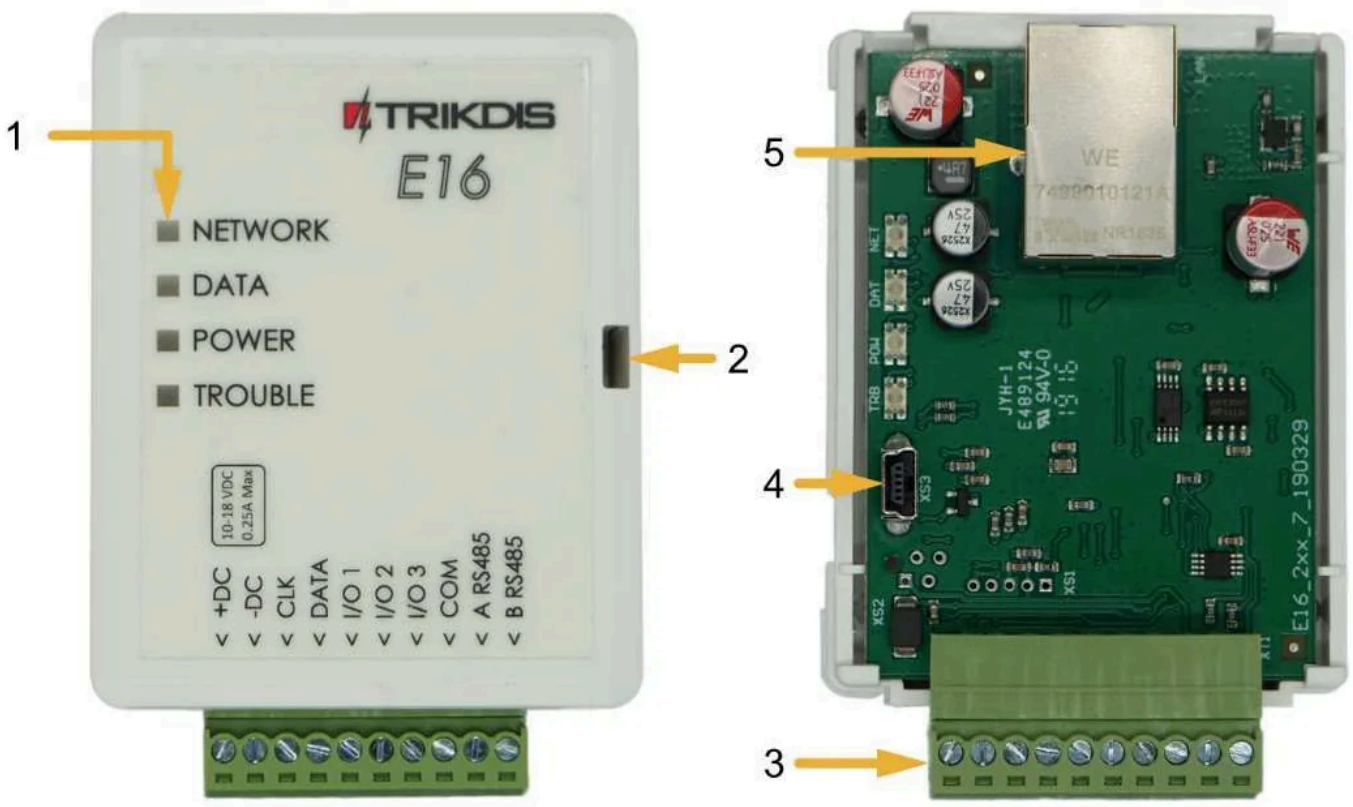


Figura 2. Le parti dell'E16 viste di fronte e con la scatola aperta.

- 1 LED di segnalazione (NETWORK, DATA, POWER, TROUBLE)
- 2 Apertura per facilitare la rimozione del coperchio frontale
- 3 Morsettiera estraibile
- 4 Presa USB Mini-B per la programmazione
- 5 Connettore Ethernet (RJ45)

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

1.5 Morsetti

Morsetto	Funzione
+DC	Alimentazione, +10–18 V DC
–DC	Alimentazione, negativo
CLK	Linea di clock / seriale del bus della centrale

Morsetto	Funzione
DATA	Linea dati del bus della centrale
I/O 1	Ingresso/uscita 1 (impostazione di fabbrica: ingresso, NO)
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 RS485	Filo A del bus RS485
B RS485	Filo B del bus RS485

Le indicazioni dei morsetti sono riportate anche sul coperchio frontale, quindi durante il cablaggio non è necessario togliere il coperchio. A quale morsetto della centrale vanno CLK e DATA cambia da produttore a produttore – gli schemi di collegamento si trovano nel paragrafo 3.3.

1.6 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 connessione di rete, DATA il traffico, TROUBLE il guasto.

NETWORK – connessione di rete

Segnalazione	Significato
spento	Nessuna connessione alla rete (manca il cavo, il router o l'indirizzo IP – il LED TROUBLE indica quale)
verde fisso	Connesso alla rete

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 di dati in corso (durante la programmazione)

Controllo rapido

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

POWER – tensione di alimentazione

Segnalazione	Significato
spento	Nessuna alimentazione, oppure l'alimentazione è scollegata

Segnalazione	Significato
verde fisso	Acceso, la tensione di alimentazione è adeguata
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	Nessun collegamento fisico alla rete (PHY link): il cavo non è inserito, oppure la porta del router / dello switch non è attiva
2 lampeggi rossi	Errore DHCP: il dispositivo non ha ottenuto un indirizzo IP
3 lampeggi rossi	Errore DNS: non riesce a risolvere il nome di dominio del ricevitore o del cloud Protegus
6 lampeggi rossi	Nessuna connessione con il ricevitore della centrale di vigilanza e/o con il server Protegus (la causa può essere anche la connessione Internet o il firewall)
7 lampeggi rossi	Collegamento con la centrale d'allarme interrotto (collegamento bus o seriale)
rosso lampeggiante (durante la programmazione)	Errore di memoria
rosso fisso (durante la programmazione)	Firmware danneggiato

1.7 Dati tecnici

Parametro	Valore
Collegamento alla centrale d'allarme	bus tastiere o porta seriale, a seconda del modello di centrale (4 fili: +DC, −DC, CLK, DATA)
Connessione di rete	Ethernet, IEEE 802.3, 10Base-T, presa RJ45
Configurazione di rete	DHCP (di fabbrica) o indirizzo IP fisso, subnet mask, gateway, DNS
Ingressi/uscite	3 I/O a doppia funzione: come ingresso NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistenza di fine linea 2,2 kΩ); come uscita a collettore aperto (OC), max. 0,15 A / 30 V DC
Espansione	sul bus RS485 al massimo 4 espansioni iO-8 (+8 I/O per espansione)
Tensione di alimentazione	10–18 V DC
Assorbimento	100 mA nominali (a riposo); al massimo 250 mA durante l'invio
Protocolli di trasmissione	TRK, DC-09_2007, DC-09_2012, TL150
Cifratura dei messaggi	AES-128
Memoria eventi	60 messaggi
Programmazione	TrikdisConfig (Windows) con cavo USB Mini-B o a distanza
Ambiente di funzionamento	−10 … +50 °C, max. 80 % di umidità relativa (a +20 °C)

Parametro	Valore
Dimensioni	88 × 65 × 26 mm
Peso	80 g

2. Messa in servizio rapida con TrikdisConfig

Tutte le impostazioni dell'E16 si fanno con il programma per Windows **TrikdisConfig** – tramite cavo USB o a distanza. In questo capitolo descriviamo la via più breve: configuri il dispositivo sul tavolo, prima del cablaggio, e poi sul posto resta solo da collegarlo. La spiegazione dettagliata delle impostazioni si trova nel capitolo 6.

2.1 Preparativi

Che cosa ti serve

Cavo USB Mini-B · cavo con almeno 4 conduttori 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 · cavo Ethernet (CAT-5 o superiore, al massimo 100 m) fino al router o allo switch · il manuale d'installazione della centrale d'allarme. I cavi e gli accessori vanno acquistati separatamente dal distributore.

1. Scarica e installa il software 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 dell'E16. 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.

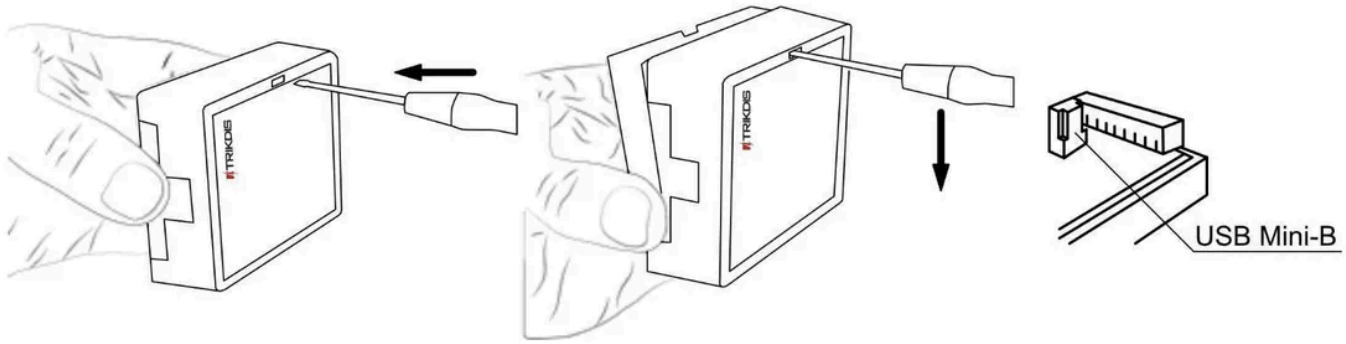


Figura 3. Sgancio del coperchio frontale con un cacciavite piatto (a sinistra, al centro) e posizione della presa USB Mini-B sul circuito stampato (a destra).

3. Collega l'E16 al computer con un cavo USB Mini-B. L'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

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

2.2 Modello di centrale e controllo diretto

Qualunque modalità tu usi, indica prima nella pagina **System settings** a quale centrale verrà collegato il comunicatore.

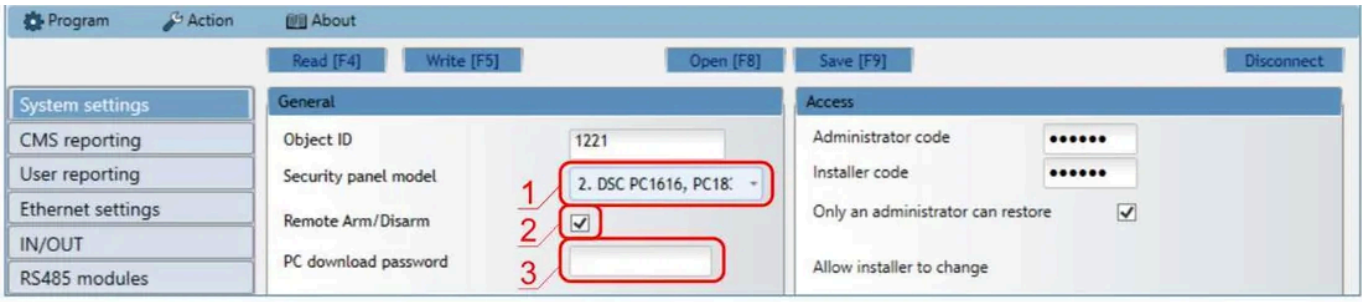


Figura 4. TrikdisConfig – pagina System settings, gruppo General.

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

Con diverse centrali serve un'impostazione anche nella centrale: 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 produttore 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 5. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- 4 **Enable connection** – spunta la casella: abilita la connessione con il cloud Protegus.
- 5 **Protegus Cloud access code** – cambia la password di fabbrica `123456`. Questa dovrà essere inserita nell'app quando crei il sistema; **dopo la creazione del sistema non può più essere modificata.**

Per le impostazioni di rete, nella pagina **Ethernet settings** di fabbrica è spuntato **Use DHCP**: il dispositivo ottiene automaticamente un indirizzo IP dal router e nella maggior parte dei casi non c'è altro da fare. Se nella rete non c'è un DHCP, o bisogna usare un indirizzo fisso, inserisci qui le impostazioni manuali (paragrafo 6.5).

L'E16 stabilisce solo connessioni **in uscita** verso il cloud Protegus e il ricevitore, quindi sul router non bisogna aprire né inoltrare porte. In una rete aziendale filtrata da un firewall, concorda il traffico in uscita con l'amministratore di rete (paragrafo 3.2).

Se il dispositivo funziona solo con Protegus 2, senza centrale di vigilanza, la configurazione è finita: premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB. Se trasmette anche alla centrale di vigilanza, prosegui con il paragrafo 2.4.

2.4 Collegamento alla centrale di vigilanza

Se il dispositivo trasmette anche al ricevitore di una centrale di vigilanza, nella pagina **System settings** inserisci anche il codice d'impianto.

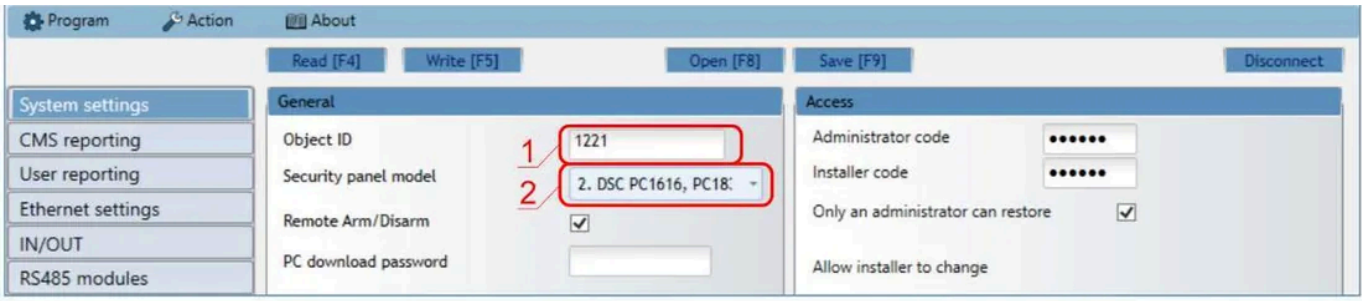


Figura 6. TrikdisConfig – pagina System settings, gruppo General.

