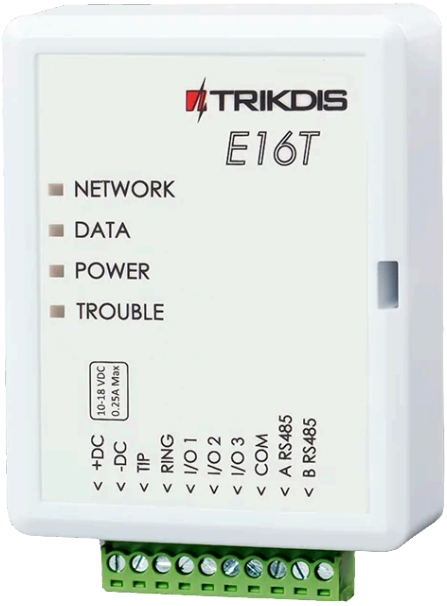
Comunicatore E16T – manuale per l'installatore e per l'utente

Manuale per l'installatore e per l'utente del comunicatore Ethernet Trikdis E16T: collegamento alla centrale d'allarme, configurazione di rete in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2, verifica e risoluzione dei problemi.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-e16t

Indice

1. Panoramica

1.1 A cosa serve e come funziona
1.2 Versioni
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 Collegamento all'app Protegus 2
2.3 Collegamento alla centrale di vigilanza

3. Installazione e collegamento

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

4. Programmazione della centrale d'allarme

4.1 Programmazione del combinatore Honeywell Vista
4.2 Centrali di altri produttori

5. Controllo a distanza con l'app Protegus 2

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

6. 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'E16T è il **comunicatore Ethernet universale** di Trikdis: si collega all'uscita della linea telefonica (TIP/RING) della centrale d'allarme e si comporta come una centrale telefonica. La centrale d'allarme «compone il numero» e invia il messaggio Contact ID con toni DTMF; l'E16T risponde alla linea, decodifica il messaggio e lo 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. Si può quindi usare con **centrali di qualsiasi marca** dotate di un combinatore Contact ID – non bisogna sostituire la centrale, basta configurarne il combinatore. L'E16T lavora su Internet cablato, senza scheda SIM e senza abbonamento.

1.1 A cosa serve e come funziona

- **Trasmette alla centrale di vigilanza.** Invia gli eventi, tramite connessione IP, al ricevitore software o hardware Trikdis (protocollo TRK; questi ricevitori collaborano con qualsiasi software di vigilanza) oppure a qualsiasi ricevitore universale (SIA DC-09 2007/2012, SUR-GARD TL150). Per impostazione predefinita verifica la connessione ogni 30 secondi (invia al ricevitore un segnale di esistenza in vita, PING; l'intervallo è modificabile) e in caso di guasto passa al canale di riserva.
- **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, ventilazione, riscaldamento, impianto di irrigazione ecc.). L'app funziona con la centrale d'allarme di qualsiasi produttore a cui è collegato l'E16T.
- 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.
- **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.
- **Nessun abbonamento.** L'E16T usa la connessione Internet già presente nel sito: non servono scheda SIM, abbonamento mobile né antenna, e l'intensità del segnale mobile non ha importanza.

La struttura del sistema è mostrata nella figura seguente: l'uscita della linea telefonica della centrale d'allarme si collega all'E16T, l'E16T raggiunge Internet tramite il router locale e da lì il ricevitore della centrale di vigilanza e il cloud Protegus, mentre l'utente vede il sistema nell'app Protegus 2.

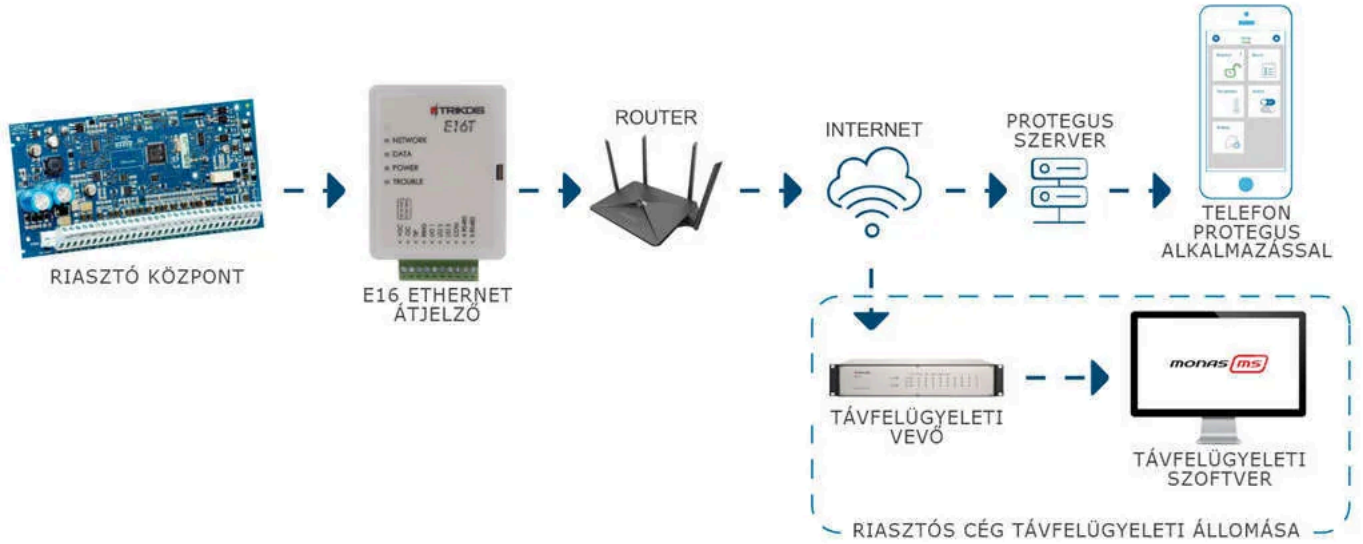


Figura 1. La posizione dell'E16T nel sistema: centrale d'allarme → E16T → router → Internet → ricevitore della centrale di vigilanza e cloud Protegus → app Protegus 2.

1.2 Versioni

Questo manuale è stato scritto per l'**attuale versione hardware v2** dell'E16T (TrikdisConfig la mostra come **E16T_2000**), ma **vale anche per l'E16T precedente**: il collegamento, la configurazione e il funzionamento sono in gran parte identici. Le differenze sono riassunte nella tabella seguente; dove il testo indica il dato della v2, per la versione precedente tieni conto di quanto segue.

	E16T precedente	**E16T v2 (attuale)**
Ingressi/uscite	2 ingressi di tipo selezionabile (T-1/IN1, R-1/IN2 – NC, NO, EOL; utilizzabili anche per la supervisione della linea telefonica) + 1 uscita a collettore aperto (OUT, max. 0,15 A, fino a 30 V; comandabile dall'app Protegus)	3 morsetti I/O a doppia funzione (I/O 1, I/O 2, I/O 3), ognuno utilizzabile come ingresso (tipi NC, NO, EOL, DEOL) o come uscita a collettore aperto (max. 0,15 A)
Assorbimento	al massimo 0,5 A	100 mA nominali, al massimo 250 mA durante l'invio
LED	NETWORK, DATA, POWER, TROUBLE, LINE (il LED LINE è verde fisso finché la centrale «ha sollevato il ricevitore», cioè sta componendo; le segnalazioni diverse degli altri LED sono elencate nella nota alla fine del paragrafo 1.6)	NETWORK, DATA, POWER, TROUBLE
Memoria eventi	100 messaggi	60 messaggi
Dimensioni	88 × 62 × 25 mm	88 × 65 × 26 mm

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

1.3 Caratteristiche principali

Collegamento alla centrale d'allarme

- Collegamento normale all'uscita della linea telefonica della centrale: DC+, DC−, TIP e RING. Se necessario, si può collegare anche con supervisione della linea (con i fili T-1 e R-1): in questo caso la connessione tra centrale e comunicatore è **supervisionata**, il comunicatore segnala l'interruzione del cavo.

- La centrale invia gli eventi in formato Contact ID con composizione DTMF; l'E16T inoltra l'informazione completa dell'evento (codice, area, zona o utente).

Comunicazione con la centrale di vigilanza

- Connessione IP con i ricevitori Trikdis (ricevitore software IPcom, RL14, RM14) e con ricevitori universali (SIA DC-09, TL150).
- Canale principale, di riserva e parallelo: può inviare contemporaneamente anche a due ricevitori, ognuno con il proprio canale di riserva.
- Comunicazione cifrata e protetta da password; 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 – per la configurazione del dispositivo, per l'amministratore della centrale di vigilanza e per l'installatore.
- Configurabile e aggiornabile a distanza con il software TrikdisConfig.

1.4 Le parti del comunicatore

L'E16T ha il circuito stampato in una scatola di plastica bianca; il coperchio frontale è rimovibile e la morsettiera è estraibile. Il connettore di rete (RJ45) si trova sul bordo superiore del circuito stampato ed è accessibile attraverso l'apertura della scatola.

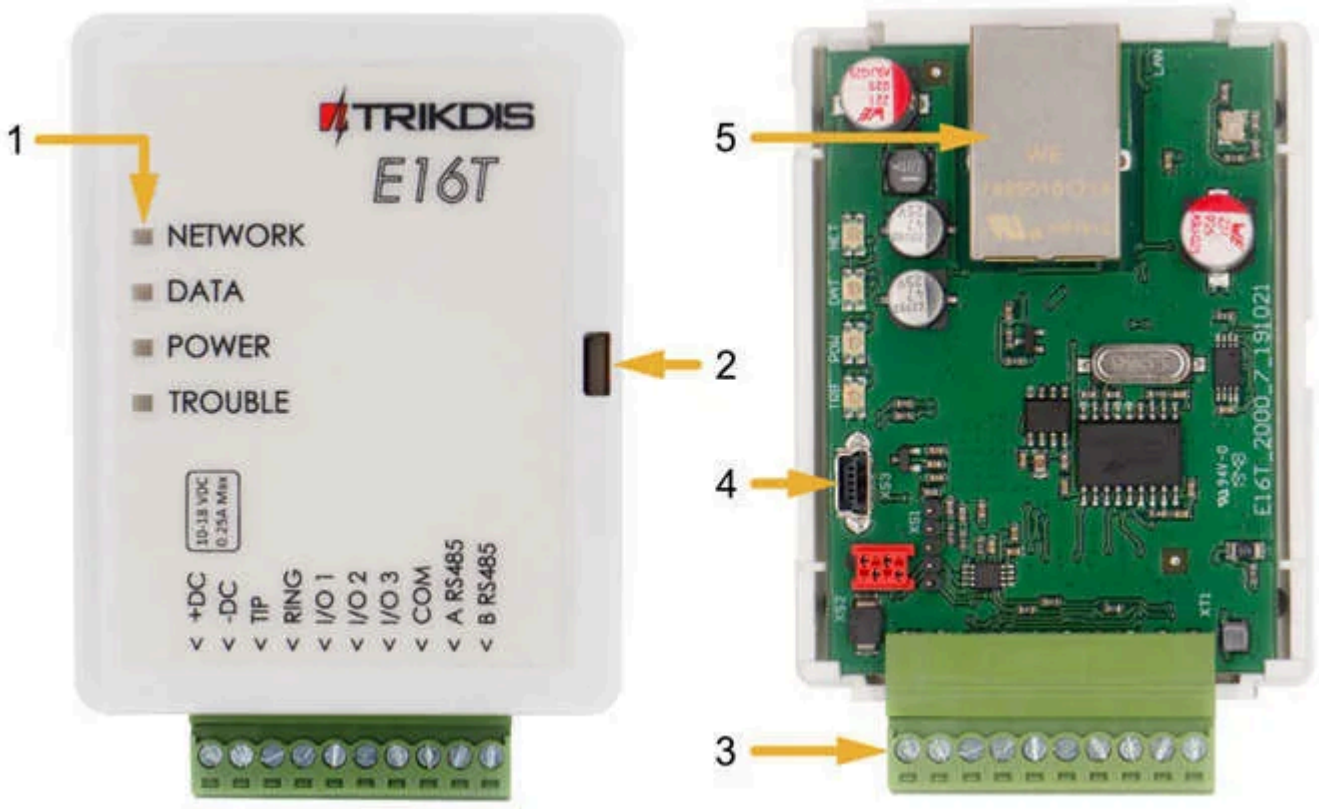


Figura 2. Le parti dell'E16T viste di fronte e con la scatola aperta.

