mobilamb
TRIKDIS Official Distributor

Comunicatore antincendio G17F – manuale di installazione e programmazione

Manuale di installazione e programmazione del comunicatore antincendio su rete mobile Trikdis G17F (EN 54-21): collegamento alle uscite o al bus RS485 della centrale antincendio (ESPA 4.4.4, NSC Solution, INIM Smartline, C-TEC Cast ZFP), configurazione in TrikdisConfig, centrale di vigilanza, Protegus 2, controllo via SMS e con chiamata.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-g17f

Indice

1. Panoramica

1.1 A cosa serve, come funziona
1.2 Varianti
1.3 Dati tecnici
1.4 Le parti del dispositivo
1.5 I morsetti
1.6 LED di segnalazione
1.7 Strumenti necessari per l'installazione

2. Configurazione rapida con il software TrikdisConfig

2.1 Configurazione per l'app Protegus 2
2.2 Configurazione per la centrale di vigilanza

3. Installazione e collegamenti

3.1 Fissaggio e inserimento della scheda SIM
3.2 Collegamento alle uscite della centrale antincendio
3.3 Centrale antincendio a protocollo ESPA 4.4.4
3.4 Centrale antincendio NSC Solution
3.5 Centrale antincendio INIM Smartline
3.6 Centrale antincendio C-TEC Cast ZFP
3.6.1 Configurazione della centrale C-TEC (ZFPtools)
3.7 Collegamento degli ingressi
3.8 Moduli di espansione della serie iO
3.9 Modulo di espansione iO-8
3.10 Moduli di espansione della serie LORA
3.11 Modulo Wi-Fi W485
3.12 Modulo Ethernet E485
3.13 Accensione del comunicatore

4. Controllo a distanza

4.1 Aggiunta del G17F a Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.2 Configurazione e controllo con messaggio SMS
4.3 Controllo delle uscite PGM con chiamata telefonica

5. Le pagine di TrikdisConfig

5.1 La barra di stato
5.2 Pagina „System Options”
5.3 Pagina „Reporting to CMS”
5.4 Pagina „Users & Reporting”
5.5 Pagina „Modules”
5.6 Pagina „Zones”
5.7 Pagina „PGM”
5.8 Pagina „System events”
5.9 Pagina „Events Log”
5.10 Ripristino delle impostazioni di fabbrica

6. Programmazione a distanza

7. Verifica del funzionamento

8. Aggiornamento del firmware

9. Risoluzione dei problemi e domande frequenti

10. Norme di sicurezza

Vedi anche

1. Panoramica

Il **G17F** è un comunicatore antincendio con cui gli eventi di qualsiasi unità o centrale di rivelazione incendio possono essere trasmessi tramite rete mobile. Quando un ingresso (zona) viene violato, cioè arriva un allarme incendio, l'evento viene trasmesso alle destinazioni impostate, per esempio ai vigili del fuoco e alla centrale di vigilanza. Inoltre anche il proprietario riceve la notifica dell'evento nell'app mobile e web **Protegus 2**.

Il G17F trasmette i messaggi della centrale antincendio tramite la rete mobile. **Principio di funzionamento:** quando un ingresso (zona) del comunicatore viene violato, il G17F invia tramite Internet mobile un messaggio di evento al ricevitore della centrale di vigilanza o all'app Protegus 2; inoltre può inviare anche SMS e avviare chiamate telefoniche. Il comunicatore è disponibile con modem 2G o 4G. Le impostazioni si eseguono con il software **TrikdisConfig**, tramite cavo USB o a distanza.

Certificazione	Dato
Norma	Il G17F è conforme ai requisiti della norma **EN 54-21:2006** e soddisfa i requisiti prestazionali previsti nell'allegato A della EN 54-21 per i sistemi di trasmissione di **tipo 1**.
Certificato	**1922-CPR-1974** – Sistemi di rivelazione e di segnalazione d'allarme incendio. Apparecchiature di trasmissione allarme e segnalazione guasti.
Organismo di certificazione	Organismo notificato di certificazione di prodotto No. 1922 „Dedal" – Nesebar, Mladost str. 50, 8230 Bulgaria
Assistenza tecnica Trikdis	support@trikdis.lt, +37067422877

1.1 A cosa serve, come funziona

Collegamento con la centrale antincendio

- Collegato alle uscite della centrale: le uscite di stato della centrale (allarme, guasto ecc.) si collegano agli ingressi del G17F (punto 3.2).
- Tramite bus RS485: con centrali antincendio a protocollo **ESPA 4.4.4**, **NSC Solution**, **INIM Smartline** e **C-TEC Cast ZFP** (punti 3.3–3.6).

Messaggi alla centrale di vigilanza

- Invia gli eventi ai ricevitori software e hardware di Trikdis, che funzionano con qualsiasi software di centrale di vigilanza.
- Può inviare eventi anche a ricevitori SIA DC-09.
- Se la connessione sul canale principale si interrompe, i messaggi vanno automaticamente al ricevitore di riserva.
- Può segnalare gli eventi alla centrale di vigilanza anche via SMS – è estremamente utile, perché funziona anche quando nella rete dell'operatore mobile la connessione IP cade.
- Riconosce il disturbo della rete mobile (jamming).
- Può segnalare contemporaneamente alla centrale di vigilanza e inviare all'app Protegus 2; all'invio alla centrale di vigilanza si può dare la precedenza.
- Invia i messaggi di evento con codici Contact ID.

Messaggi agli utenti

- Chiama i numeri di telefono scelti (fino a 8 utenti).
- Invia SMS sugli eventi.
- Invia notifiche push e notifiche di evento con suono speciale all'app Protegus 2.

Controllo a distanza delle uscite

- dall'app Protegus 2;
- chiamando il numero di telefono del dispositivo;
- con un messaggio SMS.

Configurazione e installazione

- Configurazione con cavo USB o a distanza, con il software TrikdisConfig.
- Aggiornamento del firmware a distanza.
- Due livelli di accesso (tipi di account) alle impostazioni: installatore e amministratore.