- 1 **Object ID** – il codice d'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 modello 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 principale), imposta i dati del ricevitore.

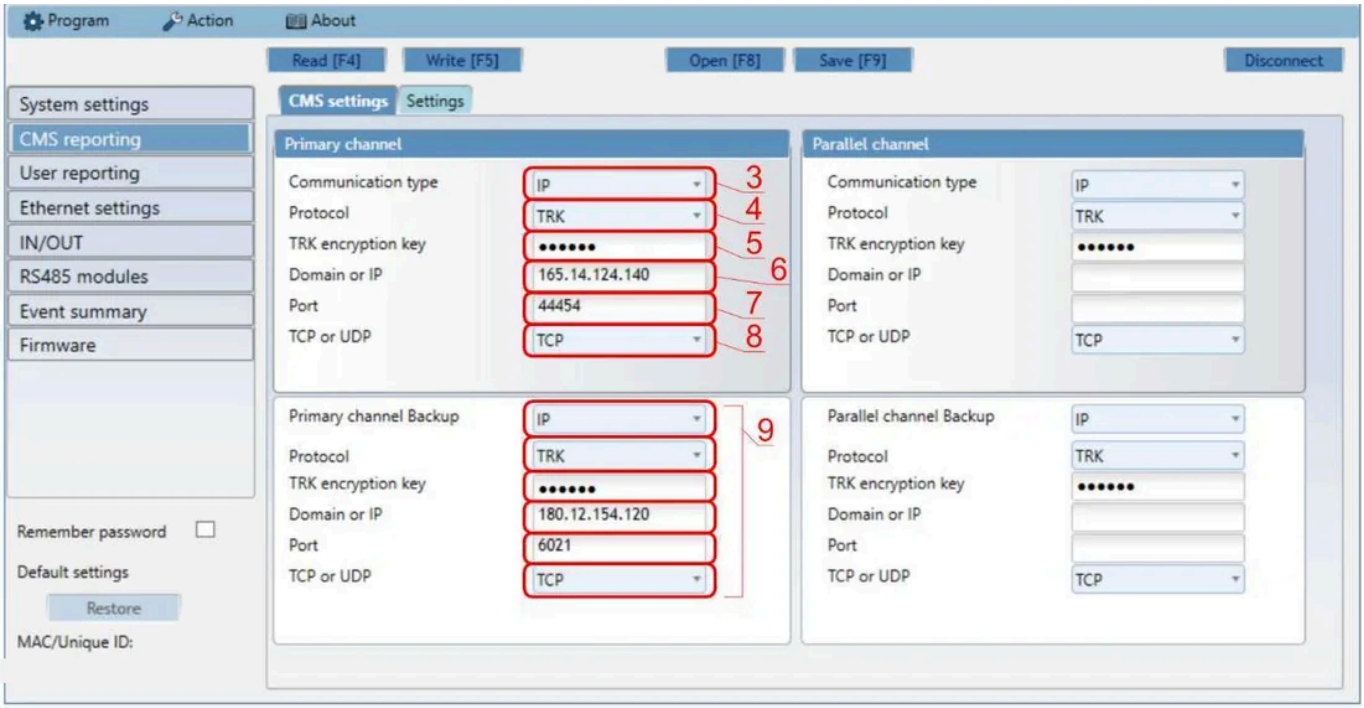


Figura 7. TrikdisConfig – CMS reporting, scheda CMS settings.

- 3 **Communication type** – **IP** (con l'E16 è l'unica possibilità).
- 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 cifratura a 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 canale principale; compilalo allo stesso modo, è consigliabile impostarlo.

È consigliabile impostare anche il **Parallel channel** (canale parallelo) e il relativo canale di riserva, se gli eventi devono arrivare a due ricevitori.

Con il protocollo **DC-09**, nella scheda **Settings** inserisci anche il numero d'impianto, di linea e di ricevitore DC-09. Se indichi il ricevitore con un nome di dominio, nella pagina **Ethernet settings** deve esserci un indirizzo DNS funzionante (di fabbrica il server dei nomi pubblico di Google).

Al termine delle impostazioni premi il pulsante **Write [F5]** (scrittura), attendi la conferma e scollega il cavo USB. A questo punto il dispositivo è pronto per il cablaggio.

3. Installazione e collegamento

Figyelem!

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

3.1 Fasi dell'installazione

1. Togli il coperchio frontale (vedi il paragrafo 2.1) ed estrai la morsettiera.
2. Estrai il circuito stampato dalla base: apri il fermo nell'angolo.
3. Fissa la base con le viti nel punto scelto.

4. Rimetti il circuito stampato nella base e reinserisci la morsettiera.
5. Inserisci il cavo Ethernet nella presa RJ45 (paragrafo 3.8).
6. Rimetti il coperchio frontale.

3.2 Posizionamento e rete

- Monta il comunicatore in un luogo **asciutto, al chiuso**, possibilmente vicino al contenitore della centrale d'allarme, in modo che il cavo del bus sia corto. Un contenitore metallico non lo disturba: l'E16 non ha antenna.
- Il cavo Ethernet (CAT-5 o superiore) fino al router o allo switch può essere lungo **al massimo 100 m**.
- Tieni il comunicatore e i cavi lontani dal trasformatore della centrale e dai cavi della rete elettrica.

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.

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

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

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

Interruzione di corrente

L'E16 è alimentato dalla centrale d'allarme, quindi durante un'interruzione di corrente continua a funzionare con la batteria della centrale – il router e il modem invece di solito no, e senza di loro non c'è Internet. Se per il sistema questo non è accettabile, alimenta anche i dispositivi di rete con un gruppo di continuità (UPS), oppure scegli un comunicatore per rete mobile (G16).

3.3 Collegamento alla centrale d'allarme

L'E16 si collega alla centrale con **al massimo quattro fili** (sul bus Caddx e Pyronix il CLK non è usato): ai morsetti **+DC** e **–DC** va l'alimentazione ausiliaria a 12 V (AUX) della centrale, ai morsetti **CLK** e **DATA** i due fili dati del bus tastiere o della porta seriale della centrale. Quale morsetto della centrale sia quale cambia da produttore a produttore – collega secondo gli schemi seguenti. Per le centrali con porta seriale (Paradox, Texecom) è disponibile un cavo originale, con un'estremità che si inserisce nel connettore della centrale e l'altra che si collega alla morsettiera dell'E16.

Durante l'invio l'E16 può assorbire fino a 250 mA. Verifica che l'uscita AUX della centrale lo sopporti insieme agli altri dispositivi collegati. Poiché l'alimentazione è fornita dalla centrale, durante un'interruzione di corrente la batteria della centrale alimenta anche il comunicatore. La maggior parte delle centrali non viene

danneggiata dall'inversione dei fili di un dispositivo collegato al bus, ma l'inversione di **+DC e −DC** può distruggere il comunicatore – controlla la polarità prima del collegamento.

Dopo il collegamento, nel campo **System settings** → **Security panel model** di TrikdisConfig va selezionato il modello 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.

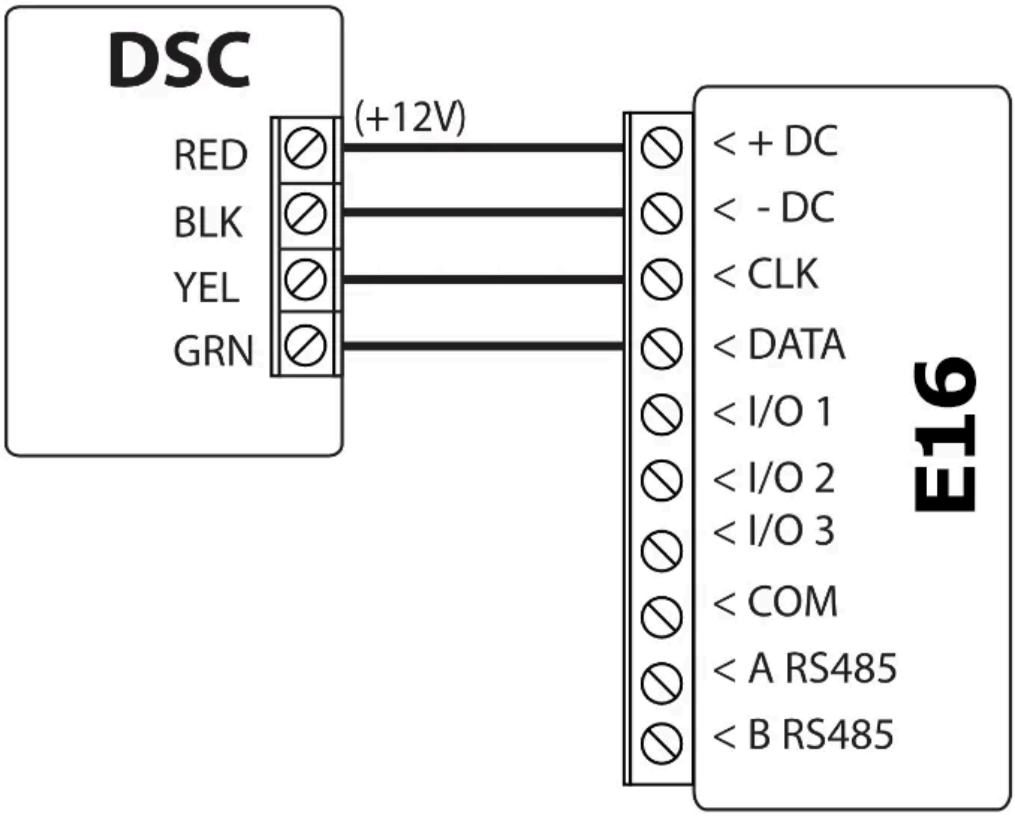


Figura 8. Collegamento al Keybus (bus tastiere, «Keypad bus») di una centrale DSC PowerSeries: RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

Il comunicatore si collega alla **porta seriale** (SERIAL) delle centrali Paradox con il cavo originale **CRP2** o **CRP2B**; l'estremità del cavo lato centrale si inserisce nel connettore seriale, l'altra estremità la colleghi alla morsettiera dell'E16. 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 l'assegnazione dei colori di entrambi i cavi. Le indicazioni del connettore seriale Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

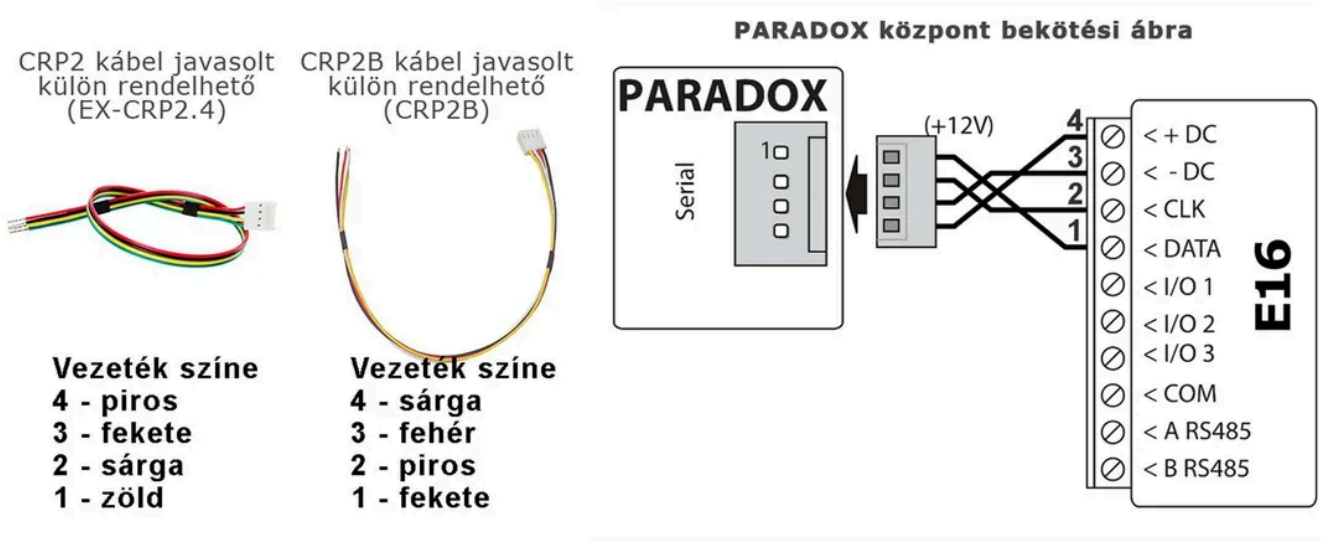


Figura 9. Collegamento alla porta seriale di una centrale Paradox con cavo CRP2 (EX-CRP2.4) o CRP2B. CRP2: 4 rosso → +DC, 3 nero → −DC, 2 giallo → CLK, 1 verde → DATA. CRP2B: 4 giallo → +DC, 3 bianco → −DC, 2 rosso → CLK, 1 nero → DATA.