- 1 LED di segnalazione (NETWORK, DATA, POWER, TROUBLE)
- 2 Apertura per facilitare la rimozione del coperchio frontale (sul bordo superiore del coperchio)
- 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
TIP	Morsetto TIP della centrale d'allarme
RING	Morsetto RING della centrale d'allarme
I/O 1 (T-1)	Ingresso/uscita 1, oppure punto T-1 della supervisione della linea telefonica
I/O 2 (R-1)	Ingresso/uscita 2, oppure punto R-1 della supervisione della linea telefonica
I/O 3	Ingresso/uscita 3
COM	Punto comune (negativo) per ingressi e uscite
A 485	Filo A del bus RS485 (iO-8 e altre espansioni della serie iO)
B 485	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.

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 i messaggi in attesa di invio, TROUBLE il guasto.

NETWORK – connessione di rete

Segnalazione	Significato
spento	Nessuna connessione alla rete (manca il cavo, la porta non è attiva oppure non ha ottenuto un indirizzo IP)
verde fisso	Connesso alla rete locale – la connessione funziona fino al router. Se anche Internet è raggiungibile lo mostra il LED DATA (vedi sotto).

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
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): cavo, connettore oppure porta del router / dello switch
2 lampeggi rossi	Errore DHCP: il dispositivo non ha ottenuto un indirizzo IP
3 lampeggi rossi	Errore DNS: la risoluzione dei nomi non funziona
6 lampeggi rossi	Nessuna connessione con il ricevitore della centrale di vigilanza
7 lampeggi rossi	Collegamento con la centrale d'allarme interrotto
rosso lampeggiante (durante la programmazione)	Errore di memoria
rosso fisso (durante la programmazione)	Firmware danneggiato

E16T precedente

I LED dell'E16T precedente indicano in parte cose diverse: **DATA** è giallo fisso se in memoria c'è un evento in attesa di invio e lampeggia in verde mentre la centrale d'allarme trasmette un messaggio al comunicatore; **POWER** lampeggia in verde se l'alimentazione è inserita e la tensione è adeguata, e lampeggia in giallo se la tensione di alimentazione non è sufficiente (al massimo 11,5 V); la luce rossa fissa di **TROUBLE** indica un errore di connessione alla rete (LAN), spento significa nessun guasto; **LINE** è verde fisso finché la centrale «ha sollevato il ricevitore» (paragrafo 1.2).

1.7 Dati tecnici

Parametro	Valore
Collegamento alla centrale d'allarme	linea telefonica cablata (TIP/RING), Contact ID, DTMF
Ingressi/uscite	3 I/O a doppia funzione (I/O 1, I/O 2, I/O 3): come ingresso NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistenza di fine linea 2,2 kΩ); come uscita a collettore aperto (OC), max. 0,15 A / 30 V DC
Espansione	sul bus RS485: espansione iO-8 (+8 I/O) e altre espansioni della serie iO, al massimo 4 moduli
Connessione di rete	Ethernet, IEEE 802.3, 10Base-T, presa RJ45
Configurazione di rete	DHCP (di fabbrica) o indirizzo IP fisso
Tensione di alimentazione	10–18 V DC
Assorbimento	100 mA nominali; al massimo 250 mA durante l'invio
Protocolli di trasmissione	TRK, DC-09_2007, DC-09_2012, TL150
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)
Dimensioni	88 × 65 × 26 mm
Peso	80 g

2. Messa in servizio rapida con TrikdisConfig

Tutte le impostazioni dell'E16T 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 (per la configurazione) · cavo con almeno 4 conduttori per la centrale · cacciavite piatto da 2,5 mm · cavo Ethernet (CAT-5 o superiore, al massimo 100 m) fino al router o allo switch · una porta di rete libera · se nella rete non c'è un DHCP: indirizzo IP fisso, subnet mask, gateway e DNS forniti dall'amministratore di rete · il manuale d'installazione della centrale d'allarme. Ciò che manca si può ordinare separatamente dal distributore locale.

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

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Apri il coperchio frontale dell'E16T e collegalo al computer. Inserisci un cacciavite piatto nell'apertura sul bordo superiore del coperchio e, facendo leva verso il basso, sgancia delicatamente il coperchio frontale, poi inserisci il cavo USB Mini-B. L'USB fornisce alimentazione sufficiente per la programmazione, non serve un alimentatore separato.

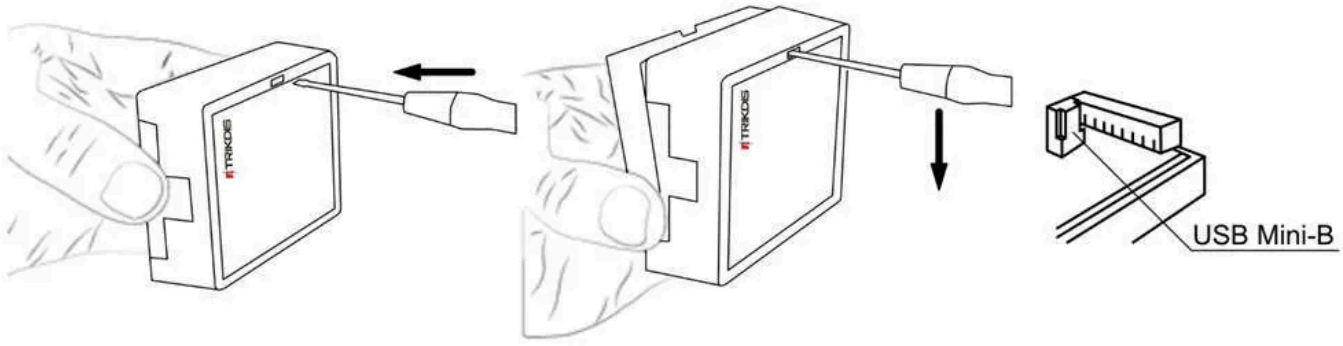


Figura 3. Sgancio del coperchio frontale e collegamento al computer con un cavo USB Mini-B.

Avvertenza

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

3. 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`).

I due paragrafi seguenti descrivono che cosa impostare perché la centrale d'allarme sia comandabile dall'app Protegus 2 (2.2) e perché il comunicatore invii gli eventi alla centrale di vigilanza (2.3).

2.2 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 4. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

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

Poi, nella pagina **System settings**, controlla il tipo di interfaccia della centrale d'allarme.

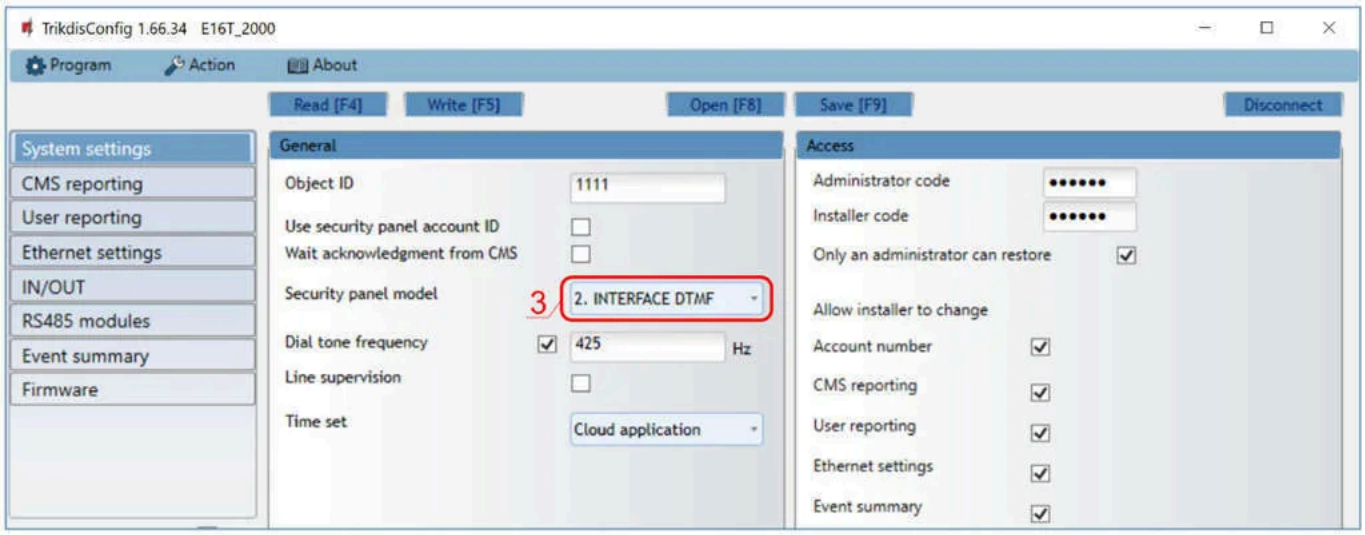


Figura 5. TrikdisConfig – pagina System settings, gruppo General.

- 3 **Security panel model** – lascia **2. INTERFACE DTMF** (il collegamento tramite linea telefonica con composizione DTMF).

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).

Se usi il dispositivo 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.

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

2.3 Collegamento alla centrale di vigilanza

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

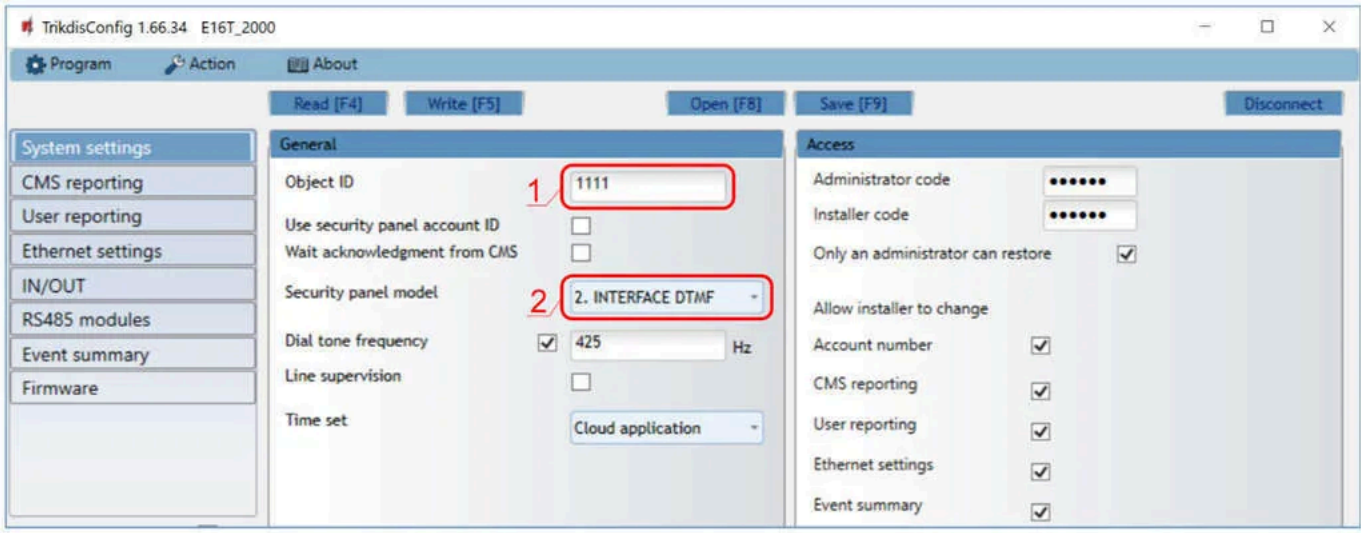


Figura 6. TrikdisConfig – pagina System settings, gruppo General.