Ingressi e uscite

- 3 ingressi, tipo selezionabile: NO, NC, EOL (4,7 kΩ, 10 kΩ).
- 3 morsetti a doppia funzione, impostabili come ingresso (IN) o uscita (OUT); come ingresso tipo selezionabile: NO, NC, EOL (4,7 kΩ, 10 kΩ).
- Bus RS485 per i moduli di espansione della serie iO.
- Con i moduli di espansione della serie iO il numero degli ingressi (IN) o delle uscite (OUT) può arrivare a 12.

1.2 Varianti

Il G17F è disponibile in due varianti di rete mobile: con modem 2G o 4G. Questo manuale vale per entrambe; la differenza sta nel modem e nelle bande della rete mobile.

Variante	Modem	Bande
G17F-4G	4G (LTE)	700 / 800 / 900 / 1800 / 2100 / 2600 MHz
G17F-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis G17F 4G GSM / IP comunicatore antincendio

Trikdis G17F 2G GSM / IP comunicatore antincendio

A causa del graduale spegnimento delle reti 2G, per le nuove installazioni consigliamo la variante 4G.

1.3 Dati tecnici

Caratteristica	Valore
Bande del modem 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Bande del modem 4G (LTE)	700 / 800 / 900 / 1800 / 2100 / 2600 MHz
Tensione di alimentazione	9–32 V DC
Assorbimento	100 mA

Caratteristica	Valore
Protocollo di trasmissione	TRK, SIA DC-09_2007, SIA DC-09_2012
Chiave di cifratura	6 caratteri
Collegamento con la centrale di vigilanza	TCP/IP o UDP/IP, SMS
Codici evento	Contact ID
Memoria dei messaggi	fino a 60 messaggi
Ingressi e uscite	3 ingressi: NO, NC, EOL (4,7 kΩ, 10 kΩ); 3 morsetti a doppia funzione (IN/OUT): come ingresso NO, NC, EOL (4,7 kΩ, 10 kΩ), come uscita a collettore aperto (OC), al massimo 100 mA
Registro eventi	fino a 1000 eventi
Configurazione	a distanza con il software TrikdisConfig o in loco con cavo USB Mini-B; a distanza con messaggi SMS
Lunghezza del bus RS485	al massimo 100 m
Moduli supportati	modulo di espansione **iO**; **iO-WL** – **iO-MOD** – ricetrasmettitore radio iO-WL; modulo di espansione **iO-8**; modulo Ethernet **E485**; modulo Wi-Fi **W485 (W17u)**; modulo di espansione **iO-LORA**; modulo di espansione **iO8-LORA**; pulsante antipanico **PB-LORA**; modulo di espansione **REL-LORA**; centrali antincendio **INIM Smartline**, **NSC Solution** e **C-TEC Cast ZFP**; centrale antincendio a protocollo **ESPA 4.4.4**
Ambiente operativo	–10 … +50 °C, umidità relativa al massimo 80 % a +20 °C
Dimensioni	92 × 62 × 25 mm
Peso	80 g

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.

1.4 Le parti del dispositivo

I numeri della figura indicano le parti del dispositivo: a sinistra il pannello frontale, a destra il circuito stampato con il pannello frontale rimosso.

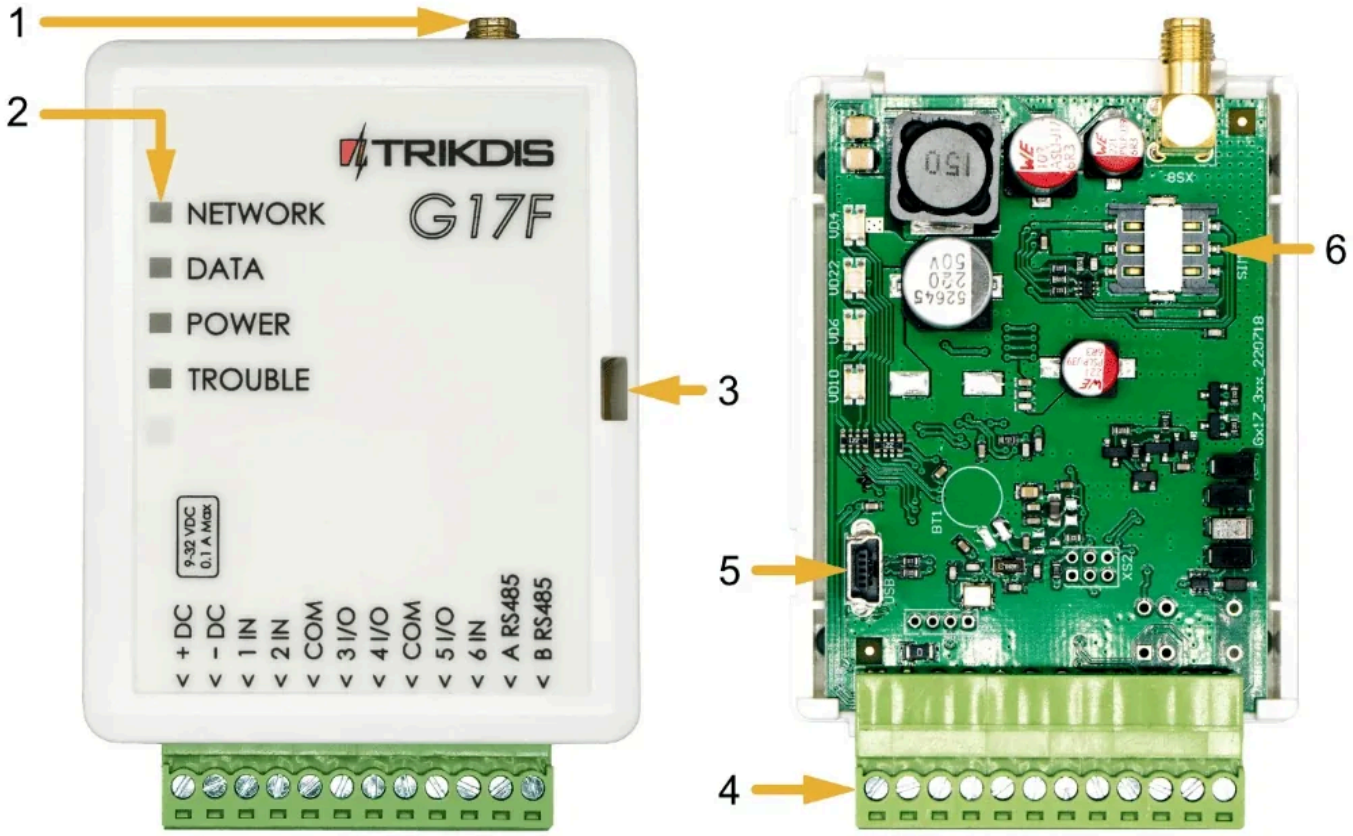


Figura 1. Le parti del G17F.