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 sulle centrali d'allarme Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

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

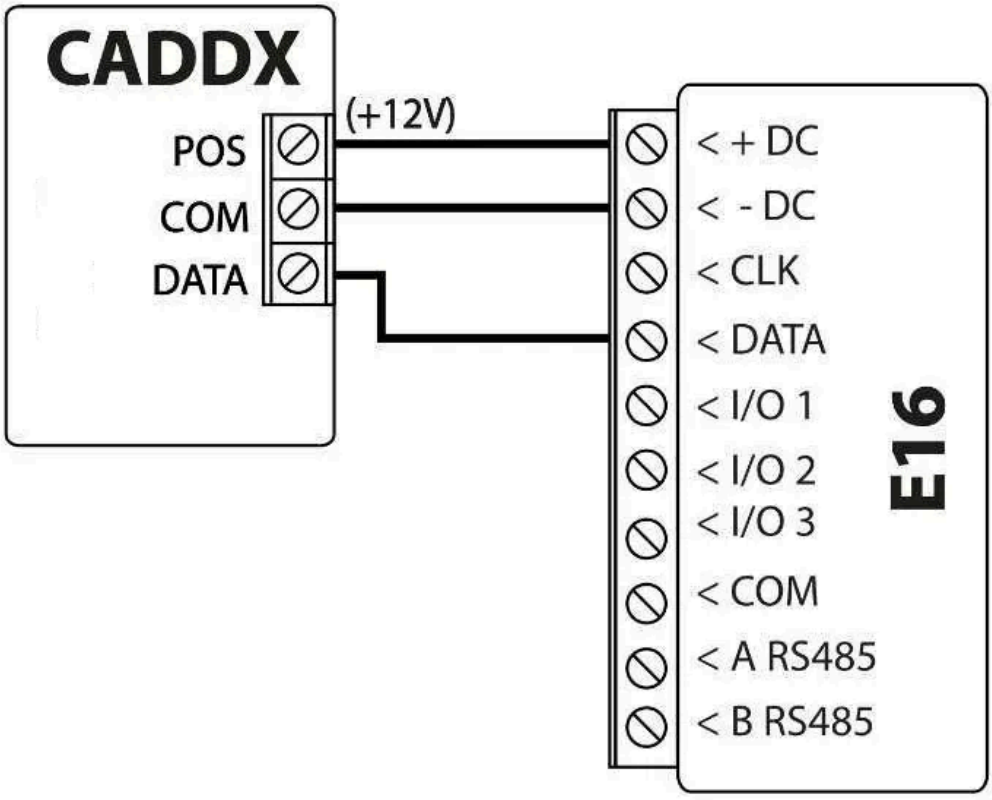


Figura 10. Collegamento al bus tastiere («Keypad bus») di una centrale Caddx NetworX: POS → +DC (+12 V), COM → −DC, DATA → DATA; il CLK resta libero.

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.

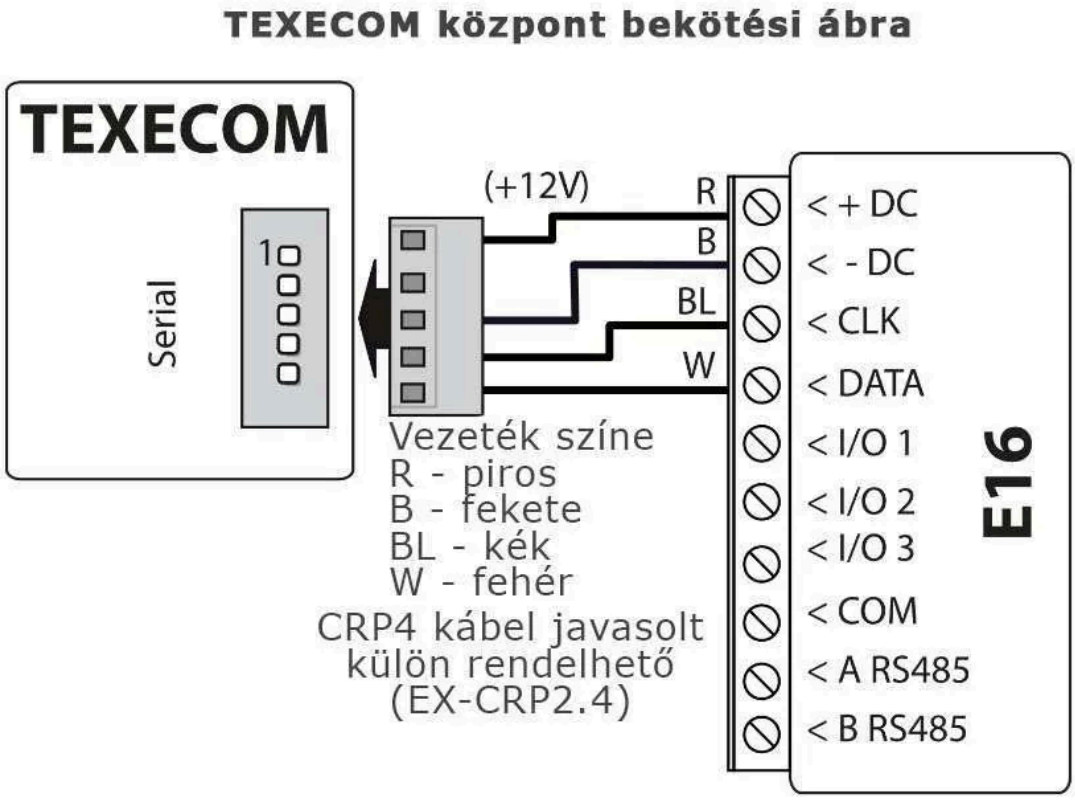


Figura 11. Collegamento alla porta seriale di una centrale Texecom con cavo CRP4: rosso → +DC, nero → −DC, blu → CLK, bianco → DATA.

3.3.5 Crow Runner

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

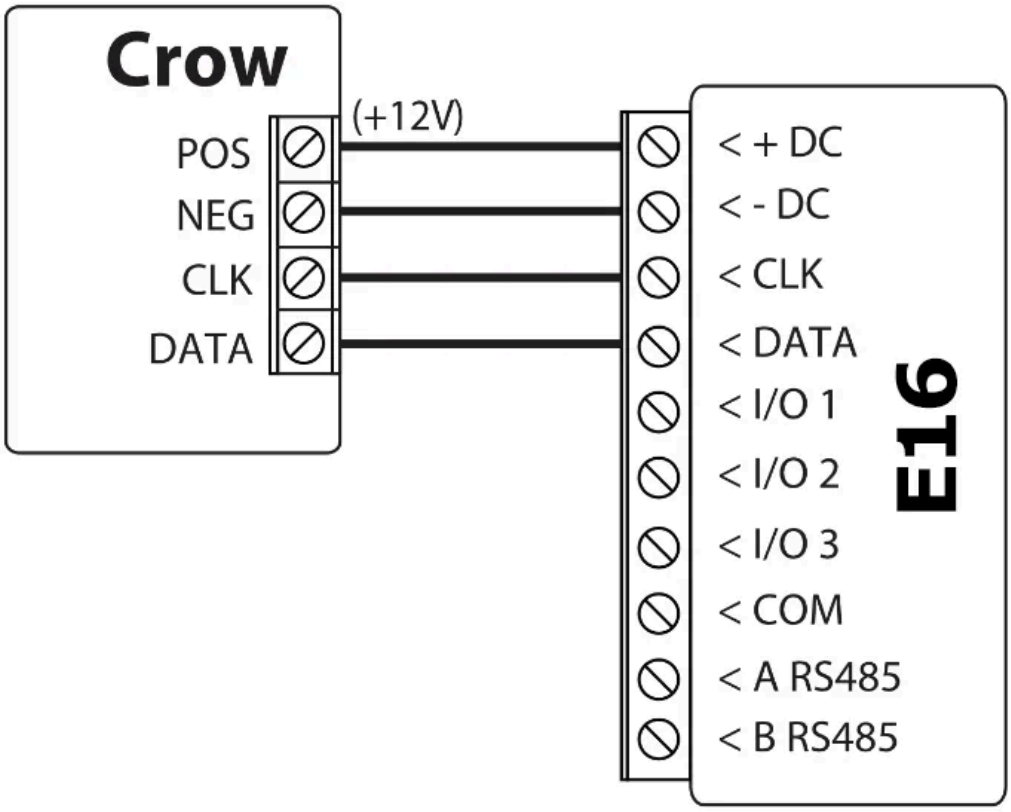


Figura 12. Collegamento al bus tastiere («Keypad bus») di una centrale Crow Runner 4/8 e Runner 8/16: POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Il bus tastiere 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 tastiere 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.

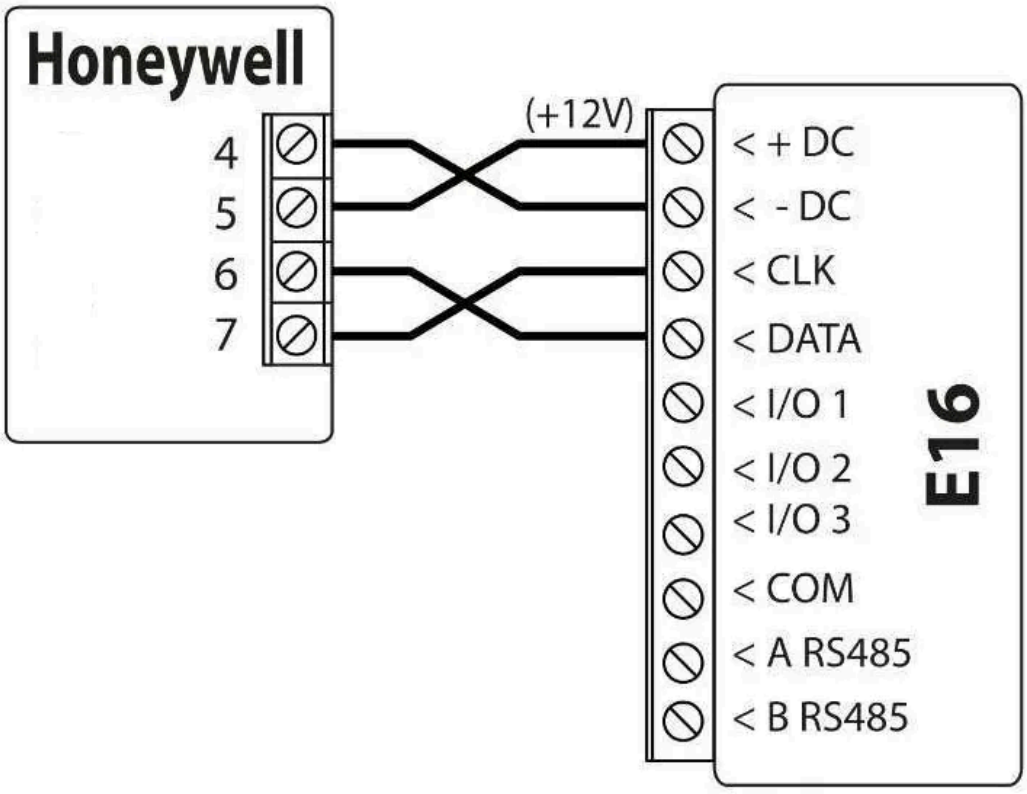


Figura 13. Collegamento al bus tastiere («Keypad bus») di una centrale Honeywell Vista-20 / Vista-48: 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

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 va abilitato l'uso della porta seriale (paragrafo 4.7).

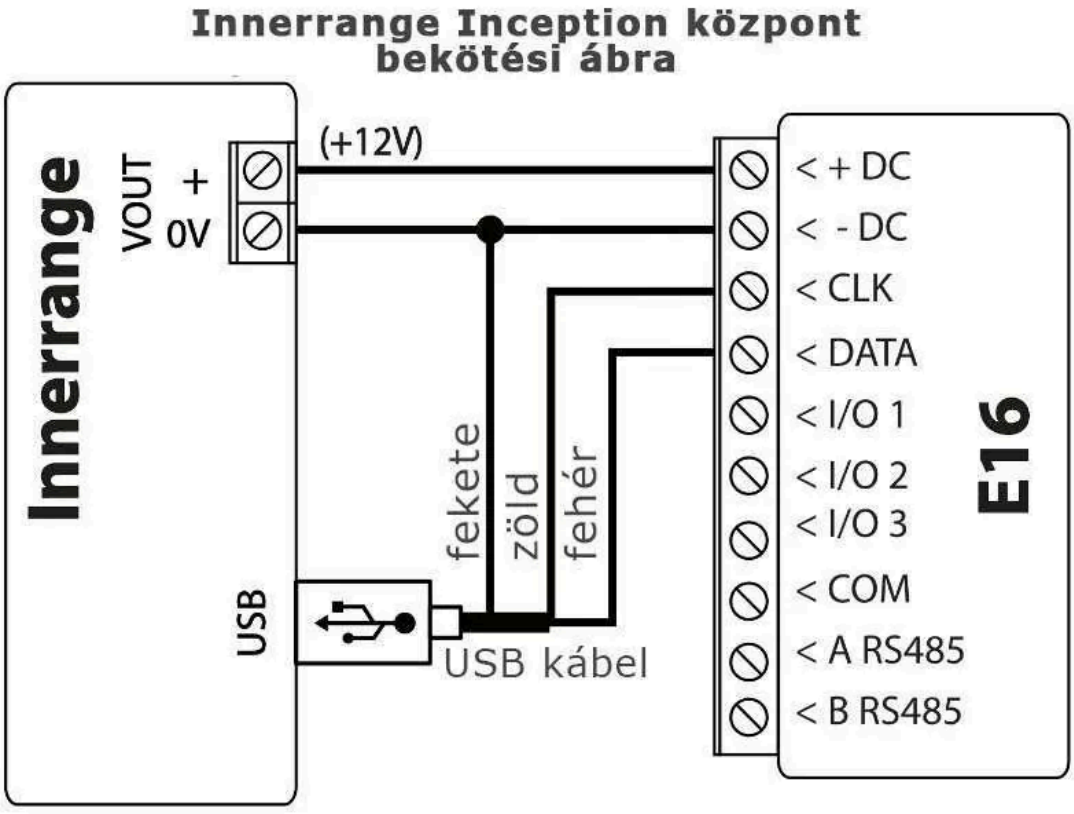


Figura 14. Collegamento a una centrale InnerRange Inception: alimentazione dai morsetti VOUT + e 0V, dati dalla porta USB con il cavo 993030USB (nero → 0V, verde → CLK, bianco → DATA).