- 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** – lascia **2. INTERFACE DTMF**.

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

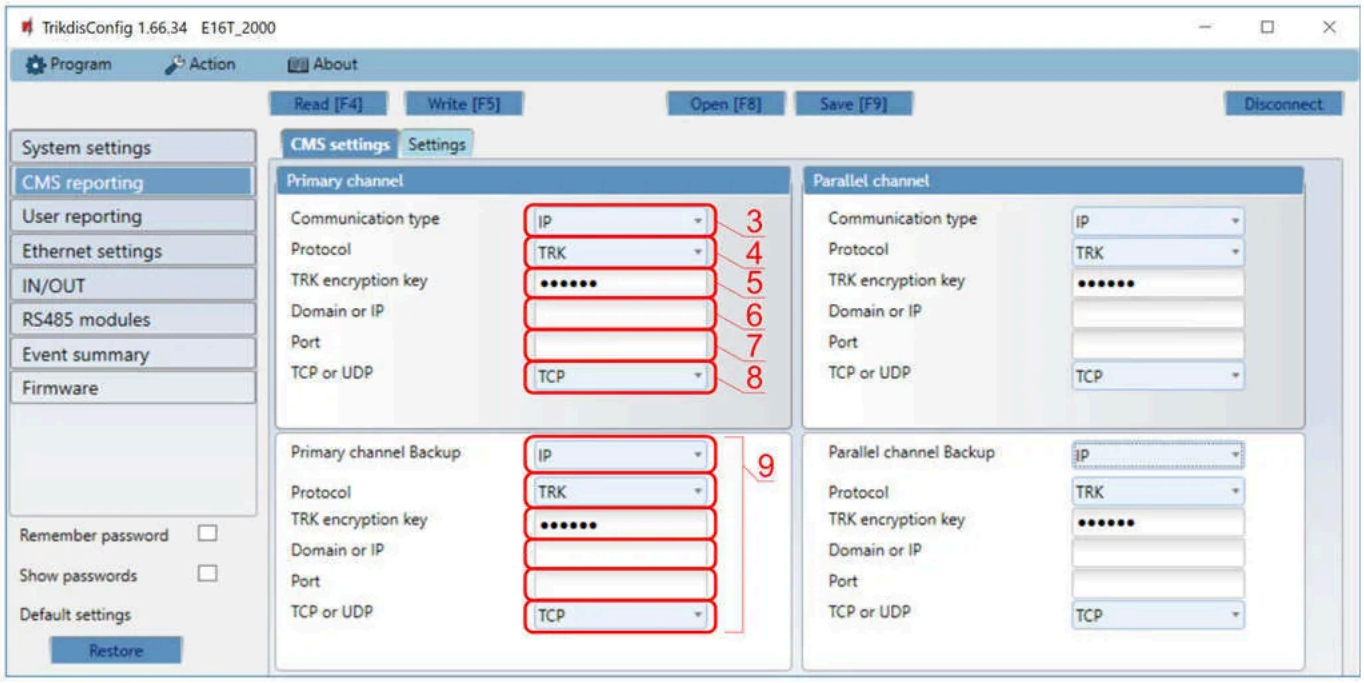


Figura 7. TrikdisConfig – CMS reporting, scheda CMS settings.

- 3 **Communication type** – **IP** (con l'E16T 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.

Con il protocollo **DC-09**, nella scheda **Settings** inserisci anche il numero d'impianto, di linea e di ricevitore DC-09 (paragrafo 6.3); con DC-09_2012 si può attivare anche la cifratura con la chiave DC-09 impostata nel ricevitore (nota del paragrafo 6.3). Per la verifica della connessione l'intervallo del segnale di esistenza in vita (PING) si imposta nella stessa scheda **Settings** (**IP ping period**, di fabbrica 30 s). Se indichi il ricevitore con un nome di dominio, per la risoluzione dei nomi serve anche l'impostazione DNS della pagina **Ethernet settings** (di fabbrica contiene il DNS pubblico di Google). Nell'E16T precedente i campi hanno nomi diversi (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**); la corrispondenza è indicata nella nota del paragrafo 6.3.

Se l'utente usa anche l'app Protegus 2, esegui anche le impostazioni del paragrafo 2.2 (**User reporting** → **PROTEGUS Cloud**). 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 3.6).
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 cablaggio sia corto. Un contenitore metallico non lo disturba: l'E16T 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'E16T 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 (G16T).

3.3 Collegamento alla centrale d'allarme

L'E16T va collegato all'uscita della linea telefonica (TIP/RING) della centrale e riceve l'alimentazione dall'uscita di alimentazione ausiliaria a 12 V (AUX) della centrale.

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

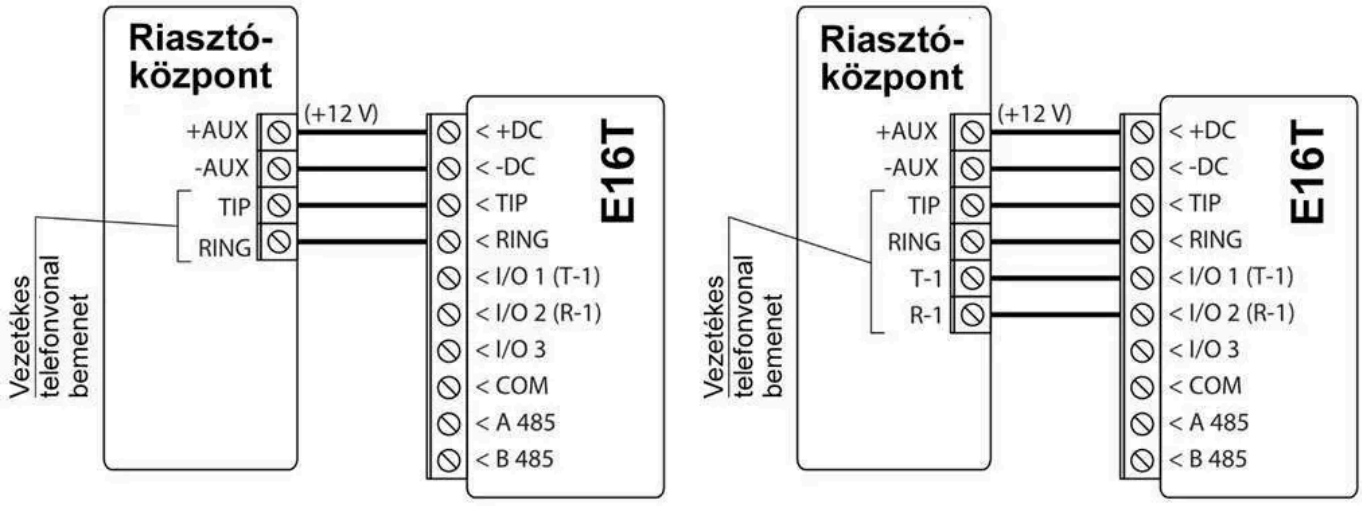


Figura 8. Collegamento all'uscita della linea telefonica della centrale: a sinistra il collegamento normale, a destra il collegamento con supervisione della linea.

Durante l'invio l'E16T assorbe al massimo 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.

3.3.1 Se necessario: supervisione della linea

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

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

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

3.4 Collegamento della zona chiave

Se vuoi inserire e disinserire la centrale a distanza, dall'app Protegus 2, imposta uno dei morsetti I/O del comunicatore come **uscita** e collegalo a una **zona 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'E16T ha tre morsetti I/O, si possono gestire fino a tre aree con uscite separate.

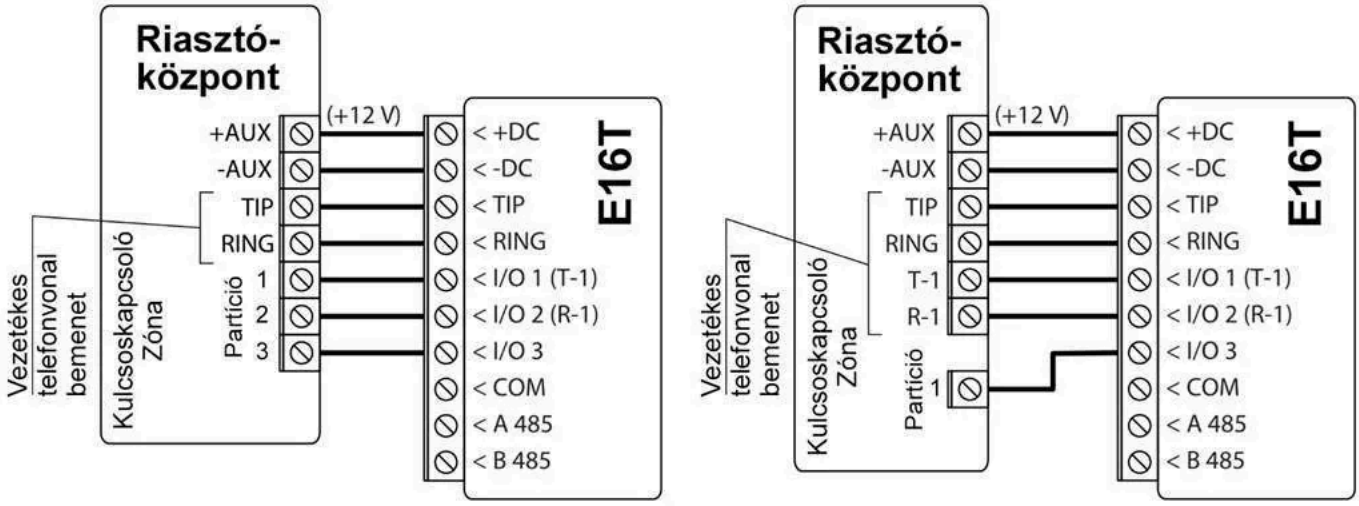


Figura 9. Inserimento e disinserimento con zona chiave: a sinistra il collegamento normale, a destra il collegamento con supervisione della linea (in questo caso per la zona chiave resta I/O 3).

La zona chiave può essere a impulso o bistabile – nell'app Protegus 2 va impostata la stessa modalità (paragrafo 5.2). 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.

E16T precedente

Nell'E16T precedente (2 ingressi + OUT) il tipo e la modalità dell'uscita si impostano nel gruppo **System settings** → **Output** di TrikdisConfig: per l'inserimento con zona chiave **OUT type** deve essere **Remote Control** e **OUT mode Pulse** (con durata dell'impulso) oppure **Level** – secondo il tipo di zona della centrale.

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 NC, NO, EOL e DEOL con resistenza di fine linea da 2,2 kΩ; con i tipi DEOL è collegato anche il circuito antimanomissione.

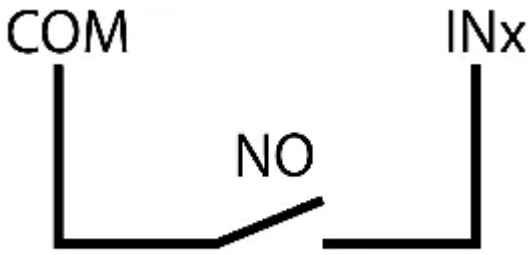


Figura 10. NO – circuito normalmente aperto: chiuso – allarme, aperto – stato di riposo.