- 1 connettore SMA dell'antenna di rete mobile
- 2 LED di segnalazione
- 3 fessura per rimuovere il pannello frontale
- 4 morsettiera per il collegamento dei cavi
- 5 connettore USB Mini-B per la programmazione
- 6 alloggiamento della scheda nano-SIM

1.5 I morsetti

I nomi dei morsetti si leggono sul pannello frontale, sopra la morsettiera (da sinistra a destra).

Morsetto	Funzione
+DC	alimentazione: polo positivo 9–32 V DC
–DC	alimentazione: polo negativo 9–32 V DC
1 IN	ingresso 1, tipo selezionabile: NO, NC, EOL (di fabbrica EOL, 10 kΩ)
2 IN	ingresso 2, tipo selezionabile: NO, NC, EOL (di fabbrica EOL, 10 kΩ)
COM	morsetto comune (negativo)
3 I/O	morsetto 3 a doppia funzione (IN/OUT): come ingresso NO, NC, EOL (di fabbrica EOL, 10 kΩ), come uscita a collettore aperto (OC), al massimo 100 mA
4 I/O	morsetto 4 a doppia funzione (IN/OUT): come ingresso NO, NC, EOL (di fabbrica EOL, 10 kΩ), come uscita a collettore aperto (OC), al massimo 100 mA
COM	morsetto comune (negativo)
5 I/O	morsetto 5 a doppia funzione (IN/OUT): come ingresso NO, NC, EOL (di fabbrica EOL, 10 kΩ), come uscita a collettore aperto (OC), al massimo 100 mA

Morsetto	Funzione
6 IN	ingresso 6, tipo selezionabile: NO, NC, EOL (di fabbrica EOL, 10 kΩ)
A RS485, **B RS485**	bus RS485: per collegare moduli di espansione iO, centrali antincendio INIM Smartline, NSC Solution e C-TEC Cast ZFP, centrali antincendio a protocollo ESPA 4.4.4, nonché i moduli E485 e W485

1.6 LED di segnalazione

LED	Luce	Significato
NETWORK	spento	non connesso alla rete mobile
	verde fisso e giallo lampeggiante	connesso alla rete mobile; il numero di lampeggi gialli indica il livello del segnale: su rete 2G (GPRS) bastano già 5 lampeggi, su rete 4G 3 lampeggi
DATA	verde, fisso	invio di un messaggio in corso
	giallo, fisso	nella memoria ci sono eventi non inviati
POWER	verde lampeggiante	la tensione di alimentazione è adeguata
	giallo lampeggiante	la tensione di alimentazione non è adeguata
	verde e giallo lampeggianti	modalità di configurazione
TROUBLE	spento	nessun guasto di funzionamento
	1 lampeggio	nessuna scheda SIM
	2 lampeggi	il codice PIN della scheda SIM è errato
	3 lampeggi	non riesce a connettersi alla rete mobile
	4 lampeggi	non riesce a connettersi al ricevitore IP sul canale principale
	5 lampeggi	non riesce a connettersi al ricevitore IP sul canale di riserva
	6 lampeggi	l'orologio interno del G17F non è impostato
	7 lampeggi	la tensione di alimentazione non è adeguata
	9 lampeggi	errore nella comunicazione con il modulo RS485

La segnalazione corretta dopo l'accensione e la valutazione del livello del segnale sono descritte al punto 3.13.

1.7 Strumenti necessari per l'installazione

Prima di iniziare l'installazione verifica di avere tutto a portata di mano:

1. cavo USB Mini-B per la configurazione;
2. cavo con almeno 4 conduttori per collegare il G17F alla centrale antincendio;
3. cacciavite a taglio da 2,5 mm;
4. antenna esterna per rete mobile, se sul posto il segnale è debole;
5. scheda nano-SIM attivata (la richiesta del PIN si può disattivare);
6. il manuale della centrale antincendio a cui colleghi il G17F.

Gli accessori elencati vanno acquistati a parte – ordinali dal tuo rivenditore. Se sul posto il segnale è debole, usa un'antenna esterna con cavo, che si può posizionare all'esterno:

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

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

2. Configurazione rapida con il software TrikdisConfig

Questo capitolo descrive le impostazioni con cui il G17F invia gli eventi all'app Protegus 2 (punto 2.1) o alla centrale di vigilanza (punto 2.2). Le altre impostazioni del G17F sono nel capitolo 5.

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!

1. Con un cacciavite a taglio rimuovi il pannello frontale del G17F come mostrato nella figura.



Figura 2. Rimozione del pannello frontale: inserendo il cacciavite nella fessura laterale e spingendolo verso il basso, il coperchio si sgancia; sotto c'è il connettore USB Mini-B.

2. Collega il G17F al computer con un cavo **USB Mini-B**.
3. Avvia TrikdisConfig. Il programma riconosce automaticamente il dispositivo collegato e apre la finestra di programmazione del G17F.
4. Fai clic sul pulsante **Read [F4]**: il programma legge e mostra le impostazioni attuali del G17F. Se il programma chiede il codice amministratore o installatore, inserisci il codice di 6 cifre.