Alla porta 0 (Port 0) della centrale **Integriti** il comunicatore si collega con il cavo INTG-996795: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA. La porta seriale della centrale va impostata sul protocollo Trikdis (paragrafo 4.7).

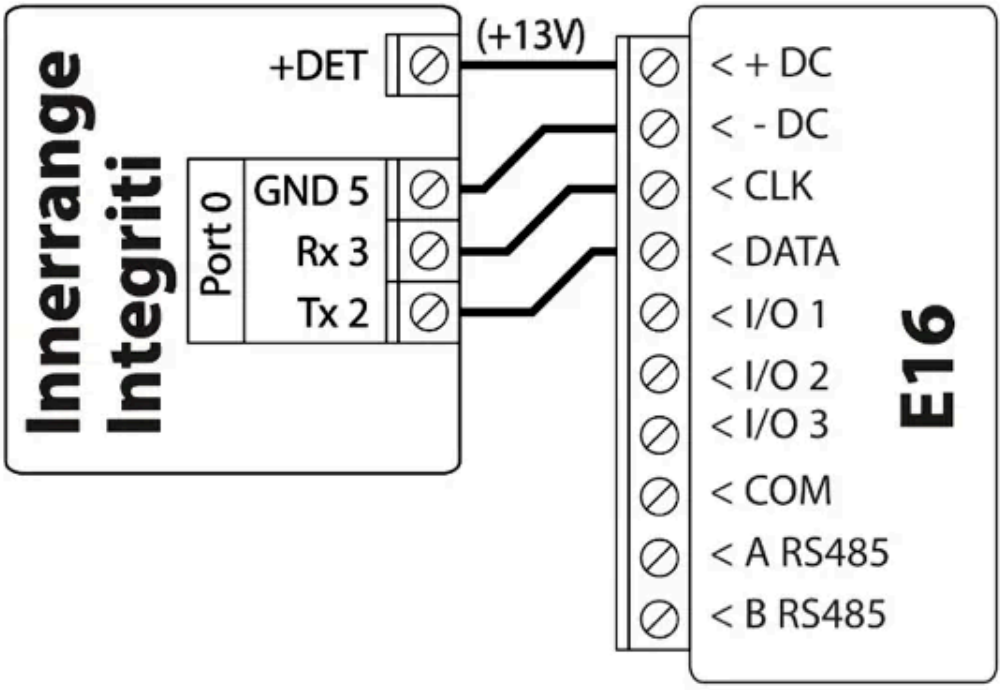


Figura 15. Collegamento a una centrale InnerRange Integriti con il cavo Inner Range codice INTG-996795: +DET (+13 V) → +DC, Port 0 GND (5) → −DC, Rx (3) → CLK, Tx (2) → DATA.

3.4 Collegamento della zona chiave

Se la centrale non rientra tra i modelli a controllo diretto, o non vuoi usare il controllo diretto, l'inserimento e il disinserimento a distanza si realizzano con una **zona chiave**: imposti uno dei morsetti I/O del comunicatore come **uscita** (pagina IN/OUT, paragrafo 6.6) e lo colleghi a una zona chiave della centrale. All'attivazione l'uscita porta la zona su COM (negativo); collega la resistenza di fine linea della zona secondo il tipo di zona della centrale. Poiché l'E16 ha tre morsetti I/O, si possono gestire fino a tre aree con uscite separate.

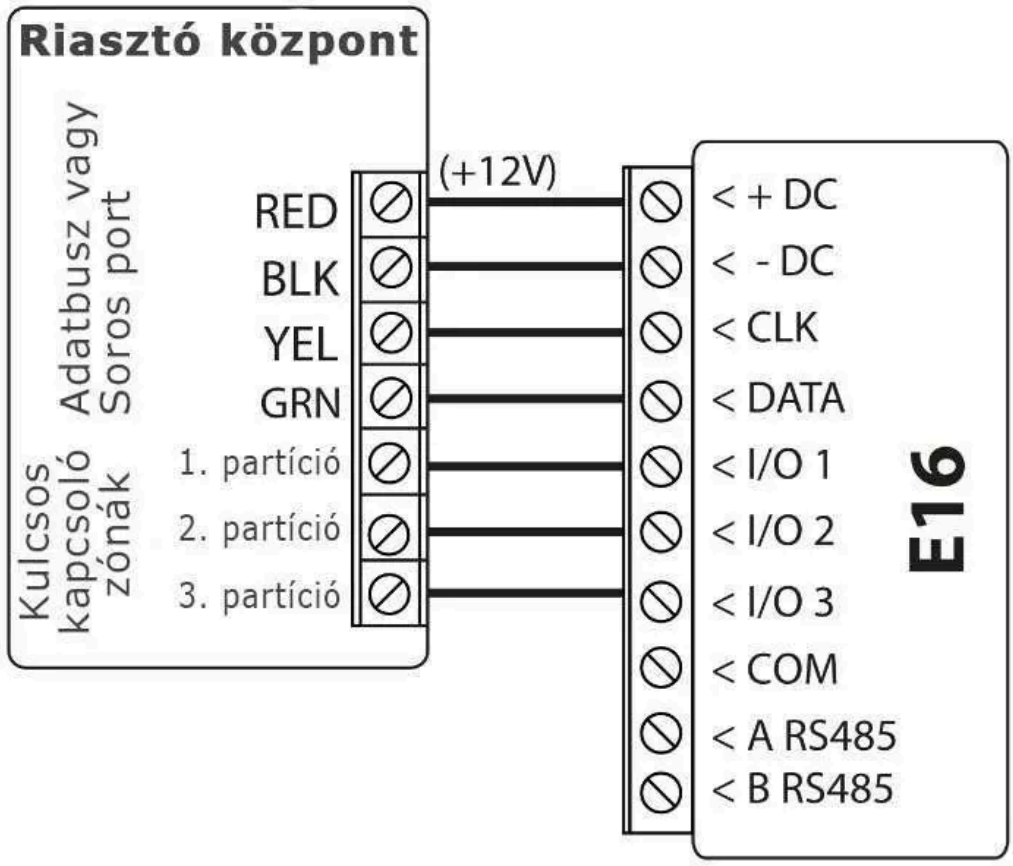


Figura 16. Inserimento e disinserimento con zona chiave: il comunicatore legge gli eventi dal bus della centrale, mentre le uscite I/O 1–3 comandano la zona chiave delle aree 1–3 della centrale.

- Nella pagina **System settings** di TrikdisConfig, **Remote Arm/Disarm** deve restare **vuoto** – le due cose non possono essere usate contemporaneamente.
- La zona chiave può essere a impulso o bistabile; nell'app Protegus 2 va impostata la stessa modalità (paragrafo 5.3).

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

3.5 Collegamento degli ingressi

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

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

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

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

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

Collegamento dei circuiti d'ingresso: tipi NO, NC, NC/EOL, NO/EOL, NO/DEOL e NC/DEOL con resistenza di fine linea da 2,2 kΩ; con i tipi DEOL è collegato anche il circuito antimanomissione.

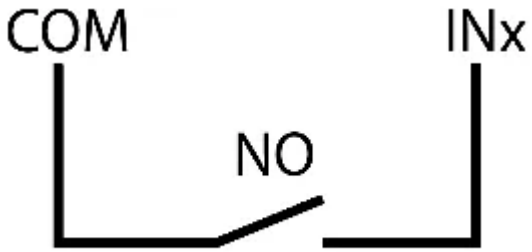


Figura 17. NO – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

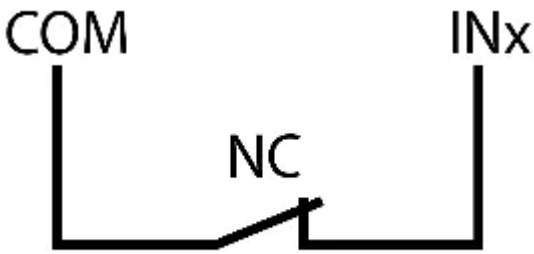


Figura 18. NC – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

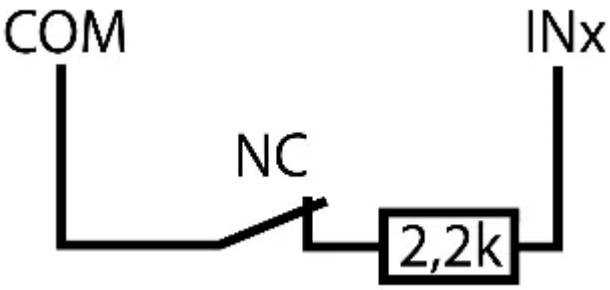


Figura 19. NC/EOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

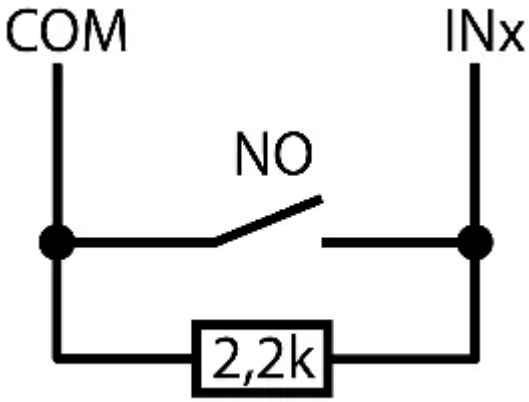


Figura 20. NO/EOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

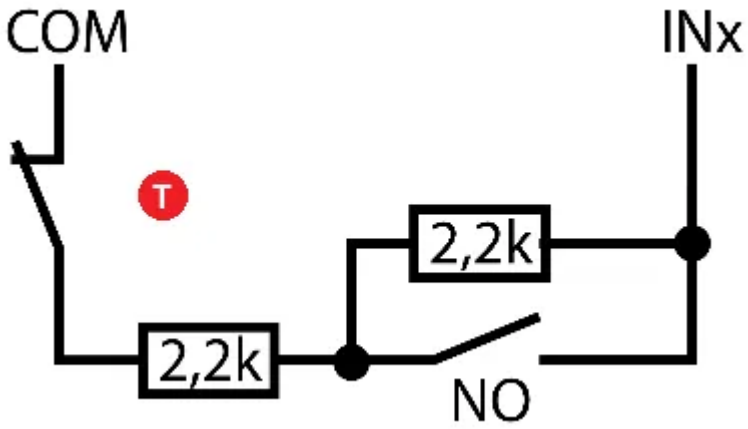


Figura 21. NO/DEOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

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

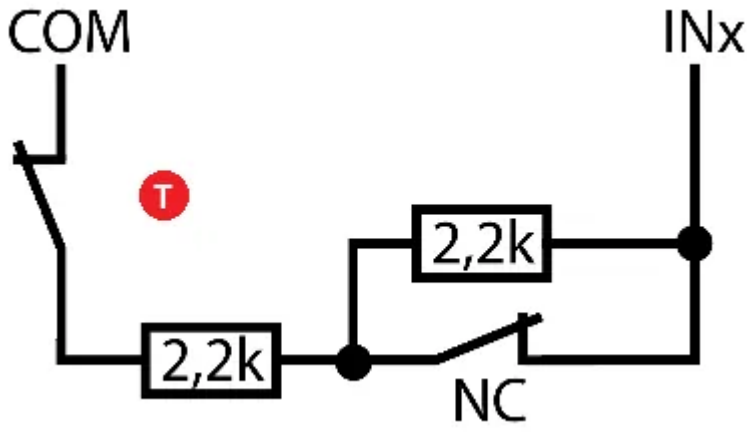


Figura 22. NC/DEOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

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

3.6 Collegamento di un'uscita con relè

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

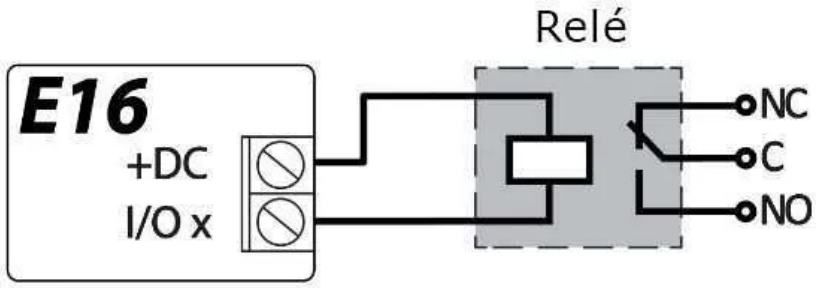


Figura 23. Collegamento di un relè all'uscita del comunicatore: la bobina va tra il morsetto +DC e il morsetto I/O x, i contatti (NC, C, NO) comandano il carico.

Le uscite possono essere comandate dall'app Protegus 2 (capitolo 5).

3.7 Collegamento dell'espansione iO-8

Se servono più ingressi o uscite, al bus RS485 dell'E16 si può collegare l'espansione **iO-8**; ognuna aggiunge 8 I/O a doppia funzione. Collega i morsetti A RS485 e B RS485 ai morsetti A e B del modulo e prendi l'alimentazione del modulo dall'uscita AUX a 12 V della centrale. Il modulo va aggiunto nella pagina **RS485 modules** di TrikdisConfig (paragrafo 6.7); gli eventi degli ingressi vanno alla centrale di vigilanza e a Protegus 2, e le uscite possono essere comandate dall'app.