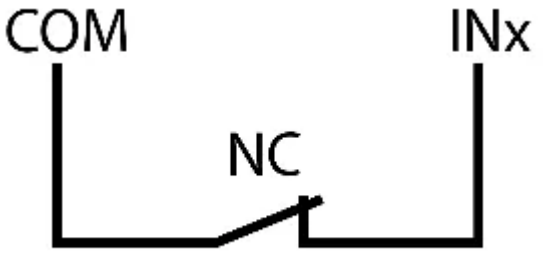


Figura 11. NC – circuito normalmente chiuso: aperto – allarme, chiuso – stato di riposo.

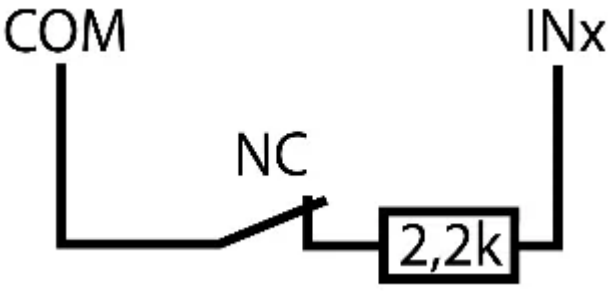


Figura 12. NC/EOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

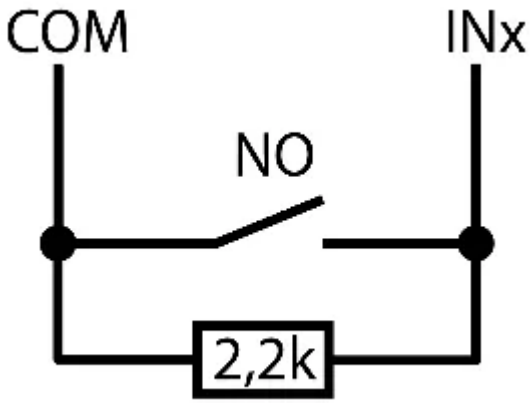


Figura 13. NO/EOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ: cortocircuito o interruzione – allarme, 2,2 kΩ – stato di riposo.

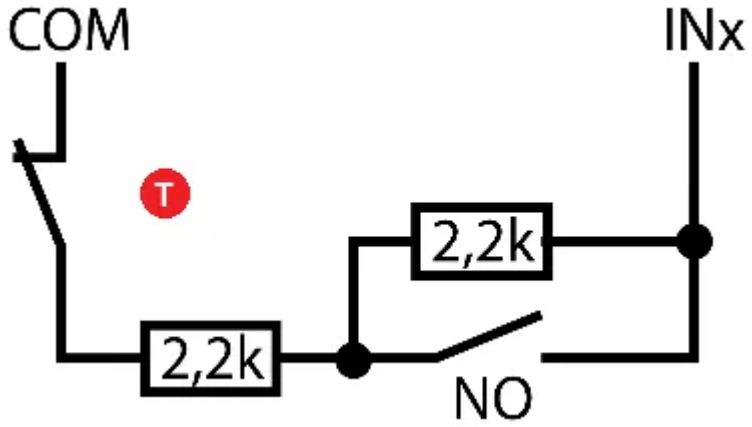


Figura 14. NO/DEOL – circuito normalmente aperto con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – allarme, 3,3–5,5 kΩ – stato di riposo.

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

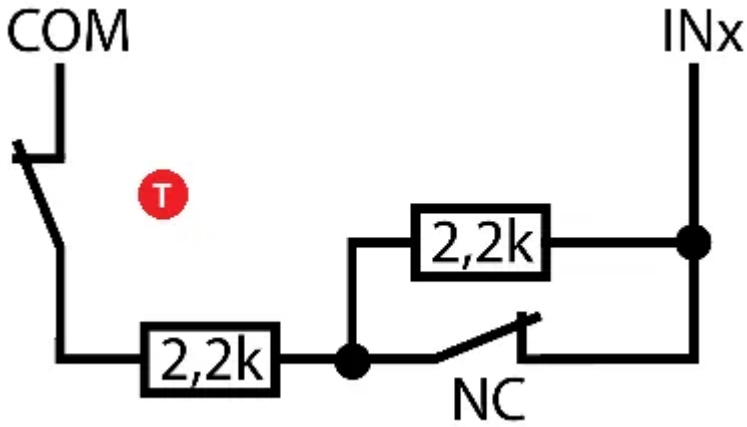


Figura 15. NC/DEOL – circuito normalmente chiuso con resistenza di fine linea da 2,2 kΩ e rilevamento della manomissione: cortocircuito o interruzione – manomissione, 2,2 kΩ – stato di riposo, 3,3–5,5 kΩ – allarme.

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

E16T precedente

I due ingressi (IN1, IN2) dell'E16T precedente (2 ingressi + OUT) accettano circuiti di tipo NO, NC o EOL; l'impostazione di fabbrica è NO. Lì il tipo di ingresso non si imposta nella pagina IN/OUT, ma nella pagina **Event summary** di TrikdisConfig (nota del paragrafo 6.6). Il collegamento è lo stesso: collega l'ingresso secondo il tipo scelto (NO, NC, EOL).

3.6 Collegamento del cavo Ethernet

Inserisci un'estremità del cavo Ethernet nella presa RJ45 sul circuito stampato dell'E16T e l'altra in una porta libera del router o dello switch. Serve un normale cavo dritto (patch); il cavo entra attraverso l'apertura superiore della scatola. Dopo l'accensione, l'avvenuta connessione alla rete è indicata dalla luce verde del LED **NETWORK**.

3.7 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. 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. Anche un LED di segnalazione può essere collegato direttamente all'uscita: da +DC, attraverso una resistenza in serie da 2,2 kΩ, al LED, e l'altro piedino del LED al morsetto I/O (nell'E16T precedente al morsetto OUT).

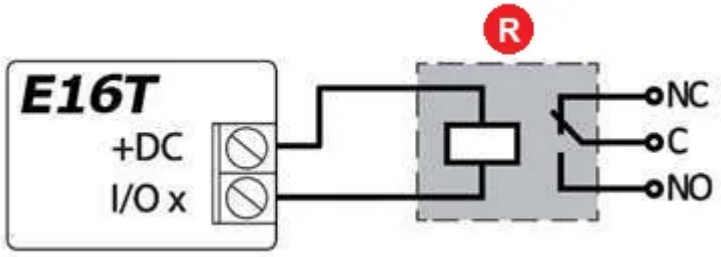


Figura 16. Collegamento di un relè all'uscita del comunicatore: la bobina va tra il morsetto +DC e il morsetto I/O x, i contatti (NC, C, NO) comandano il carico.

- R relè («Relay»)

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

3.8 Collegamento dell'espansione iO-8

Se servono più ingressi o uscite, al bus RS485 dell'E16T si possono collegare al massimo quattro espansioni **iO-8**; ognuna aggiunge 8 I/O a doppia funzione. Collega i morsetti A 485 e B 485 ai morsetti A e B del modulo e prendi l'alimentazione del modulo dai 12 V della centrale. Il bus RS485 può essere lungo al massimo 100 m – è un massimo teorico, vedi la nota del paragrafo 3.2. Il modulo va aggiunto nella pagina **RS485 modules** di TrikdisConfig (paragrafo 6.7). Allo stesso bus si possono collegare anche gli altri membri della serie iO (iO, iO-WL, iO-LO, LO-MOD); i moduli W485 ed E485 non sono destinati all'E16T, dato che l'E16T stesso è un dispositivo per Internet cablato.

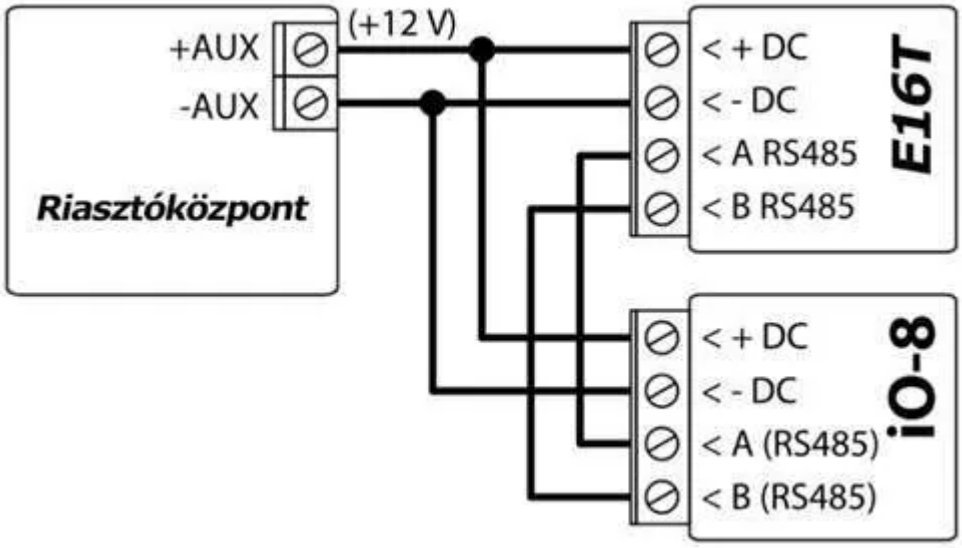


Figura 17. Collegamento dell'espansione iO-8 al bus RS485 dell'E16T; l'alimentazione è presa dall'uscita AUX della centrale d'allarme.

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 locale;
- **TROUBLE** spento.

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. Se nessun LED è acceso, controlla l'alimentazione e il cablaggio.

4. Programmazione della centrale d'allarme

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

1. **Attiva il comunicatore su linea telefonica (PSTN)** nella centrale.

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

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

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

4.1 Programmazione del combinatore Honeywell Vista

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

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

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

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

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

4.2 Centrali di altri produttori

Nel manuale d'installazione di ogni centrale cerca le stesse quattro impostazioni: abilitazione del comunicatore su linea telefonica, numero di telefono del ricevitore, modalità di composizione (DTMF) e formato di comunicazione (Contact ID). Se prima di comporre il numero la centrale attende il tono di linea (dial tone), lo fornisce l'E16T; se la chiamata comunque non parte, nella centrale disattiva il controllo del tono di linea (opzione «composizione senza tono di linea» o simile).

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

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.

5.1 Aggiunta del dispositivo

Prima di aggiungere il dispositivo verifica che:

1. L'E16T sia collegato alla rete e raggiunga Internet: il LED **NETWORK** è verde fisso e il LED **DATA** si spegne dopo un evento o un rapporto di prova.
2. Nella pagina **User reporting** → **PROTEGUS Cloud** di TrikdisConfig (paragrafo 6.4) sia spuntato **Enable connection** – cioè il cloud Protegus sia abilitato – 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.