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

2.1 Configurazione per l'app Protegus 2

Nella pagina **Users & Reporting**, nel gruppo **Cloud application**:

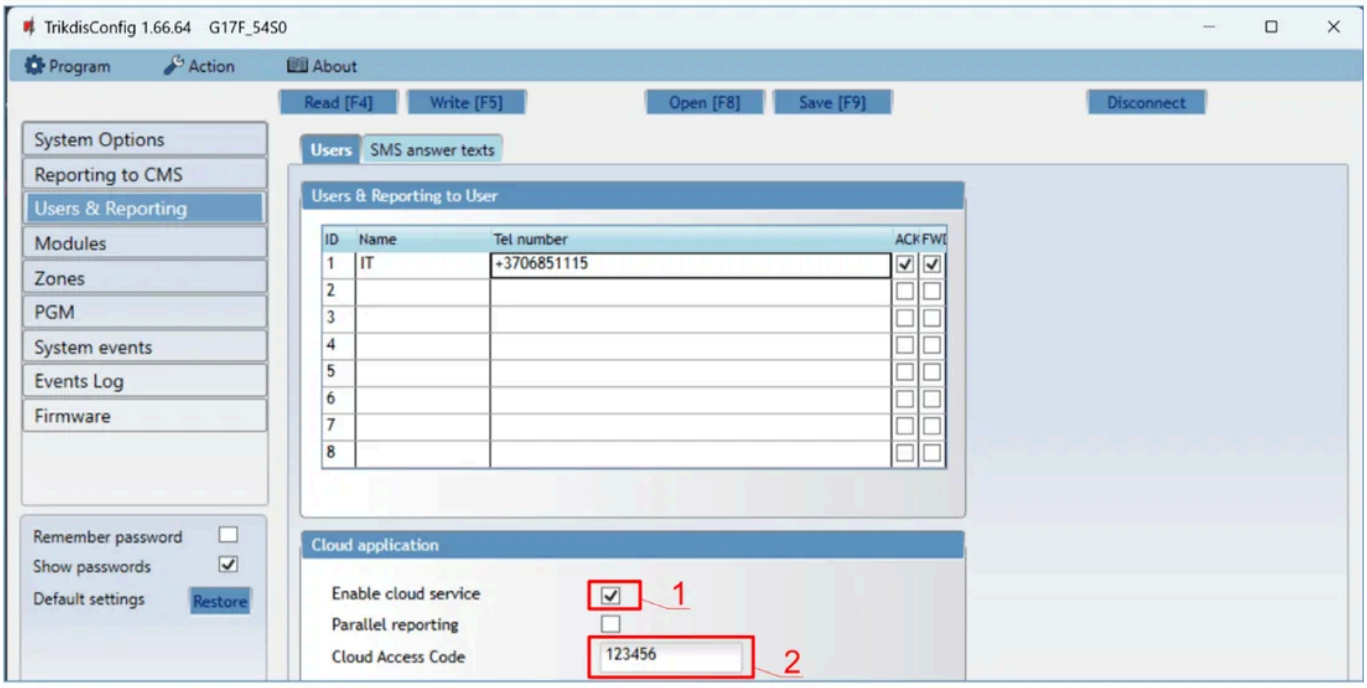


Figura 3. TrikdisConfig – **Users & Reporting**, gruppo **Cloud application**.

- 1 **Enable cloud service** – attivazione del cloud Protegus
- 2 **Cloud Access Code** – codice di accesso al cloud (di fabbrica `123456`)

1. Spunta la casella **Enable cloud service**.
2. Se vuoi che gli utenti, quando aggiungono il sistema in Protegus 2, debbano inserire il codice, cambia il valore di **Cloud Access Code** (di fabbrica `123456`).

Nella pagina **System Options**, nel gruppo **SIM**:

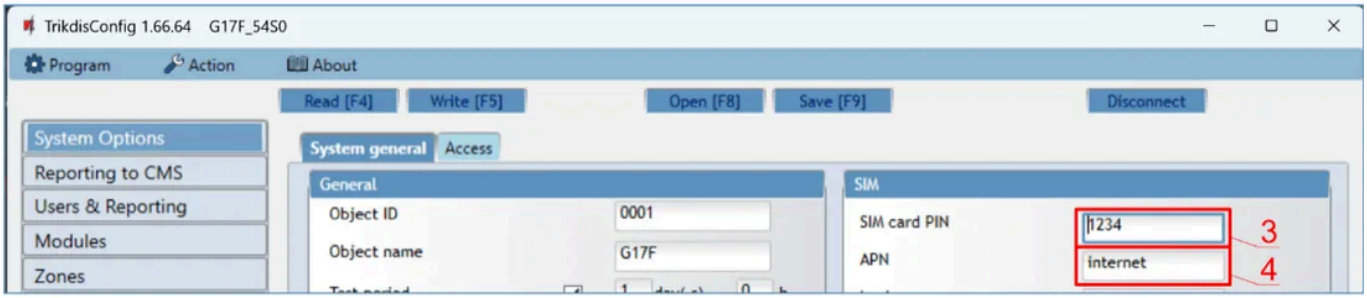


Figura 4. TrikdisConfig – **System Options**, gruppo **SIM**.

- 3 **SIM card PIN** – codice PIN della scheda SIM
- 4 **APN** – punto di accesso a Internet mobile

3. Inserisci il codice PIN della scheda SIM (**SIM card PIN**).
4. Se necessario, modifica il campo **APN**. L'APN lo trovi sul sito dell'operatore mobile; „internet" è universale e funziona nella rete della maggior parte degli operatori. I dati degli operatori nazionali ed europei: Impostazione dell'APN – elenco degli operatori mobili europei.
5. Nella pagina **Zones** spunta la casella **Prot.** per le zone sui cui cambiamenti di stato gli utenti devono ricevere una notifica in Protegus 2 (punto 5.6).
6. Nella pagina **PGM** spunta la casella **Prot.** per le uscite PGM sui cui cambiamenti di stato gli utenti devono ricevere una notifica in Protegus 2 (punto 5.7).
7. Nella pagina **System events** spunta la casella **Prot.** per gli eventi interni del comunicatore sui cui cambiamenti di stato gli utenti devono ricevere una notifica in Protegus 2 (punto 5.8).

Al termine delle impostazioni fai clic sul pulsante **Write [F5]** e scollega il cavo USB. Aggiunta del sistema all'app Protegus 2: punto 4.1.