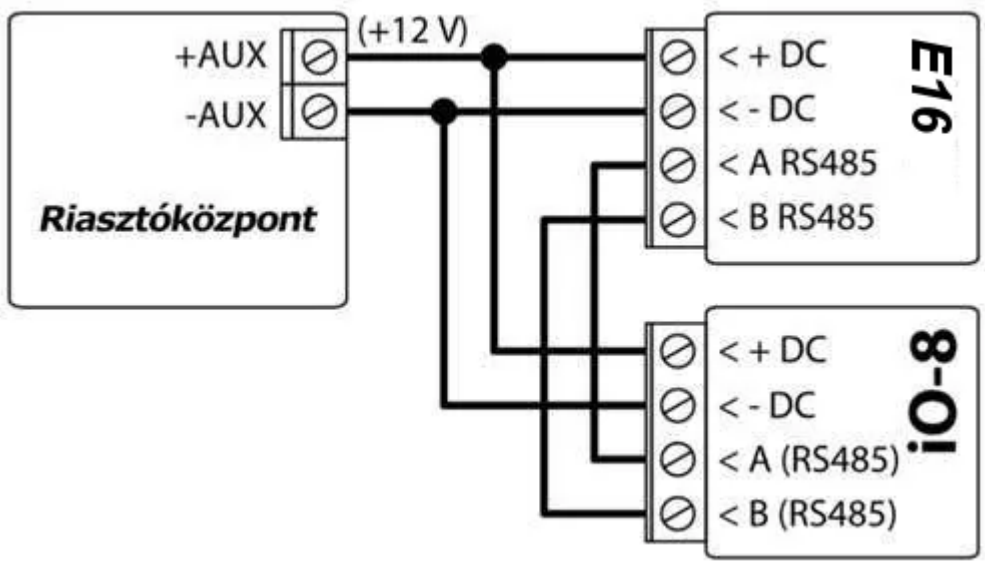


Figura 24. Collegamento dell'espansione iO-8 al bus RS485 dell'E16 (A RS485 → A, B RS485 → B); entrambi i dispositivi sono alimentati dall'uscita AUX della centrale d'allarme (+12 V).

3.8 Collegamento del cavo Ethernet

Inserisci un'estremità del cavo Ethernet nella presa RJ45 sul circuito stampato dell'E16 e l'altra in una porta libera del router o dello switch. Serve un normale cavo dritto (patch); il cavo entra attraverso l'apertura della scatola. Dopo l'accensione, l'avvenuta connessione alla rete è indicata dalla luce verde del LED **NETWORK**.

3.9 Accensione e primo controllo

A TRIKDIS átjelző elindítása

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

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

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

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

- **POWER** verde fisso – l'alimentazione è adeguata;
- **NETWORK** verde fisso – connesso alla rete;
- **TROUBLE** spento.

Qualsiasi altro stato dei LED indica un guasto; identificane la causa in base alla tabella dei LED del paragrafo 1.6. Se TROUBLE lampeggia, il numero di lampeggi indica la causa (paragrafo 1.6): 1 = nessun collegamento fisico (cavo, porta), 2 = non ha ottenuto un indirizzo IP (DHCP), 3 = errore DNS, 6 = non raggiunge il ricevitore o il cloud Protegus. **7 lampeggi** indicano la mancanza di collegamento con la centrale: controlla i fili CLK e DATA, il modello di centrale selezionato e – dove serve – la programmazione della centrale (capitolo 4). Se nessun LED è acceso, controlla l'alimentazione e il cablaggio.

4. Programmazione della centrale d'allarme

Questo capitolo descrive, produttore per produttore, che cosa va impostato nella centrale d'allarme affinché l'E16 legga gli eventi e – dove possibile – comandi la centrale a distanza. Con la maggior parte delle centrali non bisogna programmare nulla per la lettura degli eventi; 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 comandi la centrale non direttamente ma tramite una zona chiave (paragrafo 3.4), **Remote Arm/Disarm** deve restare vuoto, e questo capitolo riguarda solo le impostazioni necessarie alla 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
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 chiave (paragrafi 1.2 e 3.4).

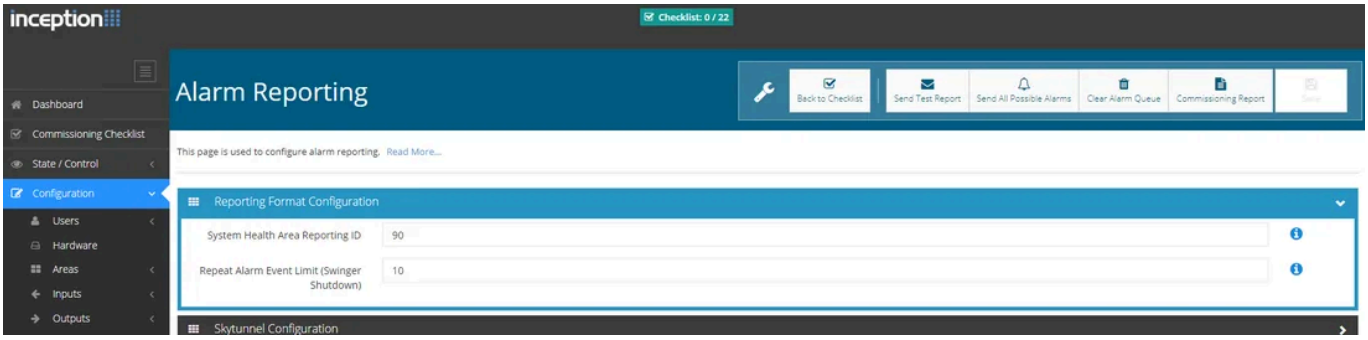


Figura 25. Interfaccia web Inception – Configuration → General → Alarm Reporting.



Figura 26. 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 l'E16 l'inserimento può avvenire in due modi: con le centrali **a controllo diretto** l'utente usa il proprio **codice della tastiera**, con le centrali collegate tramite zona chiave si usa l'**uscita** del comunicatore.

5.1 Aggiunta del dispositivo

Prima di aggiungere il dispositivo verifica che:

1. L'E16 sia collegato alla rete e raggiunga Internet: il LED **NETWORK** è verde fisso, il LED **TROUBLE** non lampeggia.
2. Nella pagina **User reporting** → **PROTEGUS Cloud** di TrikdisConfig sia spuntato **Enable connection** e sia impostato il **Protegus Cloud access code** (dopo la creazione del sistema non può più essere modificato).
3. Il LED **POWER** sia verde fisso.

Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un

rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

A rendszer létrehozása a Protegus 2 alkalmazásban

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

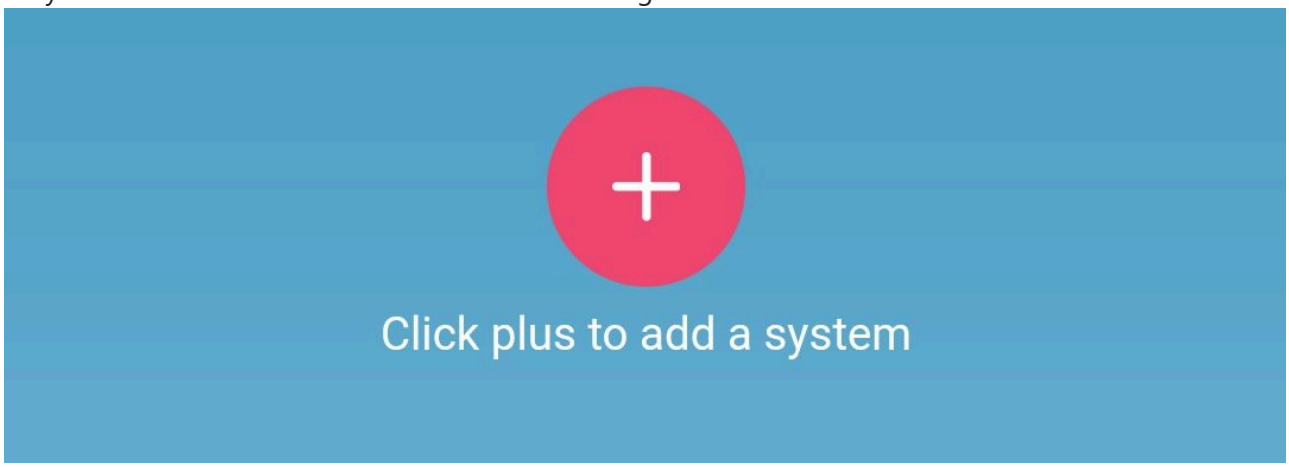
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

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

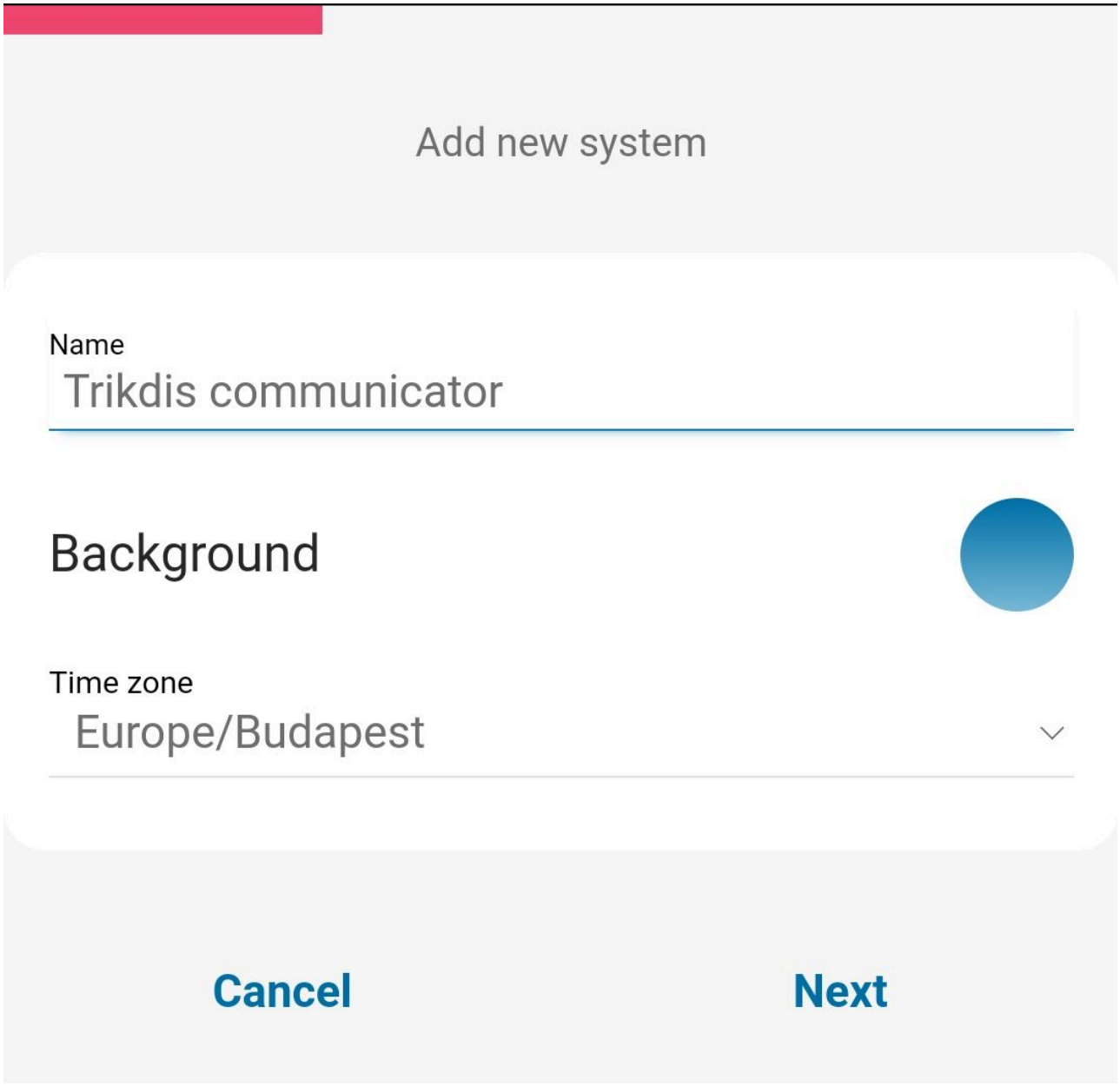


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

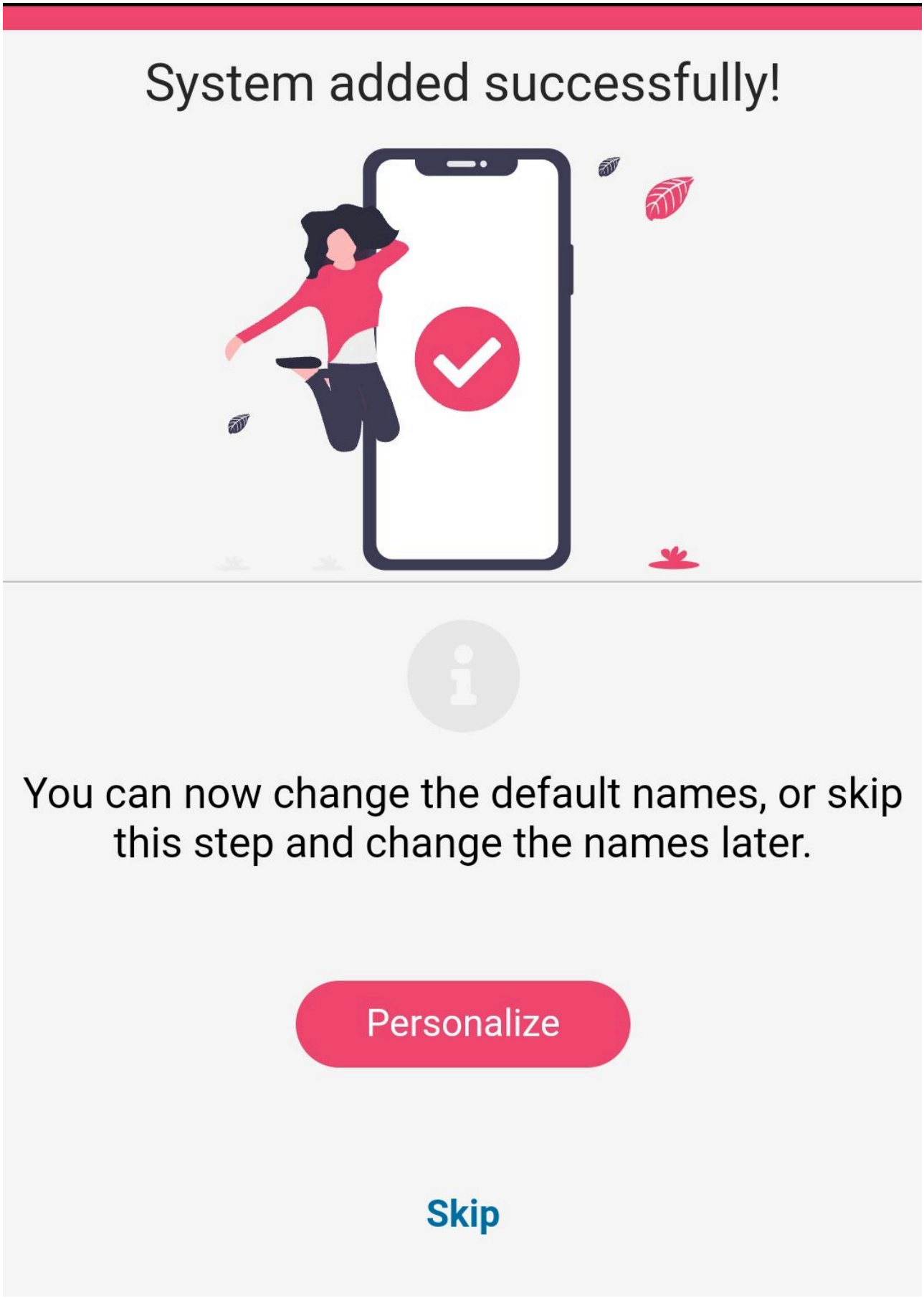
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