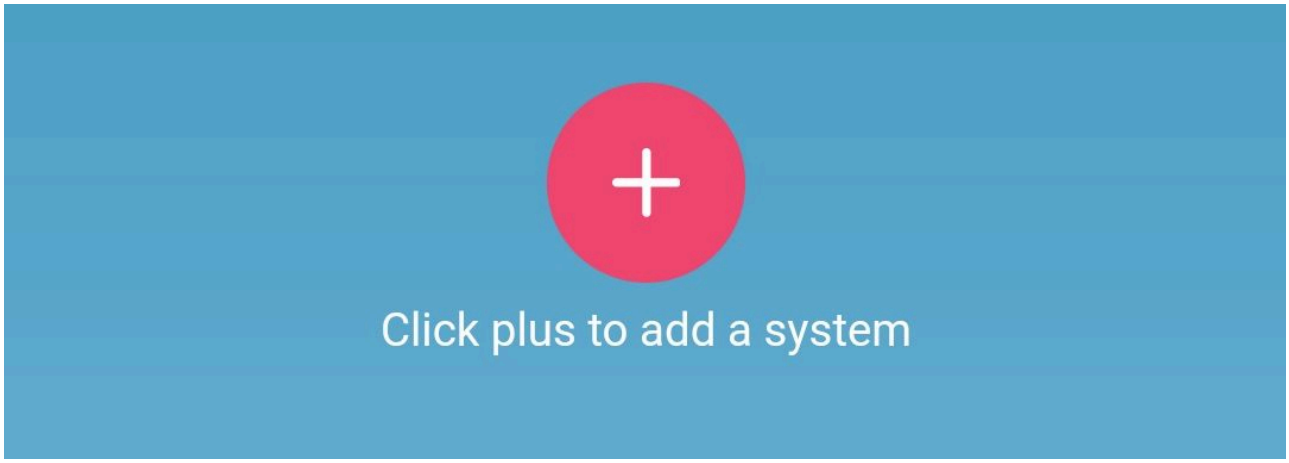
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è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



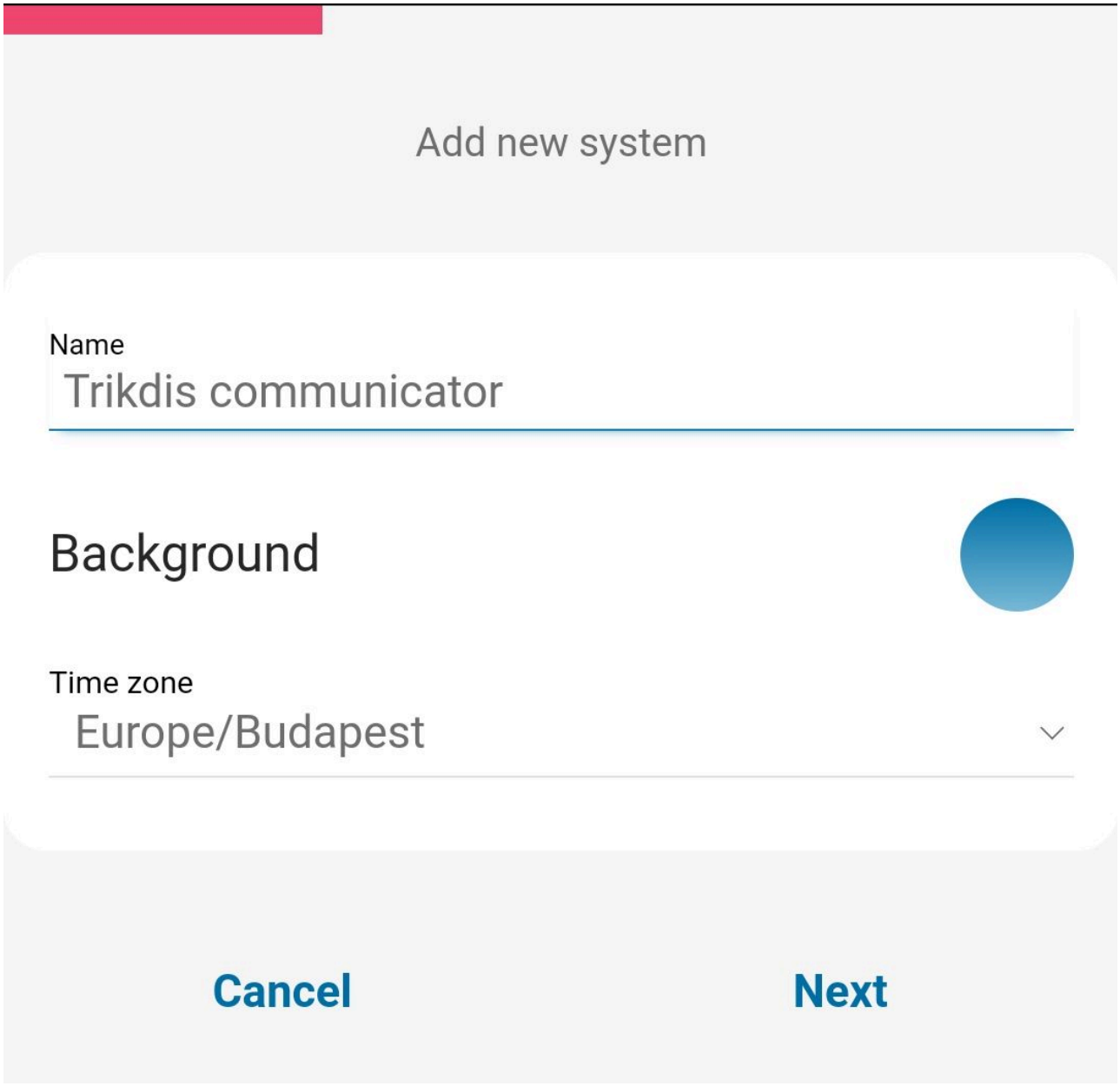
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



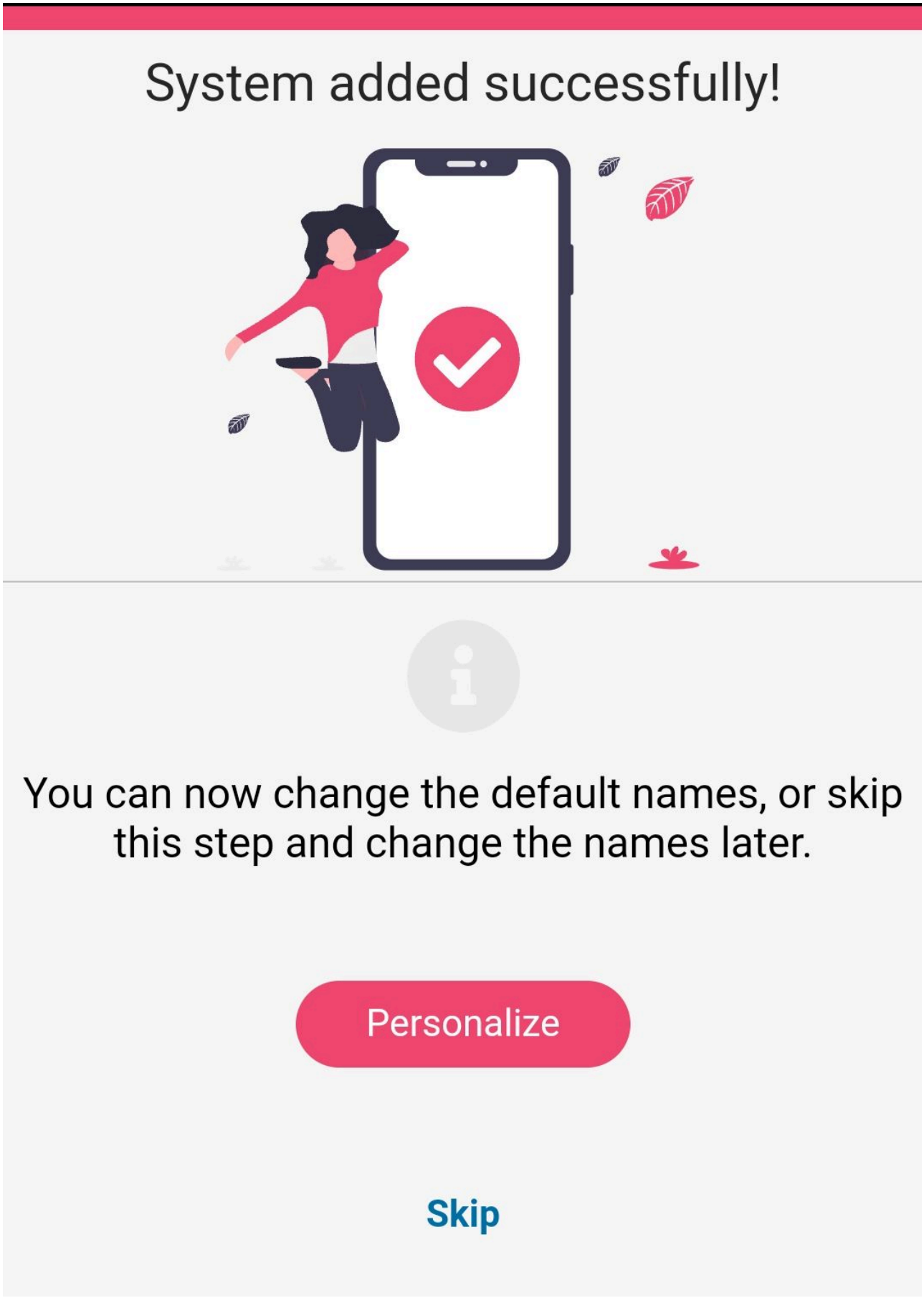
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



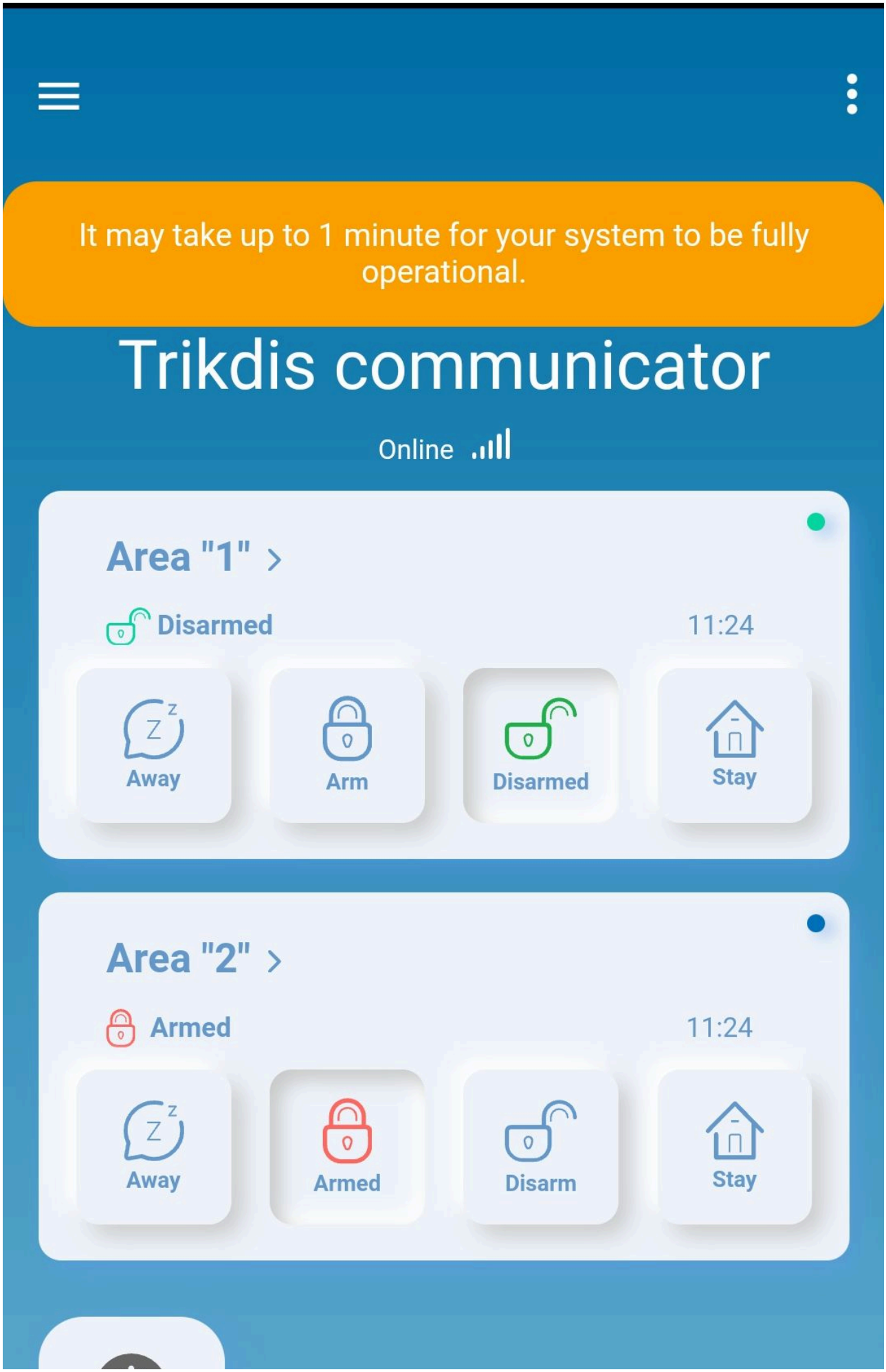
6. Add meg a rendszer nevét és válassz idozónát



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'E16T l'identificativo univoco del dispositivo è l'**indirizzo MAC**: è riportato sulla scatola e sul retro del dispositivo, e lo mostra anche TrikdisConfig (**MAC / Unique ID**).