2.2 Configurazione per la centrale di vigilanza

Le impostazioni per la centrale di vigilanza si trovano in due pagine. Nella pagina **System Options**:

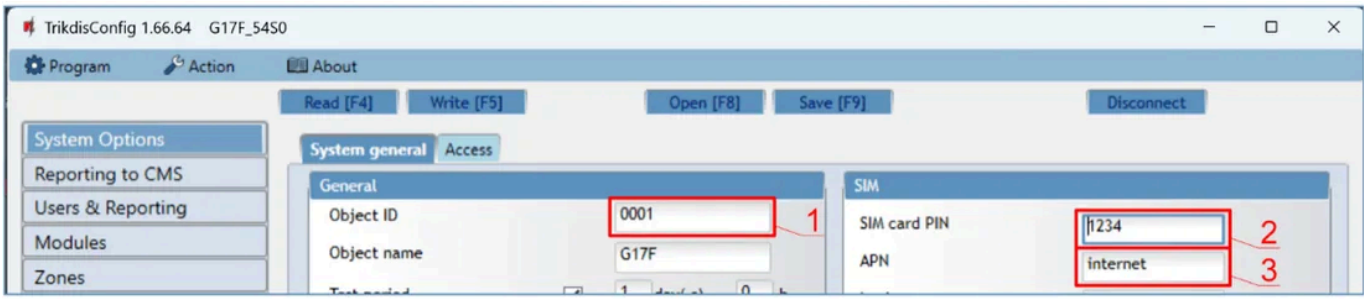


Figura 5. TrikdisConfig – **System Options**.

- 1 **Object ID** – codice identificativo dell'impianto
- 2 **SIM card PIN** – codice PIN della scheda SIM
- 3 **APN** – punto di accesso a Internet mobile

1. Inserisci il codice identificativo dell'impianto ricevuto dalla centrale di vigilanza (**Object ID**): 4 caratteri, 0–9 e A–F. Non usare i codici FFFE e FFFF.
2. Inserisci il codice PIN della scheda SIM.
3. Se necessario, modifica il campo **APN**. L'APN lo trovi sul sito dell'operatore mobile; „internet” è universale e funziona nella rete della maggior parte degli operatori.

Nella pagina **Reporting to CMS**:

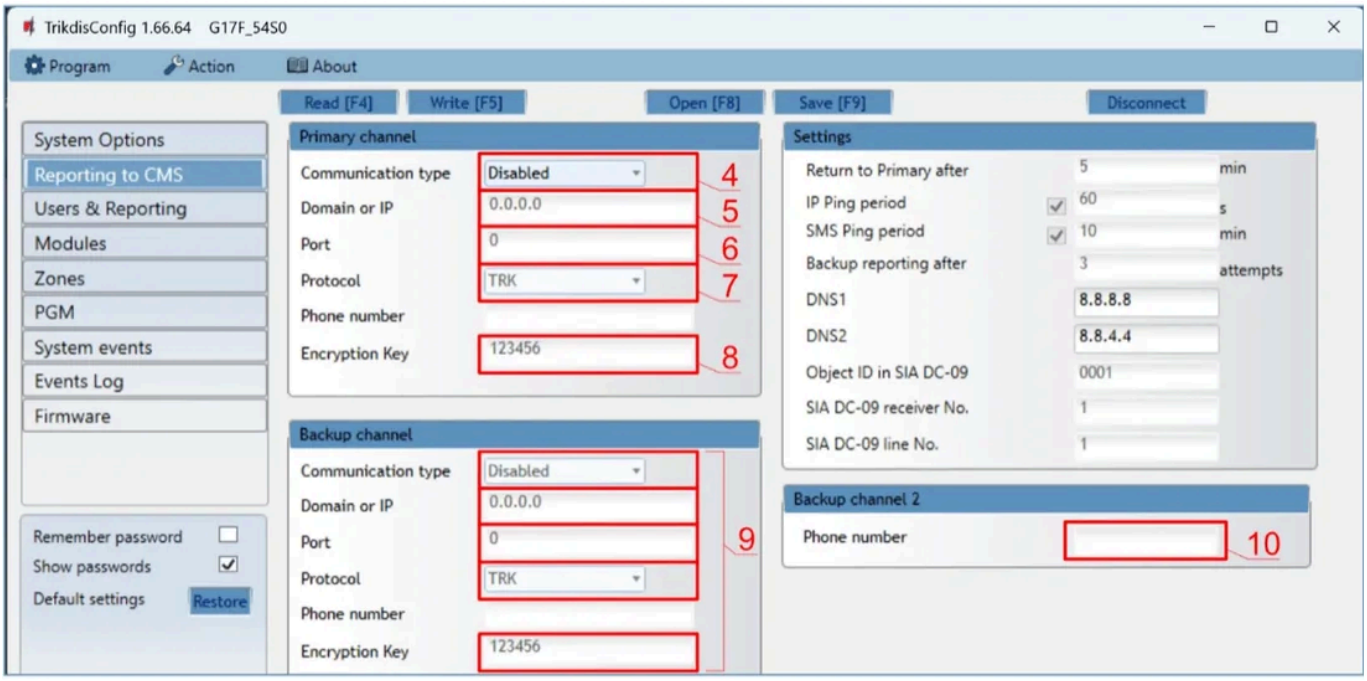


Figura 6. TrikdisConfig – **Reporting to CMS**.

- 4 **Communication type** – tipo di connessione
- 5 **Domain or IP** – indirizzo del ricevitore
- 6 **Port** – porta del ricevitore
- 7 **Protocol** – protocollo di trasmissione
- 8 **Encryption Key** – chiave di cifratura
- 9 **Backup channel** – il canale di riserva
- 10 **Backup channel 2** – numero di telefono del ricevitore SMS

4. **Communication type** – scegli il tipo di connessione (sul canale principale l'SMS non è consigliato).
5. **Domain or IP** – inserisci il nome di dominio o l'indirizzo IP del ricevitore.
6. **Port** – inserisci la porta di rete del ricevitore.
7. **Protocol** – scegli con quale protocollo il dispositivo invia i messaggi: **TRK** (per i ricevitori Trikdis), **DC-09_2007** o **DC-09_2012** (per ricevitori universali).
8. **Encryption Key** – inserisci la chiave di cifratura del ricevitore.