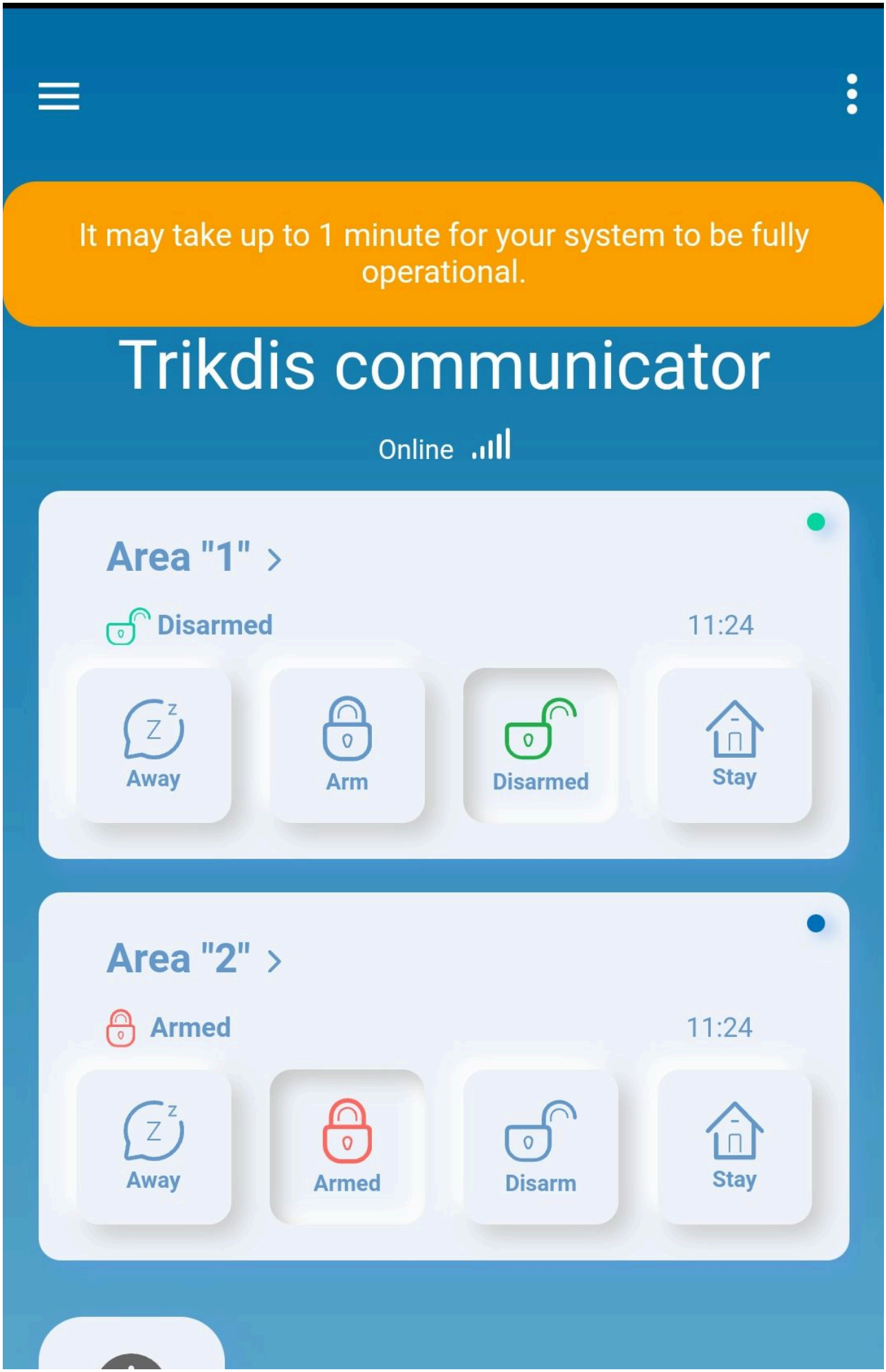
6. Add meg a rendszer nevét és válassz idozónát



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



Con l'E16 l'identificativo univoco del dispositivo è l'**indirizzo MAC (Unique ID)**: è riportato sulla scatola e sul retro del dispositivo, e lo mostra anche la barra di stato di TrikdisConfig (paragrafo 6.1). Quando crei il sistema nell'app, devi inserire questo come identificativo del dispositivo.

5.2 Controllo diretto con il codice della tastiera

Se la centrale rientra tra i modelli a controllo diretto (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 della tastiera della centrale** – lo stesso che usa sulla tastiera. Non servono un'uscita separata né una zona chiave.

- A seconda del produttore, nella centrale serve un'impostazione (Paradox: password PC, Texecom: password UDL; con le centrali Caddx, Honeywell e InnerRange l'abilitazione del bus o della porta seriale, già necessaria per la lettura degli eventi) – vedi il capitolo 4.
- Il codice della tastiera viene verificato dalla centrale, e anche il registro eventi della centrale annota l'utente, non il comunicatore.
- Con le centrali Paradox il codice dell'utente **non può essere il codice master**; dopo aver modificato un 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 (l'articolo riguarda il G16, ma vale allo stesso modo per l'E16).

Quando crei il 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 e lo stato arriva dal bus.

5.3 Inserimento con zona chiave

Se la centrale non può essere comandata direttamente, o non vuoi usarla così, colleghi una delle uscite del comunicatore alla zona chiave della centrale (paragrafo 3.4), in TrikdisConfig **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 della tastiera della centrale; con l'inserimento tramite zona chiave – se è attivata – la password di Protegus 2.

L'E16 non ha comando né notifiche via SMS: l'inserimento, il disinserimento e il comando delle uscite avvengono dall'app Protegus 2, e le notifiche arrivano come notifiche push.

6. TrikdisConfig – le impostazioni in dettaglio

Sul lato sinistro della finestra di TrikdisConfig si vede l'elenco delle pagine (System settings, CMS reporting, User reporting, Ethernet settings, IN/OUT, RS485 modules, Event summary, Firmware), in alto la barra dei pulsanti (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), in basso la barra di stato. Questo capitolo passa in rassegna le impostazioni dell'E16 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.

Etichetta	Significato
Status	Lo stato di funzionamento attuale.
Device	Il tipo (la sigla) del dispositivo. Verifica che qui compaia il tipo del tuo dispositivo.
SN	Numero di serie.
BL	La versione del bootloader.
FW	La versione del firmware.
HW	La versione dell'hardware.
State	La modalità di connessione: USB o da remoto (remote).
Administrator / Installer	Il livello di accesso di chi esegue la programmazione (dopo l'inserimento della password).

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



Figura 27. La barra di stato di TrikdisConfig con un E16 letto: indirizzo MAC (Unique ID, lasciato vuoto nell'immagine), stato, tipo (E16_1100), numero di serie, versioni, modalità di connessione e livello di accesso.

Con l'E16 l'identificativo univoco del dispositivo è l'**indirizzo MAC**: è quello che Protegus 2 chiede alla creazione del sistema e che TrikdisConfig chiede per l'accesso remoto (Unique ID). Lo stesso indirizzo è riportato anche sulla scatola e sul retro del dispositivo.

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 alla centrale d'allarme, nel gruppo **Access** i livelli di accesso.

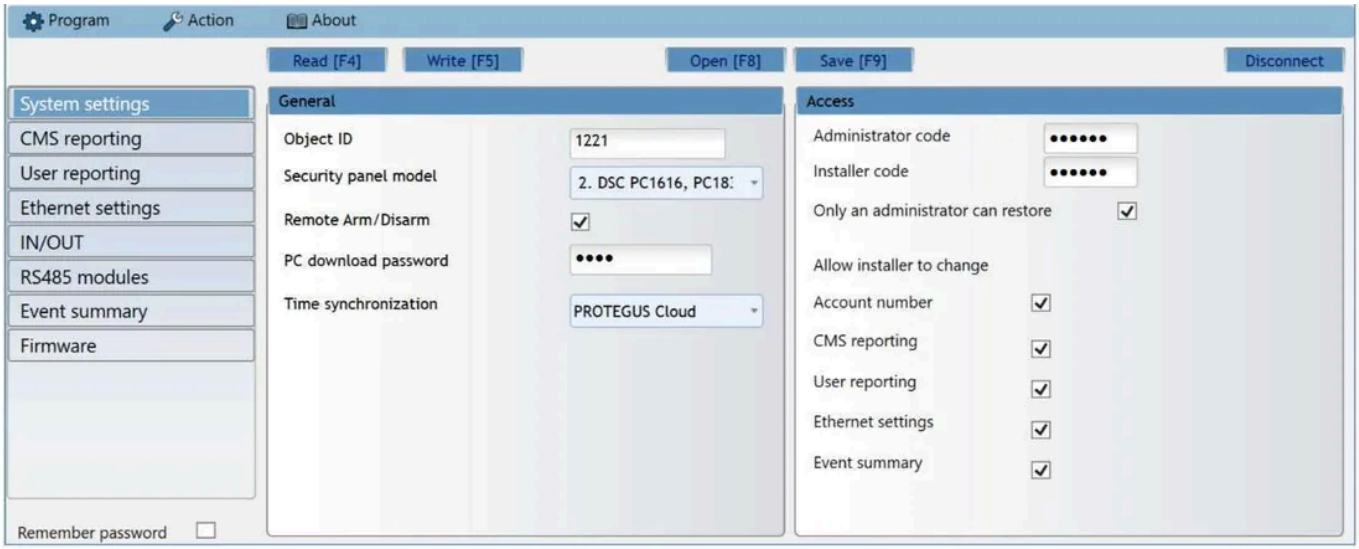


Figura 28. TrikdisConfig – pagina System settings: gruppi General e Access.

- **Object ID** – il codice d'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 modello della centrale d'allarme collegata, scelto dall'elenco. Da questo dipende come il comunicatore legge il bus, quindi scegli il modello esatto della centrale collegata.
- **Remote Arm/Disarm** – se spuntato, il comunicatore comanda direttamente la centrale: l'utente inserisce e disinserisce da Protegus 2 con il proprio codice della tastiera. Compare solo con i modelli di centrale a controllo diretto; a seconda del produttore richiede un'impostazione nella centrale (capitolo 4). Con l'inserimento tramite zona 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 synchronization** – la fonte dell'orologio del dispositivo (predefinito **PROTEGUS Cloud**, il cloud Protegus).

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

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

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

Non lasciare le password di fabbrica nel dispositivo!

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

6.3 CMS reporting

Il comunicatore invia gli eventi alla centrale di vigilanza tramite connessione IP. Gli eventi possono passare anche su più canali: il canale **principale** e il canale **parallelo** funzionano contemporaneamente (verso due ricevitori insieme), e a ciascuno appartiene un canale **di riserva**, che entra in funzione se quel canale si interrompe. La comunicazione è cifrata e protetta da password; per la ricezione e l'inoltro al software di vigilanza serve un ricevitore Trikdis (ricevitore software IPcom per Windows o Linux, ricevitore hardware IP/SMS RL14, ricevitore multicanale RM14) oppure un ricevitore universale che conosca il protocollo DC-09 / TL150.