5.2 Inserimento e disinserimento con un'uscita

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

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

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

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

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

5.3 Inserimento e disinserimento dall'app

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

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

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'E16T pagina per pagina.

6.1 La barra di stato

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

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

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



Figura 18. La barra di stato di TrikdisConfig con un E16T letto: a sinistra il pulsante di ripristino delle impostazioni di fabbrica e il MAC / Unique ID, in basso lo stato, il tipo, il numero di serie, le versioni, la modalità di connessione e il livello di accesso.

Dopo **Read [F4]** il programma legge e mostra le impostazioni presenti nel dispositivo; nel campo **Device** deve comparire il tipo del dispositivo (E16T; per la v2 **E16T_2000**). Esegui le impostazioni secondo le descrizioni delle pagine riportate di seguito.

6.2 System settings

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

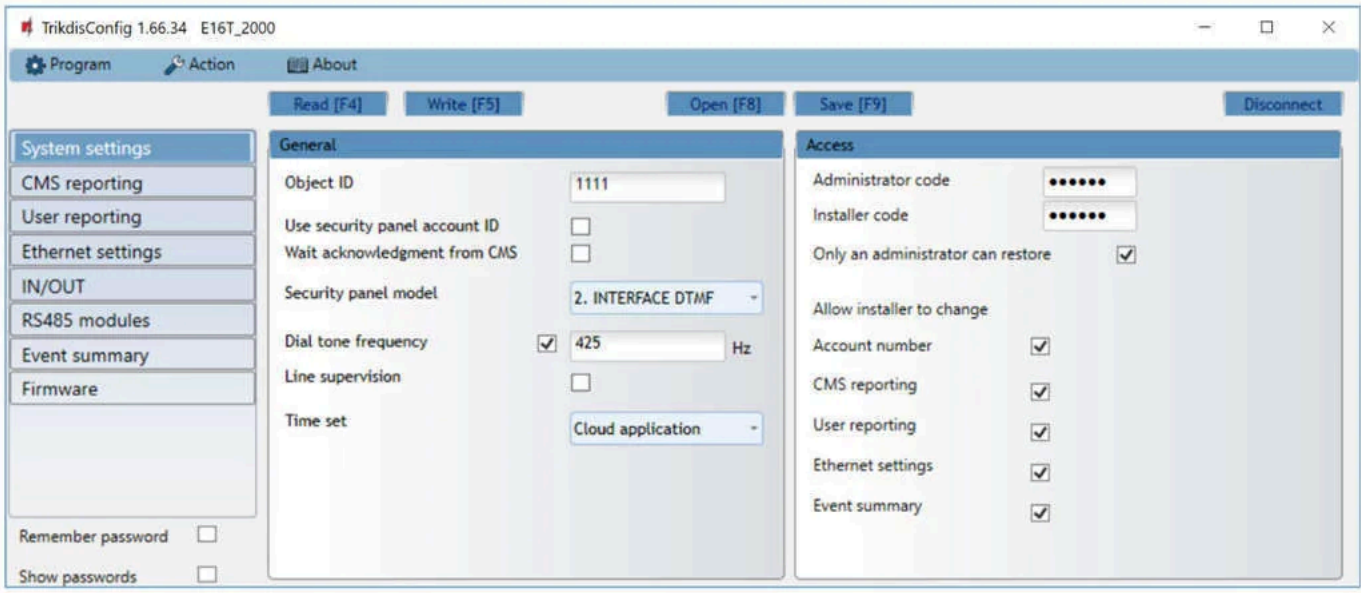


Figura 19. TrikdisConfig – pagina System settings: gruppi General e Access.

- **Object ID** – il codice d'impianto ricevuto dalla centrale di vigilanza (4 caratteri esadecimali: 0–9, A–F; `FFFE` e `FFFF` non possono essere usati). Obbligatorio se il dispositivo trasmette anche alla centrale di vigilanza.
- **Use security panel account ID** – se spuntato, il comunicatore non usa il proprio Object ID, ma il codice d'impianto inviato dalla centrale nel messaggio Contact ID. Utile se più aree trasmettono con codici separati.
- **Wait acknowledgment from CMS** – se spuntato, dopo ogni evento il comunicatore attende la conferma del ricevitore e solo dopo invia alla centrale il segnale di chiusura (kiss-off). Se la conferma non arriva, la centrale invia di nuovo l'evento. In un sistema senza centrale di vigilanza, solo con Protegus 2, lascialo disattivato (stato di fabbrica).
- **Security panel model** – il tipo di interfaccia della linea telefonica; predefinito **2. INTERFACE DTMF**. Con questa impostazione attivi o disattivi l'interfaccia della linea telefonica DTMF del comunicatore.
- **Dial tone frequency** – la frequenza del tono di linea che l'E16T fornisce alla centrale (predefinita 425 Hz, il tono di linea standard nella maggior parte dei paesi europei, Italia compresa).
- **Line supervision** – supervisione del cavo tra la centrale e il comunicatore; richiede anche il collegamento dei fili T-1 e R-1 (paragrafo 3.3.1).
- **Time set** – la fonte dell'orologio del dispositivo (predefinita **Cloud application**, il cloud Protegus).

E16T precedente

Nell'E16T precedente la pagina System settings contiene anche altri gruppi:

- **General** → **Test period** – il rapporto di test periodico viene inviato all'intervallo indicato qui (nella v2 si trova nella scheda **CMS reporting** → **Settings**).
- Gruppo **Ethernet settings** (nella v2 una pagina separata, paragrafo 6.5): **Internal MAC** – l'identificativo univoco del dispositivo, l'indirizzo MAC; **Use DHCP** – se spuntato, il dispositivo si registra automaticamente nella rete; se la registrazione automatica non riesce, compila manualmente i campi **Internal IP address**, **Mask** (subnet mask), **Gateway** e **DNS**.

- Gruppo **Output** (nella v2 la pagina IN/OUT, paragrafo 6.6): **OUT type** – il funzionamento dell'uscita, scelto dall'elenco: Disabled (disattivata), LAN OK (la rete funziona), Communication Trouble (guasto di comunicazione), Remote Control (comando a distanza dall'app Protegus); **Inverted** – se spuntato, l'uscita funziona al contrario; **OUT mode**: **Pulse** – l'uscita resta nel nuovo stato per il tempo indicato nel campo **Pulse Time** (secondi), **Level** – lo stato resta fino al comando successivo; **Pulse time** – la durata dell'impulso in secondi; in modalità Pulse l'uscita si attiva per questo tempo.

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.

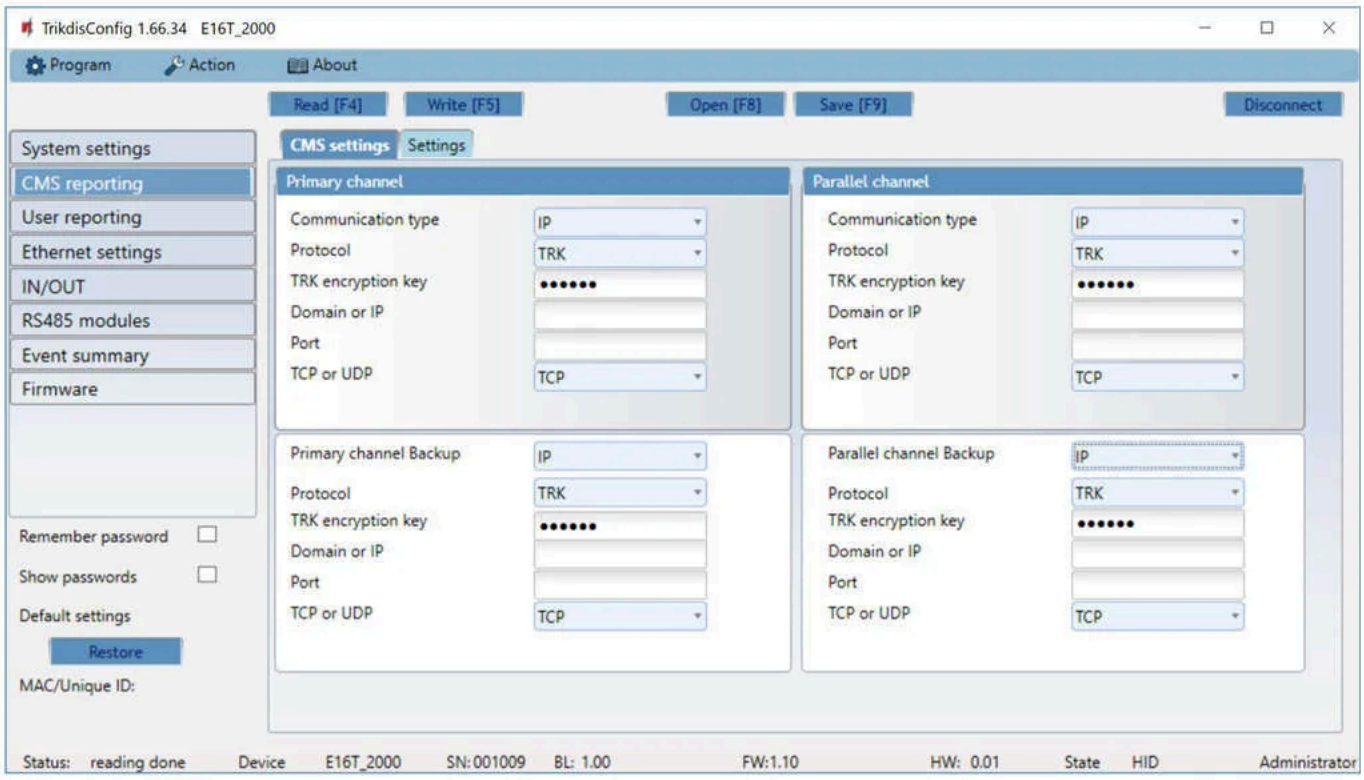


Figura 20. TrikdisConfig – CMS reporting, scheda CMS settings: canale principale, di riserva e parallelo.

Primary channel – canale principale

- **Communication type** – con l'E16T si può scegliere solo **IP**.
- **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 del ricevitore (nome di dominio o indirizzo IP) e il suo numero di porta di rete.
- **TCP or UDP** – il protocollo di trasmissione con cui invia gli eventi (secondo l'impostazione del ricevitore).

Primary channel Backup – canale di riserva. Subentra nella comunicazione se il canale principale non funziona; le sue impostazioni sono le stesse descritte sopra. Conviene impostarlo anche con un dispositivo cablato – ad esempio con il secondo indirizzo o la seconda porta del ricevitore –, perché il canale di riserva supera anche un guasto lato ricevitore.

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.

E16T precedente

Nell'E16T precedente TrikdisConfig mostra le stesse cose nella scheda **CMS Reporting** della finestra **Reporting**, con nomi di campo diversi:

- Gruppo **Primary**: **Enable** – se spuntato, il canale principale verso la centrale di vigilanza è attivo; **Remote Host** – il nome di dominio o l'indirizzo IP del ricevitore; **Remote Port** – il numero di porta di rete del ricevitore; **TCP or UDP** – il protocollo di trasmissione; **PING Time** – attivalo e indica il tempo tra i segnali di esistenza in vita (valore di fabbrica 30) – serve per la supervisione della connessione; **Encryption key** – chiave di cifratura a 6 cifre, la stessa nel comunicatore e nel ricevitore.