Se segnali alla centrale di vigilanza via SMS, devi compilare solo i campi **Encryption Key** e **Phone number**. I messaggi SMS vengono ricevuti dal ricevitore IP/SMS Trikdis **RL14**, dal ricevitore multicanale **RM14** e dal ricevitore SMS **GM14**. Se come protocollo di trasmissione scegli DC-09, nella pagina **Reporting to CMS**, nel gruppo **Settings**, inserisci anche il numero dell'impianto, della linea e del ricevitore (punto 5.3).

9. (Consigliato) Imposta il canale di riserva (**Backup channel**).
10. (Consigliato) Inserisci il numero di telefono del **Backup channel 2**.

Al termine delle impostazioni fai clic sul pulsante **Write [F5]** e scollega il cavo USB. Le altre impostazioni del G17F sono descritte nel capitolo 5.

3. Installazione e collegamenti

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.

Il capitolo descrive il fissaggio del G17F, il collegamento della centrale antincendio (alle uscite della centrale oppure, tramite bus RS485, alla centrale a protocollo ESPA 4.4.4, NSC Solution, INIM Smartline e C-TEC Cast ZFP), il collegamento degli ingressi e dei moduli di espansione (iO, iO-8, LORA, W485, E485) e infine l'accensione del comunicatore. Negli schemi i nomi dei morsetti del G17F corrispondono alle scritte del dispositivo (punto 1.5).

3.1 Fissaggio e inserimento della scheda SIM

1. Prima dell'installazione assicurati che nel punto di montaggio del G17F il segnale della rete mobile sia sufficiente.
2. Rimuovi il pannello frontale ed estrai la morsettiera.
3. Estrai il circuito stampato.
4. Fissa con le viti la parte posteriore della scatola nel punto desiderato.
5. Rimetti al suo posto il circuito stampato e la morsettiera.
6. Avvita l'antenna della rete mobile.
7. Inserisci la scheda nano-SIM. La scheda SIM deve essere registrata in una rete mobile e i suoi servizi devono essere attivi e funzionanti: deve poter chiamare, inviare e ricevere SMS e avere i dati mobili. Per l'attivazione dei servizi necessari rivolgiti all'operatore mobile della scheda SIM.

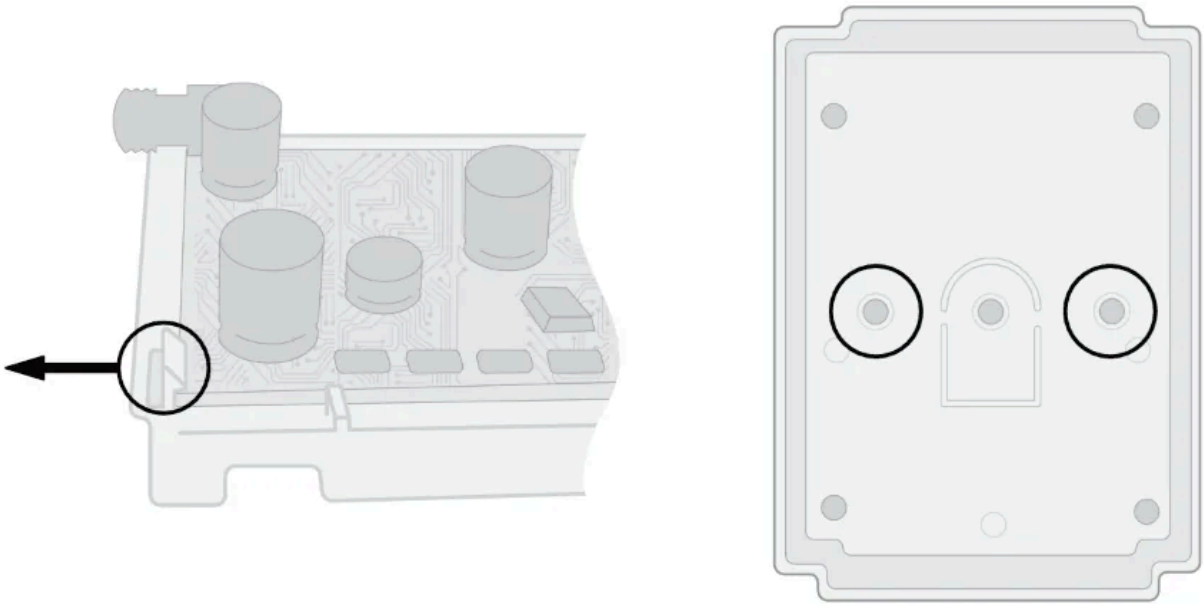


Figura 7. A sinistra la linguetta di fissaggio del circuito stampato sul bordo sinistro della scheda (con questa la scheda si libera dalla scatola), a destra i due fori per le viti della parte posteriore.

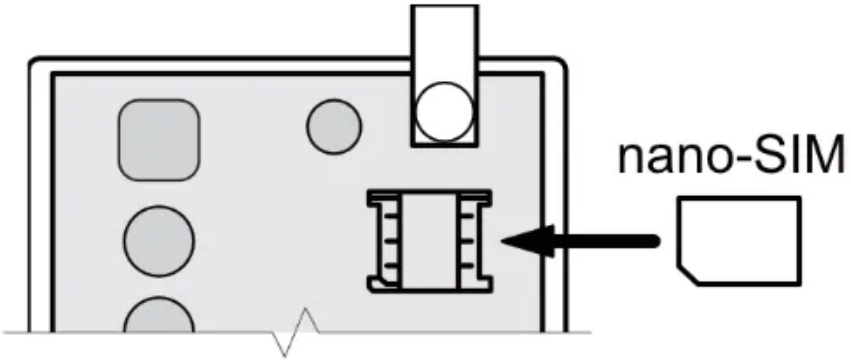


Figura 8. Inserimento della scheda nano-SIM da destra, nell'alloggiamento sul circuito stampato.

- Verifica che la scheda SIM sia attivata.
- Se comunichi anche su canale IP o con l'app Protegus 2, verifica che i dati mobili siano attivi.
- Se non vuoi inserire il codice PIN in TrikdisConfig, metti la scheda SIM in un telefono e disattiva la richiesta del PIN.