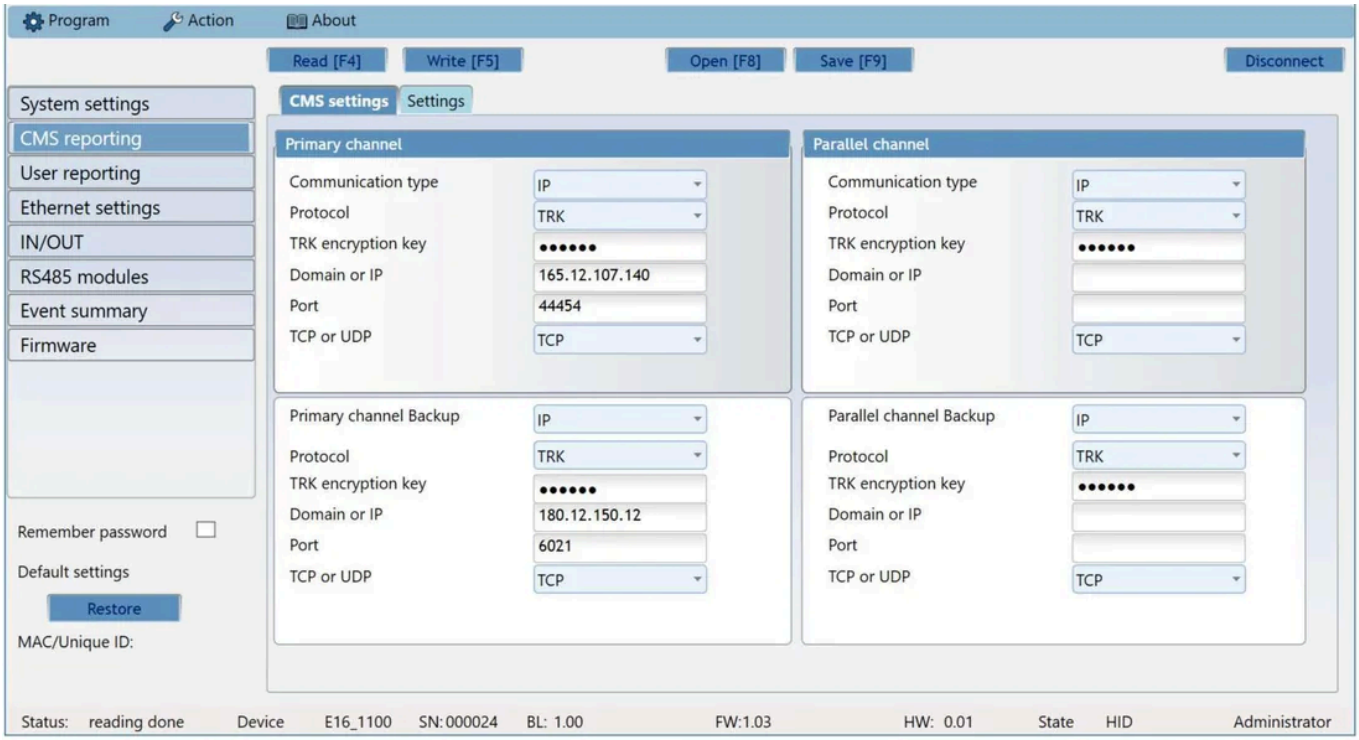


Figura 29. TrikdisConfig – CMS reporting, scheda CMS settings: canale principale e canale parallelo (in alto), i relativi canali di riserva (in basso).

Primary channel – canale principale

- **Communication type** – **IP**; con il valore **Disable** il canale può essere disattivato (ad esempio se il dispositivo funziona solo con Protegus 2, senza centrale di vigilanza).
- **Protocol** – TRK (ricevitori Trikdis), DC-09_2007 o DC-09_2012 (ricevitori universali), TL150 (SUR-GARD).
- **TRK encryption key** – chiave di cifratura a 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.

Primary channel Backup – canale di riserva. Subentra nella comunicazione se il canale principale non funziona; le sue impostazioni sono le stesse descritte sopra. Poiché l'E16 comunica su un'unica via di rete (la rete locale), il canale di riserva è un secondo indirizzo di ricevitore sulla stessa via: supera un guasto lato ricevitore, non la caduta della connessione Internet.

Parallel channel – canale parallelo. Oltre al principale, invia contemporaneamente a un secondo ricevitore (ad esempio a una centrale di vigilanza locale e a una centrale). Ha un proprio canale di riserva.

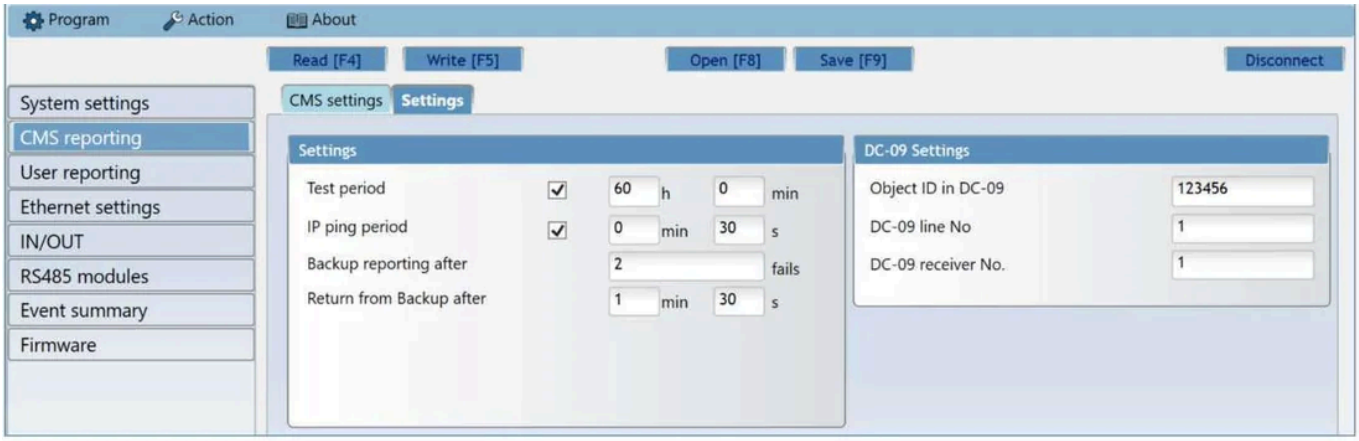


Figura 30. TrikdisConfig – CMS reporting, scheda Settings: rapporto di test, PING, temporizzazioni del canale di riserva e dati DC-09.

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

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

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

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

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

Il gruppo **DC-09 settings** è visibile solo se su uno dei canali è impostato il protocollo DC-09. I server dei nomi (DNS), con l'E16, non si inseriscono qui ma nella pagina **Ethernet settings** (paragrafo 6.5).

6.4 User reporting

Nella scheda **PROTEGUS Cloud** abiliti il servizio Protegus, con cui l'utente può monitorare e comandare il comunicatore a distanza; maggiori informazioni sul servizio: www.protegus.app. L'E16 non ha notifiche né comando via SMS, quindi in questa pagina c'è solo questa scheda.



Figura 31. 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 a Protegus (di fabbrica `123456`). Può essere impostato solo prima di creare il sistema in Protegus 2; in seguito non può essere modificato.

6.5 Ethernet settings

Qui imposti come l'E16 si collega alla rete locale. Di fabbrica è spuntato **Use DHCP**: il dispositivo riceve automaticamente dal router l'indirizzo, il gateway e i server dei nomi, e nella maggior parte dei casi non c'è nulla da fare.



Figura 32. TrikdisConfig – pagina Ethernet settings: DHCP o configurazione di rete manuale, server dei nomi.

- **Use DHCP** – con la spunta il dispositivo riceve automaticamente indirizzo IP, subnet mask e gateway dal server DHCP del router. È l'impostazione di fabbrica e nella maggior parte dei casi non c'è altro da fare. Se nella rete non c'è DHCP, se la connessione automatica alla rete non riesce o se l'amministratore di rete richiede un indirizzo fisso, togli la spunta e compila a mano i campi seguenti e i server DNS:
- **Static IP** – l'indirizzo IP fisso del dispositivo nella rete locale (un indirizzo non usato da altri dispositivi e al di fuori dell'intervallo DHCP).
- **Subnet mask** – la subnet mask della rete.
- **Default gateway** – il gateway predefinito, di solito l'indirizzo del router. Con un gateway sbagliato il dispositivo raggiunge la rete locale, ma non Internet.
- **DNS 1, DNS 2** – server dei nomi; tramite questi il dispositivo trova il cloud Protegus e il ricevitore indicato con nome di dominio. Di fabbrica è impostato il DNS pubblico di Google; se la rete verso l'esterno consente solo il proprio server dei nomi, inserisci qui l'indirizzo del DNS locale. 3 lampeggi del LED TROUBLE indicano un errore DNS.

L'identificativo univoco del dispositivo, l'indirizzo MAC (nel programma **Internal MAC**), nella finestra più recente di TrikdisConfig non si trova in questa pagina, ma in fondo alla finestra, nel campo **MAC / Unique ID** della barra di stato.

Il dispositivo stabilisce solo connessioni **in uscita** verso il ricevitore e il cloud Protegus, quindi sul router non serve aprire né inoltrare porte, e non serve nemmeno un indirizzo IP pubblico fisso.

6.6 IN/OUT

Qui definisci 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 e I/O 2 ingressi (NO), I/O 3 uscita.

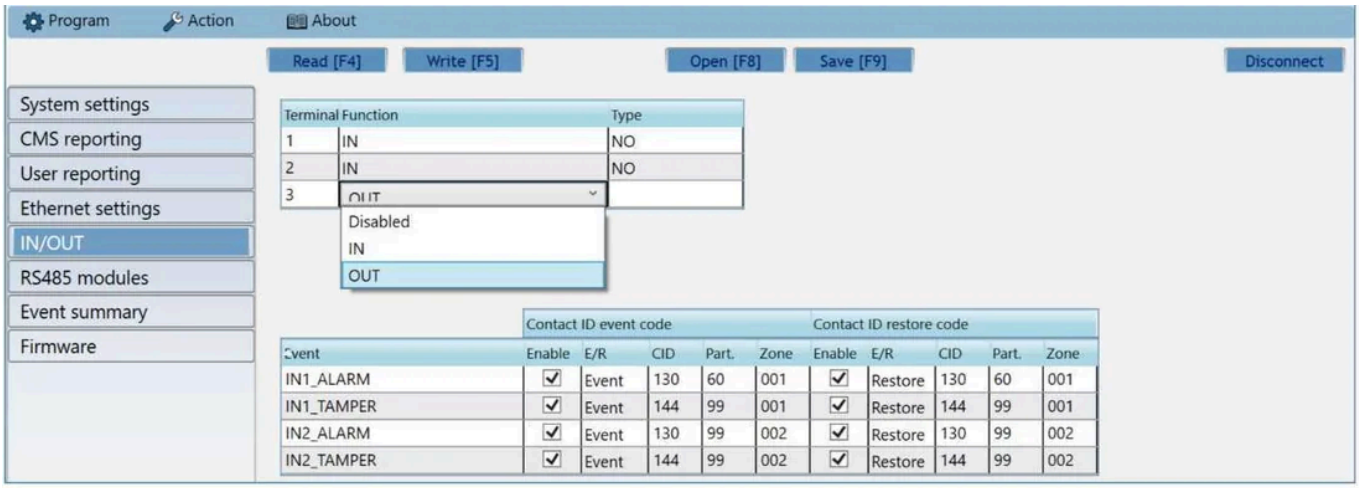


Figura 33. TrikdisConfig – pagina IN/OUT: funzione dei morsetti I/O ed eventi degli ingressi.

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 antimanomissione 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; puoi inserirlo o lasciare il valore predefinito. L'evento viene inviato con questo codice a Protegus 2 e alla centrale di vigilanza.
- **Part.** – il numero di area nel messaggio.
- **Zone** – il numero di zona nel messaggio.

6.7 RS485 modules

Le espansioni iO-8 collegate al bus RS485 vanno aggiunte nella scheda **Modules list**.

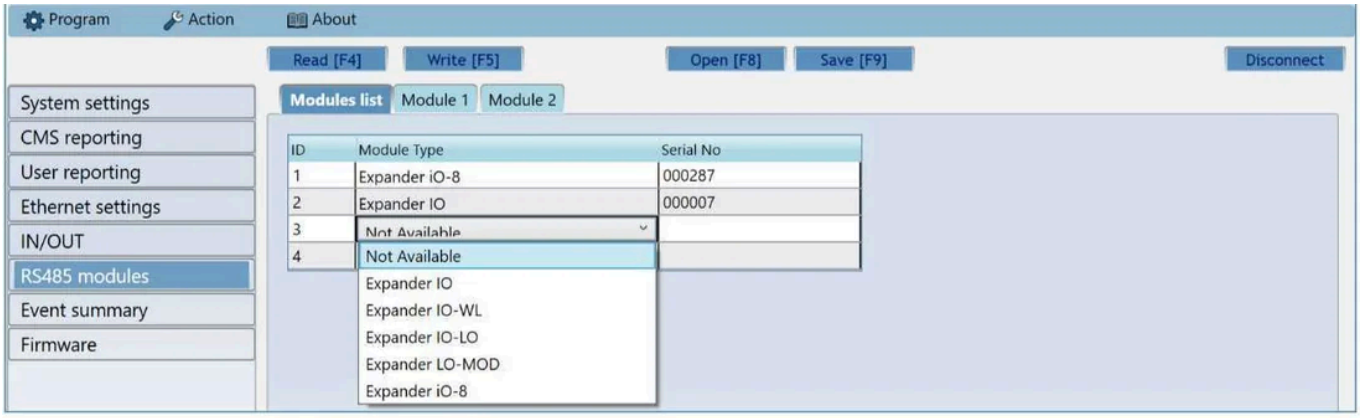


Figura 34. TrikdisConfig – RS485 modules, scheda Modules list: tipo di modulo (Expander iO-8) e numero di serie.