- Gruppo **Backup**: **Enable** – attiva il canale di riserva, che invia se la connessione principale si interrompe; gli altri campi sono gli stessi del canale principale.
- Gruppo **Settings**: **TCP protocol** – la codifica dell'invio: TRK (per un ricevitore Trikdis), DC-09_2007 o DC-09_2012 (per un ricevitore universale).
- Gruppo **SIA IP parameter** – modificabile solo se nel campo **TCP protocol** c'è DC-09_2007 o DC-09_2012: **Encryption enabled** – con DC-09_2012 si può attivare la cifratura; **DC09-2012 encryption key** – la chiave di cifratura impostata nel ricevitore; **DC09-2012 receiver No.** – il numero del ricevitore; **DC-09 line No.** – il numero di linea del ricevitore; **Use time stamp** – se spuntato, il messaggio contiene anche l'ora (marca temporale).

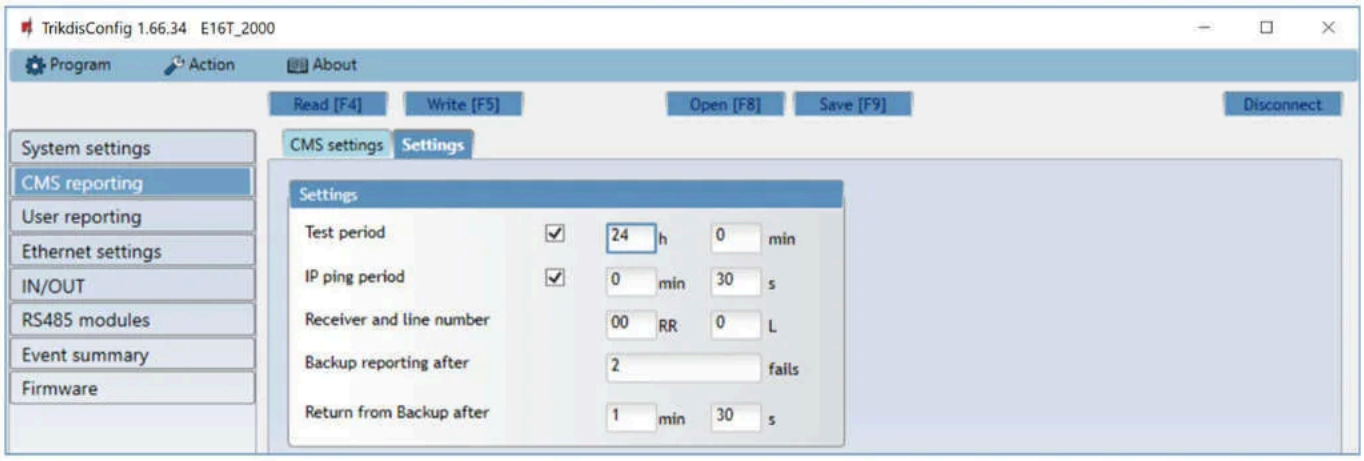


Figura 21. TrikdisConfig – CMS reporting, scheda Settings: rapporto di test, PING, numero di ricevitore e di linea (Receiver and line number: RR = numero del ricevitore, L = numero di linea) e temporizzazioni del canale di riserva.

Nella scheda **Settings** imposti le temporizzazioni e il numero di ricevitore e di linea; il gruppo DC-09 serve solo se invii con il protocollo DC-09 (nella schermata del 2022 non è ancora visibile).

- **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.

6.4 User reporting

Nella scheda **PROTEGUS Cloud** abiliti il servizio Protegus. L'E16T non ha notifiche né comando via SMS, quindi in questa pagina c'è solo questa scheda.

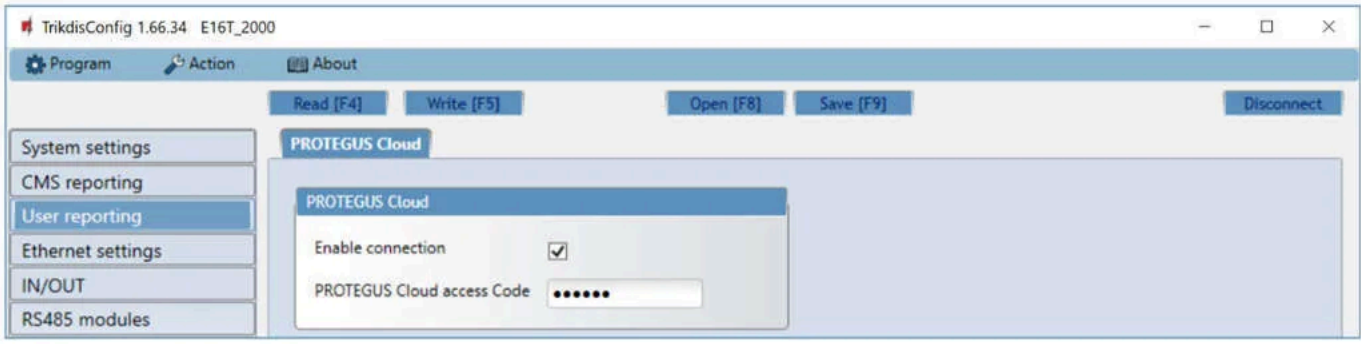


Figura 22. TrikdisConfig – User reporting, scheda PROTEGUS Cloud.

- **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`). Se lo hai cambiato, va inserito quando aggiungi il sistema in Protegus 2. 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'E16T si collega alla rete locale.



Figura 23. TrikdisConfig – pagina Ethernet settings; di fabbrica è attivo il DHCP.

- **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.

Nell'E16T precedente l'indirizzo MAC è mostrato nel campo **Internal MAC** del gruppo Ethernet settings della pagina **System settings** (nota del paragrafo 6.2).

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).

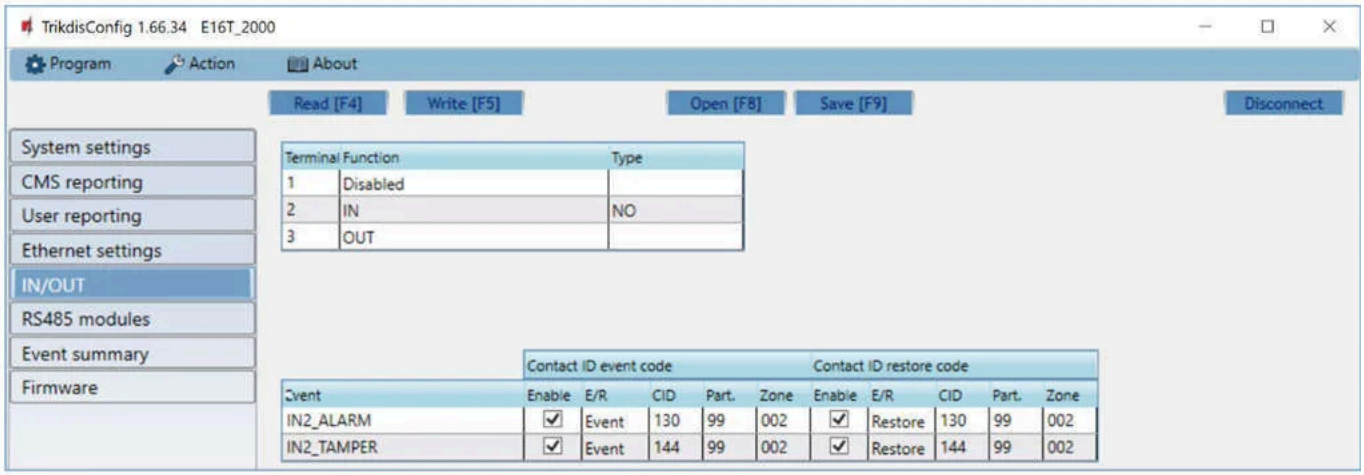


Figura 24. TrikdisConfig – pagina IN/OUT: funzione dei morsetti I/O ed eventi degli ingressi.

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.
- **Part.** – il numero di area nel messaggio.
- **Zone** – il numero di zona nel messaggio.

E16T precedente

Nell'E16T precedente non c'è la pagina IN/OUT: il tipo e gli eventi dei due ingressi si impostano nel gruppo **Input description** della pagina **Event summary**. **Partition** – il numero di area; **Contact ID** – il codice evento (può restare il valore di fabbrica); quando l'ingresso viene violato, invia questo codice a Protegus e alla centrale di vigilanza; **Zone No.** – il numero di zona, che viene inviato nei messaggi; **Type** – il tipo di ingresso (NO, NC, EOL); **Enable / Alarm** – se spuntato, trasmette quando l'ingresso viene violato (evento); **Enable / Restore** – se spuntato, trasmette quando l'ingresso torna a riposo. L'impostazione dell'uscita si trova nel gruppo **System settings** → **Output** (nota del paragrafo 6.2).

6.7 RS485 modules

Le espansioni iO-8 e le altre espansioni della serie iO collegate al bus RS485 vanno aggiunte nella scheda **Modules list**.

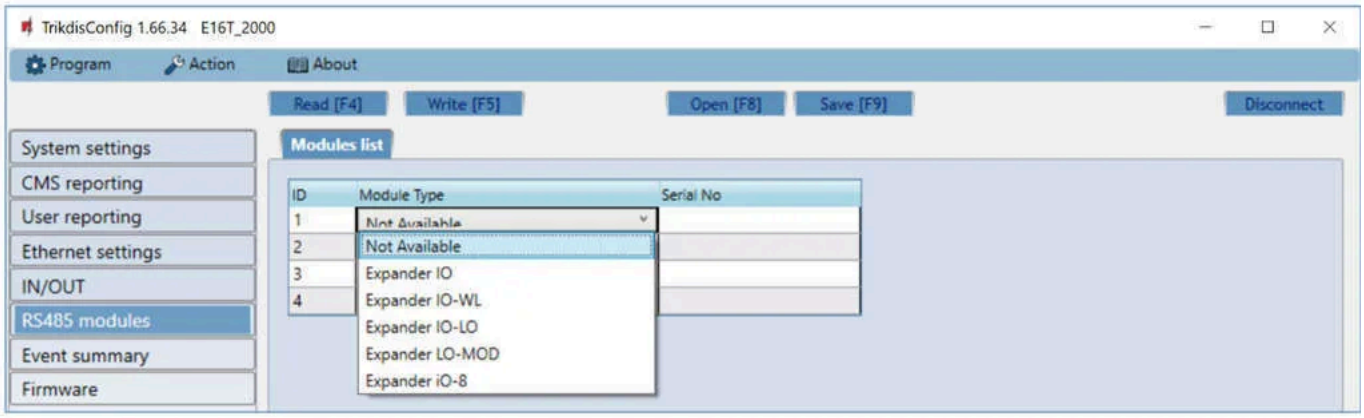


Figura 25. TrikdisConfig – RS485 modules, scheda Modules list: i tipi di modulo selezionabili.

- **Module Type** – il tipo di modulo collegato, scelto dall'elenco (Expander iO-8, IO, IO-WL, IO-LO, LO-MOD).
- **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.