8. Per la configurazione a distanza del G17F inserisci una scheda SIM con la richiesta del PIN disattivata e accendi l'alimentazione del comunicatore. Se non hai ancora configurato il G17F con TrikdisConfig e il servizio Protegus non è attivo, invia al dispositivo questo SMS:

```
CONNECT 123456 PROTEGUS=ON,APN=INTERNET
```

9. La configurazione a distanza dei parametri è descritta nel capitolo 6.
10. Rimetti al suo posto il pannello frontale.

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

3.2 Collegamento alle uscite della centrale antincendio

Se vuoi monitorare lo stato della centrale antincendio, collega le uscite corrispondenti della centrale agli ingressi del G17F. Le uscite della centrale (**PGM1**, **PGM2**, **PGM3**) vanno impostate nella centrale come uscite di stato (allarme, guasto ecc.).

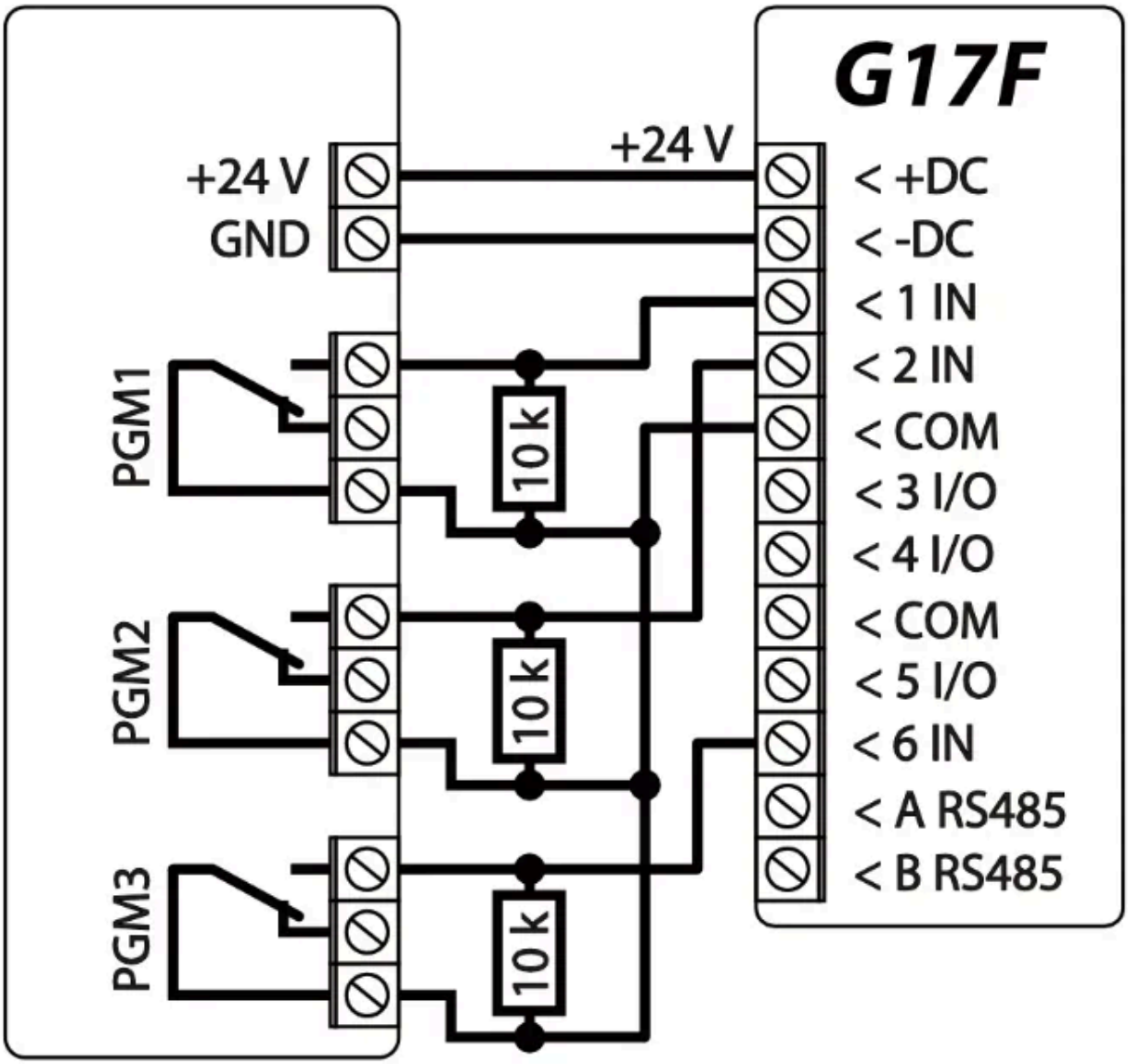


Figura 9. Collegamento del G17F alle uscite della centrale antincendio (**Fire control panel**). Le scritte dello schema: il morsetto **+24 V** della centrale va al morsetto **+DC** del G17F, il **GND** al **–DC**; un conduttore delle uscite **PGM1**, **PGM2** e **PGM3** va rispettivamente all'ingresso **1 IN**, **2 IN** e **6 IN** del G17F, l'altro al morsetto **COM**; tra i due conduttori di ogni uscita si collega in parallelo una resistenza da **10 k** (10 kΩ).

3.3 Centrale antincendio a protocollo ESPA 4.4.4

Collega la centrale antincendio a protocollo ESPA 4.4.4 al G17F tramite il bus RS485, secondo lo schema seguente.