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

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

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

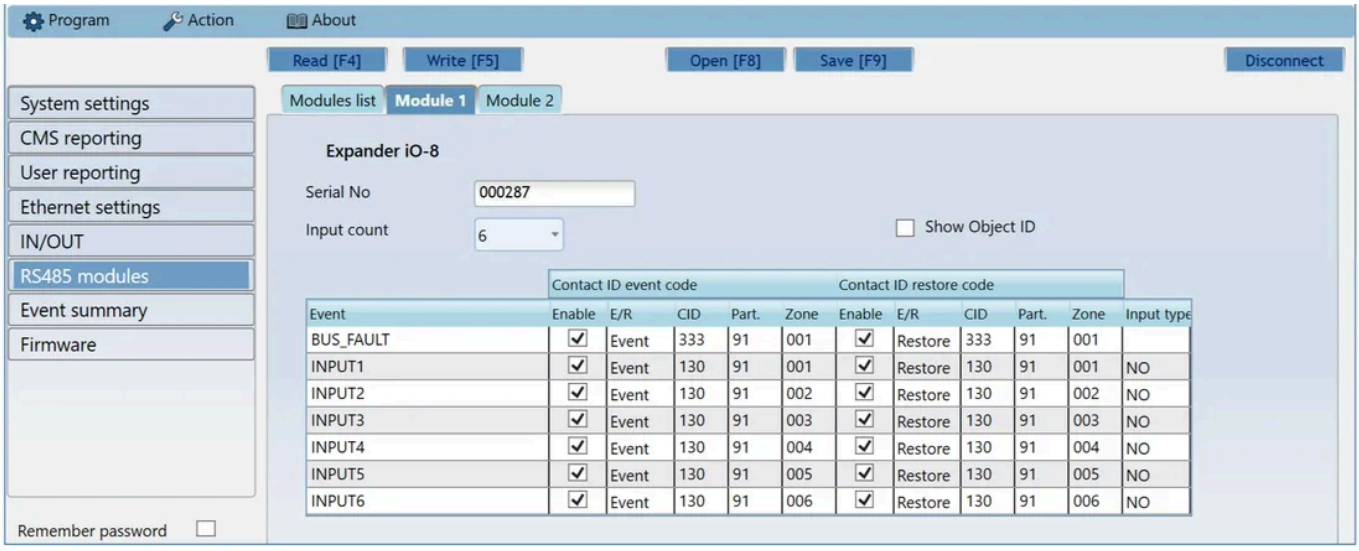


Figura 35. TrikdisConfig – RS485 modules, scheda del modulo iO-8 (in alto) e tabella degli eventi dell'espansione (in basso).

- **Input Count** – quanti morsetti devono essere ingressi; gli altri saranno uscite. Il tipo di ingresso (**Input type**: NO o NC) si imposta nella tabella. Il ruolo delle uscite (inserimento / disinserimento con zona 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**). 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 un codice d'impianto diverso da quello del comunicatore.

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).

Messaggio	Contact ID	Quando viene generato
TEST	602	Rapporto di test periodico.
PING	760	Il messaggio di esistenza in vita PING. Non compare nell'elenco di tutti i dispositivi: sulla schermata della versione hardware precedente sì, nella pagina Event summary delle versioni più recenti questa riga non c'è. L'intervallo si imposta nel campo **CMS reporting → Settings → IP ping period**.

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

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

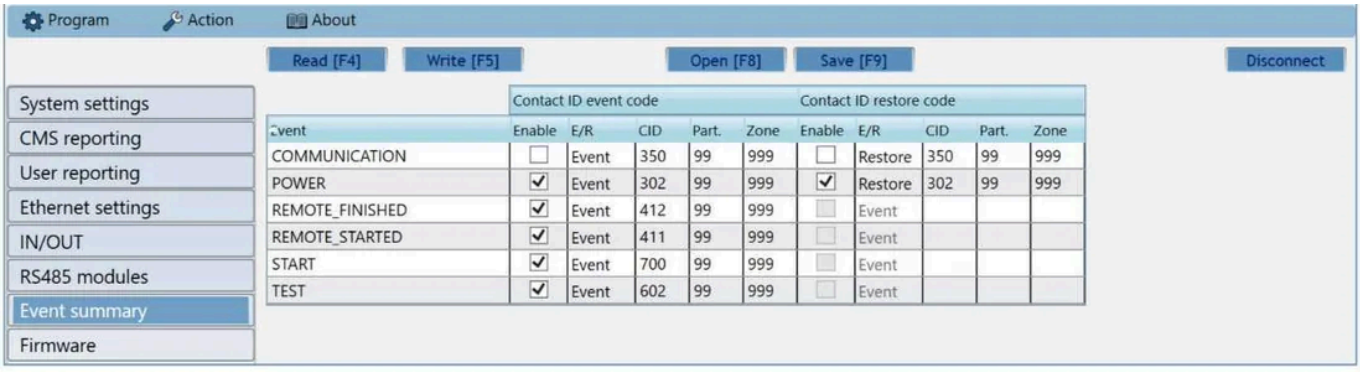


Figura 36. TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo (COMMUNICATION, POWER, REMOTE_FINISHED, REMOTE_STARTED, START, TEST) e i relativi codici Contact ID.

6.9 Ripristino delle impostazioni di fabbrica

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

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

7. Programmazione a distanza

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

Per l'accesso da remoto servono:

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

Passaggi:

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

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

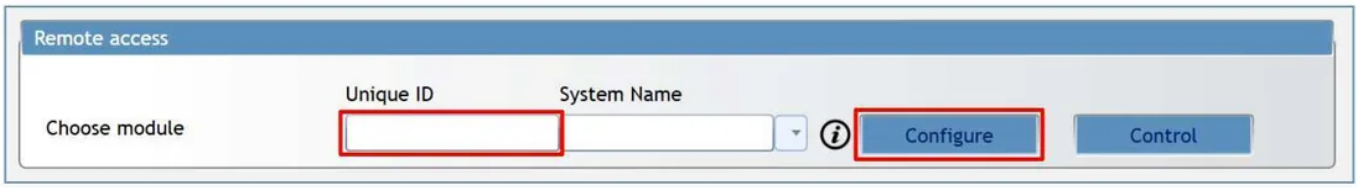


Figura 37. TrikdisConfig – Remote access: l'identificativo del dispositivo (Unique ID – con l'E16 l'indirizzo MAC), il nome del sistema e il pulsante Configure.

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 della tastiera dell'utente.

Verifica anche la riserva di rete: scollega il cavo Ethernet e controlla che il LED TROUBLE segnali la mancanza con 1 lampeggio, poi, dopo aver ricollegato il cavo, che il LED NETWORK torni verde fisso e che gli eventi memorizzati arrivino alla centrale di vigilanza e all'app.

9. Aggiornamento del firmware

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

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

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

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

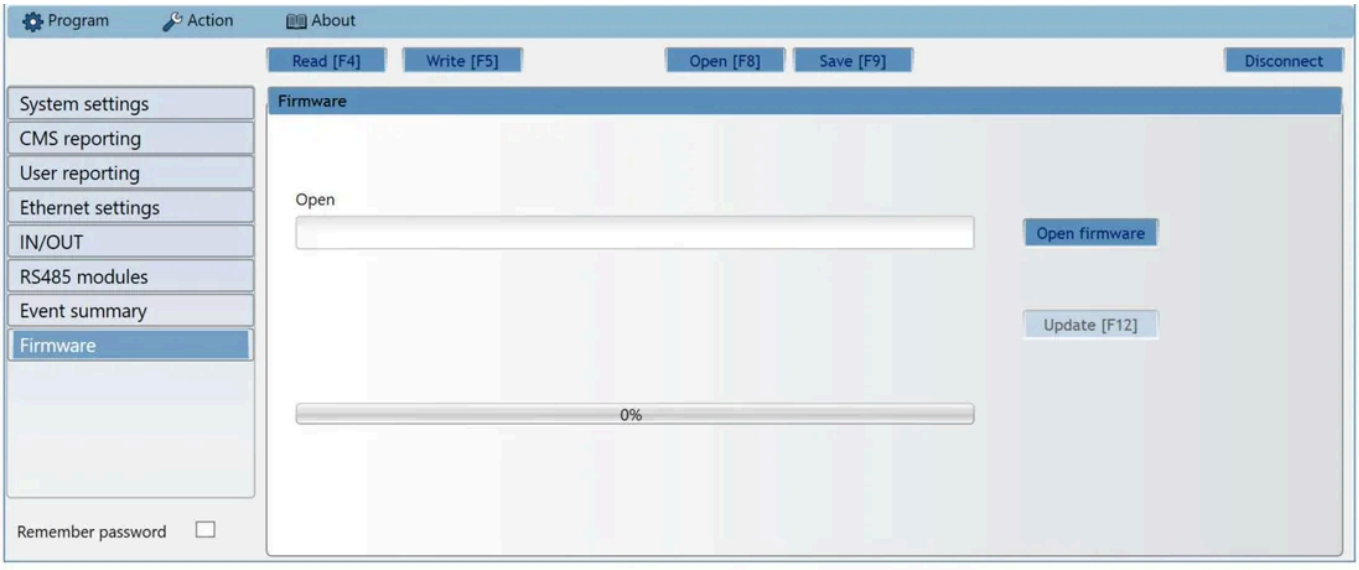


Figura 38. TrikdisConfig – pagina Firmware: Open firmware e Update [F12] (in alto), indicatore di avanzamento dell'aggiornamento (in basso).

Per l'aggiornamento serve una connessione Internet. Un antivirus, un firewall o impostazioni di rete restrittive possono impedire il download automatico del firmware; in questo caso modifica le impostazioni dell'antivirus, 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 è spento – nessuna rete

1. Guarda i lampeggi del LED **TROUBLE**: 1 = nessun collegamento fisico (cavo, porta), 2 = non ha ottenuto un indirizzo IP (DHCP), 3 = non riesce a risolvere il nome del ricevitore o del cloud Protegus (DNS).
2. **1 lampeggio:** controlla il cavo Ethernet a entrambe le estremità e che la porta del router o dello switch sia attiva (il LED della porta è acceso); prova un'altra porta o un altro cavo.
3. **2 lampeggi:** sul router deve essere attivo il DHCP, oppure assegna al dispositivo un indirizzo IP fisso nella pagina **Ethernet settings** (paragrafo 6.5). In una rete aziendale l'amministratore di rete può autorizzare il dispositivo in base all'indirizzo MAC.
4. **3 lampeggi:** il server dei nomi non è raggiungibile. Di fabbrica è impostato il DNS pubblico di Google; se la rete blocca i DNS esterni, inserisci il server dei nomi locale nella pagina **Ethernet settings**.

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

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

1. 6 lampeggi del LED **TROUBLE** indicano che non c'è connessione con il ricevitore: controlla l'indirizzo, la porta, l'impostazione TCP/UDP e la chiave di cifratura del ricevitore (**CMS reporting**).
2. Se il ricevitore è indicato con un nome di dominio, controlla l'impostazione DNS (**Ethernet settings**).
3. In una rete filtrata da un firewall va consentito il traffico TCP/UDP in uscita verso la porta del ricevitore; sul router non bisogna aprire porte (in ingresso).

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

1. Controlla il collegamento secondo lo schema del paragrafo 3.3: l'errore più frequente sono i fili **CLK** e **DATA** invertiti, o la linea dati collegata al morsetto sbagliato della centrale.
2. Nel campo **System settings** → **Security panel model** di TrikdisConfig deve essere selezionato il modello 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 una centrale Paradox può darsi che la porta seriale sia bloccata di fabbrica – ecco come sbloccarla.
5. Dopo il collegamento, togli l'alimentazione a una centrale Pyronix e riavviala, affinché accetti il comunicatore.

6. Con una centrale DSC PowerSeries **NEO** l'E16 non funziona (il bus della NEO non accetta dispositivi esterni) – qui serve un comunicatore per linea telefonica (E16T).

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 una centrale Paradox il firmware della centrale deve essere almeno **V.4**; il codice dell'utente non deve essere il codice master; dopo aver modificato un codice riavvia il comunicatore.
4. Con una centrale 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 chiave:

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

Protegus 2 non vede il dispositivo

1. Nella pagina **User reporting** → **PROTEGUS Cloud** deve essere spuntato **Enable connection**.
2. Quando crei il 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'**indirizzo MAC (Unique ID)** esattamente, copiandolo dalla scatola o dal retro.
4. Il dispositivo deve essere online: il LED NETWORK è verde, TROUBLE non lampeggia e il LED DATA si spegne dopo un evento. In una rete con firewall va consentita la connessione in uscita verso il cloud Protegus.

Non riesco ad accedere a distanza con TrikdisConfig

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

Ho dimenticato la password

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

Bisogna aprire o inoltrare porte sul router?

No. L'E16 stabilisce solo connessioni **in uscita** verso il ricevitore e il cloud Protegus, quindi non servono né l'inoltro delle porte né un indirizzo IP pubblico; anche la programmazione a distanza avviene tramite questa connessione in uscita. Fai solo attenzione che il firewall non blocchi il traffico in uscita verso la porta del ricevitore e verso il cloud Protegus.

Funziona su Wi-Fi o su rete mobile?

No: l'E16 ha solo un connettore Ethernet cablato. Se il router non ha un'alimentazione affidabile, alimenta i dispositivi di rete con un gruppo di continuità (UPS).

Che cosa succede durante un'interruzione di corrente?

L'E16 è alimentato dalla centrale d'allarme, quindi continua a funzionare con la batteria della centrale, ma il router e il modem di solito si fermano, e con loro viene meno Internet. Finché non c'è connessione, il LED TROUBLE segnala con 1 o 6 lampeggi, il dispositivo memorizza gli eventi (al massimo 60 messaggi) e al ritorno di Internet li invia in ordine. Se per il sistema la caduta di Internet non è ammissibile, alimenta anche i dispositivi di rete con un gruppo di continuità (UPS).

11. Norme di sicurezza

Figyelem!

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

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

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

- L'installazione e la manutenzione delle apparecchiature di sicurezza possono essere eseguite solo da un installatore qualificato.
- Prima dell'installazione leggi il manuale; ignorare le istruzioni può causare malfunzionamenti o guasti.
- Prima del collegamento, a ogni collegamento elettrico e prima di ogni intervento di assistenza, scollega l'apparecchiatura dall'alimentazione.
- I guasti dovuti a 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 della tastiera, stato delle zone, esclusione delle zone; vale allo stesso modo per l'E16.
- DSC Power Series NEO e comunicatori Trikdis: compatibilità e soluzioni – perché l'E16 non può essere collegato alla NEO, e qual è la soluzione.
- Sblocco della porta seriale bloccata sulle centrali d'allarme Paradox – lo sblocco della porta seriale delle centrali Paradox più recenti.
- Inserimento a distanza con zona chiave dall'app Protegus 2 – i dettagli e le insidie dell'inserimento con zona chiave.
- Documentazione Trikdis: docs.trikdis.com.

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

Prodotti correlati

Trikdis E16 Ethernet comunicatore - modulo IP

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-e16