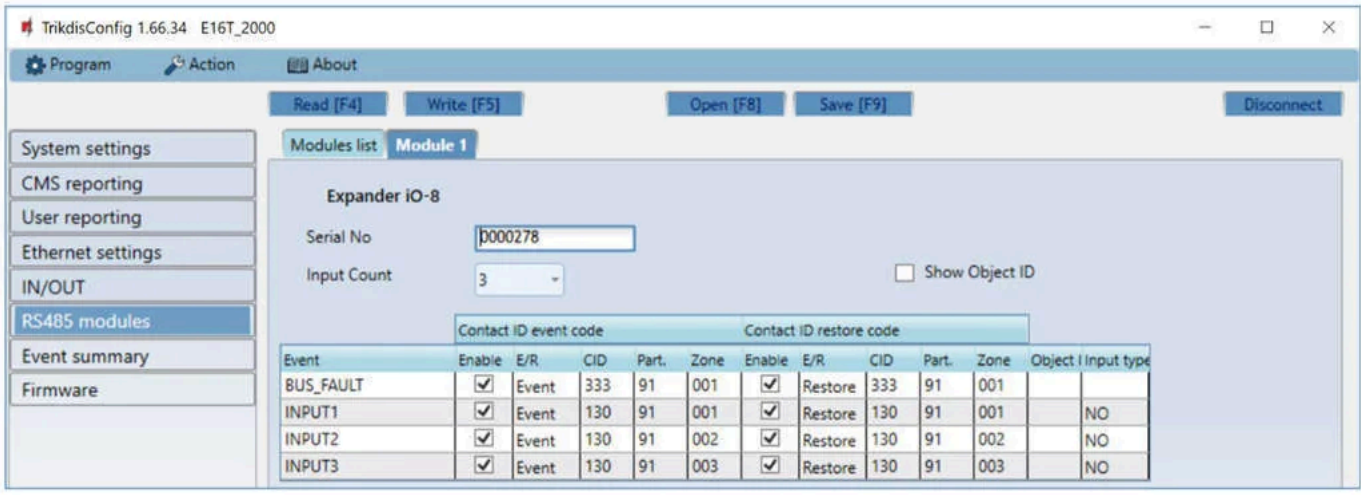


Figura 26. TrikdisConfig – RS485 modules, scheda del modulo iO-8.

- **Input Count** – quanti morsetti devono essere ingressi; gli altri saranno uscite. Il tipo di ingresso (**Input type**: NO o NC) si imposta nella tabella. Il ruolo delle uscite (inserimento / disinserimento o comando di un dispositivo) 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).
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**.

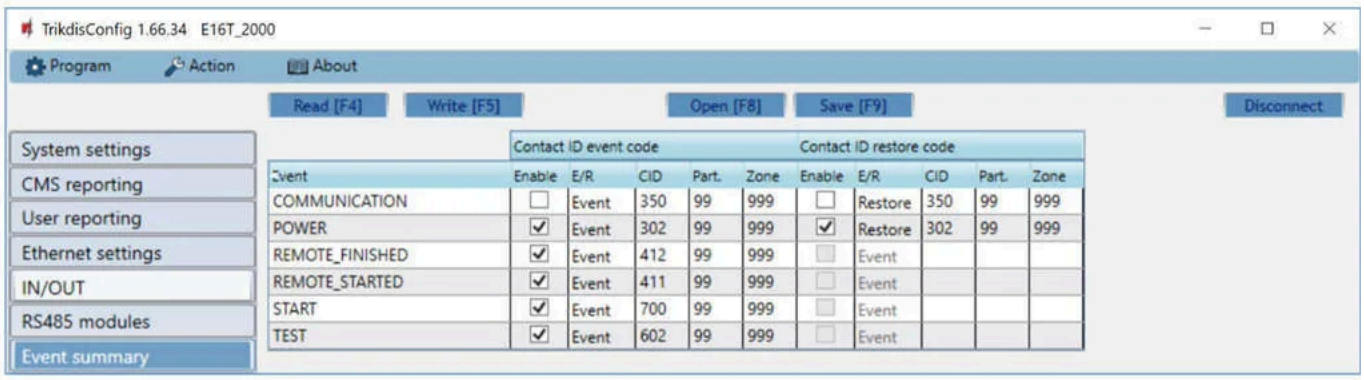


Figura 27. TrikdisConfig – pagina Event summary: i messaggi interni del dispositivo.

Nell'E16T precedente anche l'impostazione degli ingressi si trova in questa pagina (nota del paragrafo 6.6).

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.

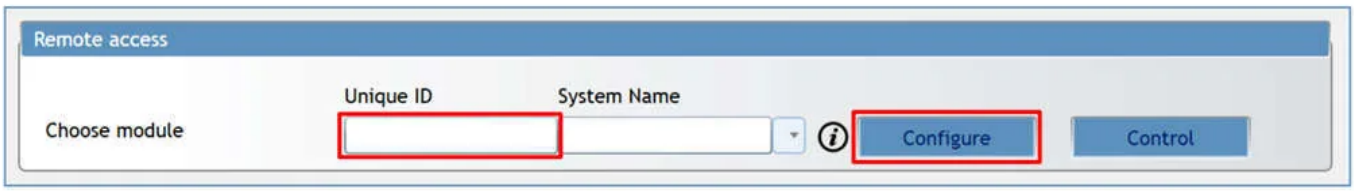


Figura 28. TrikdisConfig – Remote access: l'identificativo del dispositivo (con l'E16T l'indirizzo MAC), il nome del sistema e il pulsante Configure.

L'abilitazione del servizio Protegus è descritta nel paragrafo 6.4, il download di TrikdisConfig nel paragrafo 2.1.

8. Verifica del funzionamento del comunicatore

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

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

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

9. Aggiornamento del firmware

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

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

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

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

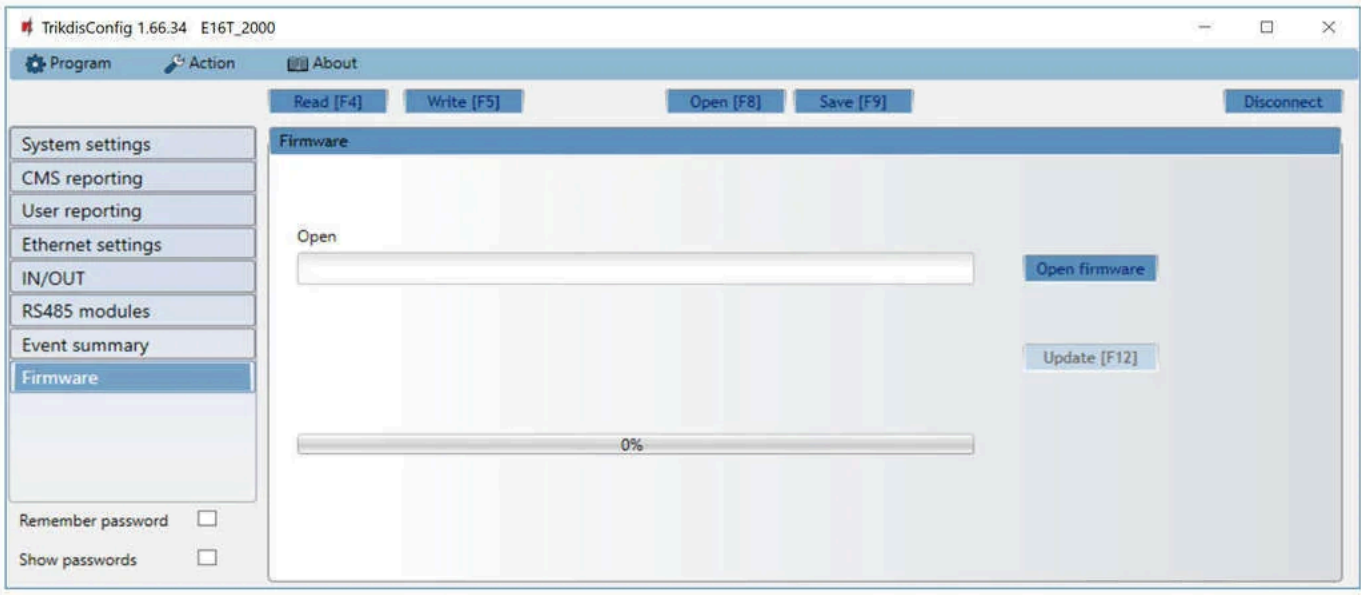


Figura 29. TrikdisConfig – pagina Firmware: Open firmware e Update [F12].

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

10. Risoluzione dei problemi e domande frequenti

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

Il LED NETWORK è spento – non c'è rete

1. Osserva i lampeggi del LED **TROUBLE**: 1 = nessun collegamento fisico, 2 = non ha ottenuto un indirizzo IP (DHCP), 3 = errore DNS.
2. **Con 1 lampeggio** controlla il cavo e i connettori (se l'RJ45 è inserito fino allo scatto), la porta del router o dello switch (se è attiva, se non è disabilitata), e prova un altro cavo o un'altra porta.
3. **Con 2 lampeggi** nella rete il server DHCP manca o non risponde: attivalo sul router, oppure assegna al dispositivo un indirizzo IP fisso, una subnet mask e un gateway nella pagina **Ethernet settings** (paragrafo 6.5).
4. **Con 3 lampeggi** la risoluzione dei nomi non funziona: controlla i campi DNS 1 / DNS 2 (di fabbrica il DNS pubblico di Google) e che la rete consenta il traffico DNS in uscita.

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 e la porta del ricevitore, l'impostazione TCP/UDP e la chiave di cifratura (**CMS reporting**).
2. Se il ricevitore è indicato con un nome di dominio, controlla l'impostazione DNS (**Ethernet settings**).
3. Con un indirizzo IP fisso controlla il gateway (**Default gateway**): con un gateway errato il dispositivo raggiunge la rete locale, ma non Internet.
4. In una rete aziendale o filtrata il firewall può bloccare la connessione in uscita verso la porta del ricevitore – concordalo con l'amministratore di rete (paragrafo 3.2).

La centrale non invia gli eventi al comunicatore

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

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 esattamente, dalla scatola o dal retro del dispositivo – oppure scansiona con l'app il codice QR dell'etichetta, così non si può sbagliare a digitarlo.
4. La connessione Internet deve funzionare: il LED NETWORK è verde e il LED DATA si spegne dopo un evento. Per raggiungere il cloud Protegus serve anche un DNS funzionante (**Ethernet settings**).

Non riesco ad accedere a distanza con TrikdisConfig

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

Ho dimenticato la password

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

Servono un indirizzo IP fisso o l'inoltro delle porte sul router?

No. L'E16T avvia da sé la connessione in uscita verso il ricevitore e il cloud Protegus, quindi non servono né un indirizzo IP pubblico fisso, né un DNS dinamico, né l'inoltro delle porte. Nella rete locale va bene anche l'indirizzo ottenuto tramite DHCP; assegna un indirizzo locale fisso solo se nella rete non c'è un DHCP o se lo richiede l'amministratore di rete (paragrafo 6.5).

Funziona in Wi-Fi?

No: l'E16T conosce solo la connessione di rete cablata (RJ45). Se vicino alla centrale non c'è un cavo di rete, si può realizzare un ponte Wi-Fi fino al router, oppure scegli il comunicatore per rete mobile G16T.

Che cosa succede durante un'interruzione di corrente?

Il comunicatore è alimentato dalla batteria della centrale, ma se il router e il modem restano senza corrente non c'è Internet e gli eventi attendono in memoria (il LED DATA è acceso). Il dispositivo li invia quando Internet ritorna. Se l'interruzione non è accettabile, la soluzione è un gruppo di continuità per i dispositivi di rete oppure un comunicatore per rete mobile (paragrafo 3.2).

11. Norme di sicurezza

Figyelem!

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

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

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

- L'installazione e la manutenzione delle apparecchiature di sicurezza possono essere eseguite solo da un installatore qualificato.
- Prima dell'installazione leggi attentamente il manuale; ignorare le istruzioni può causare malfunzionamenti o guasti.
- Prima del collegamento, 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

- Inserimento a distanza con zona chiave dall'app Protegus 2 – i dettagli e le insidie dell'inserimento con zona chiave.
- Documentazione in inglese: docs.trikdis.com.

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

Prodotti correlati

Trikdis E16T Ethernet comunicatore universale - modulo IP

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-e16t