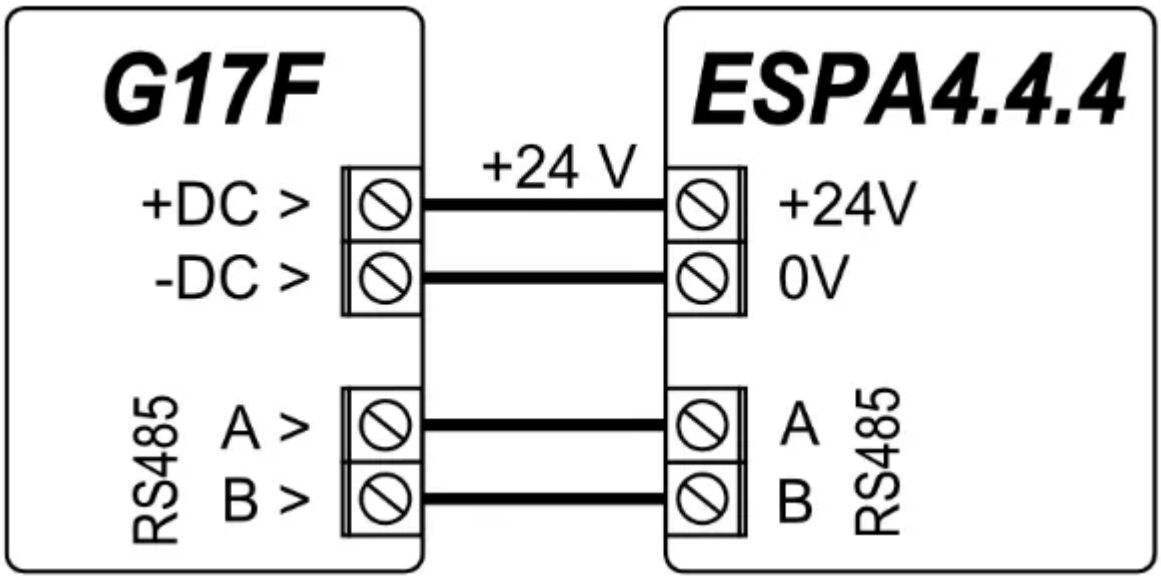


Figura 10. Collegamento tra il G17F e la centrale antincendio a protocollo ESPA 4.4.4. Le scritte dello schema: alimentazione – il morsetto **+DC** del G17F va al morsetto **+24V** della centrale, il **–DC** al morsetto **0V**; RS485 – il morsetto **A** del G17F va al morsetto **A** della centrale, il **B** al **B**.

Configurazione del G17F in TrikdisConfig, se è collegato a una centrale antincendio a protocollo ESPA 4.4.4:

1. Nella pagina **Modules** scegli il protocollo **ESPA 4.4.4**.
2. Scegli la velocità di trasmissione dati dell'interfaccia (**Baudrate**).
3. I parametri di trasmissione dati del G17F e della centrale antincendio devono essere identici.

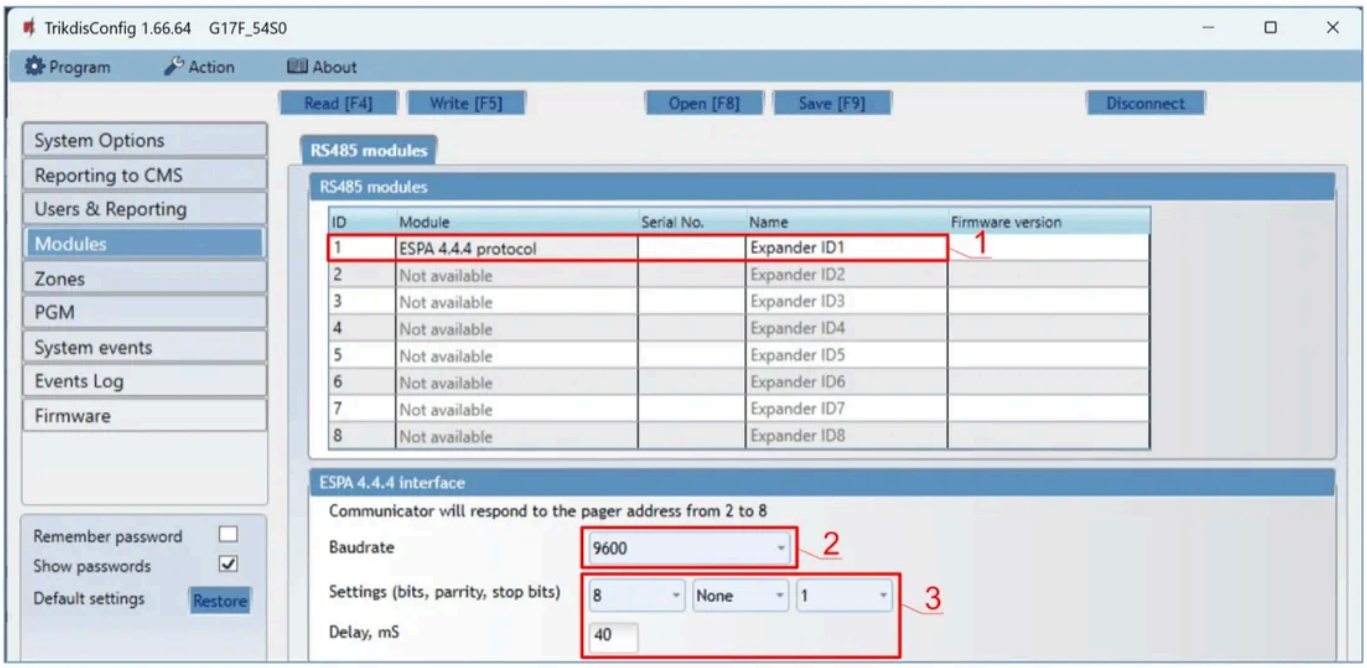


Figura 11. TrikdisConfig – **Modules**: il modulo RS485 n. 1 è **ESPA 4.4.4 protocol**. La scritta del gruppo **ESPA 4.4.4 interface**: „Communicator will respond to the pager address from 2 to 8" – il comunicatore risponde agli indirizzi cercapersone (pager address) da 2 a 8.

- 1 scelta di **ESPA 4.4.4 protocol**
- 2 **Baudrate** – velocità di trasmissione dati (nell'immagine 9600)
- 3 bit di dati, parità, bit di stop e ritardo (nell'immagine 8, None, 1, 40 ms)

4. Nella pagina **Users & Reporting** inserisci i numeri di telefono degli utenti che ricevono i messaggi dal G17F (punto 5.4).

5. Se vuoi che l'utente riceva un messaggio (o una chiamata) sugli eventi, nella pagina **System events**, scheda **SMS & Call reporting**, spunta la casella **SMS** (o **Call**).

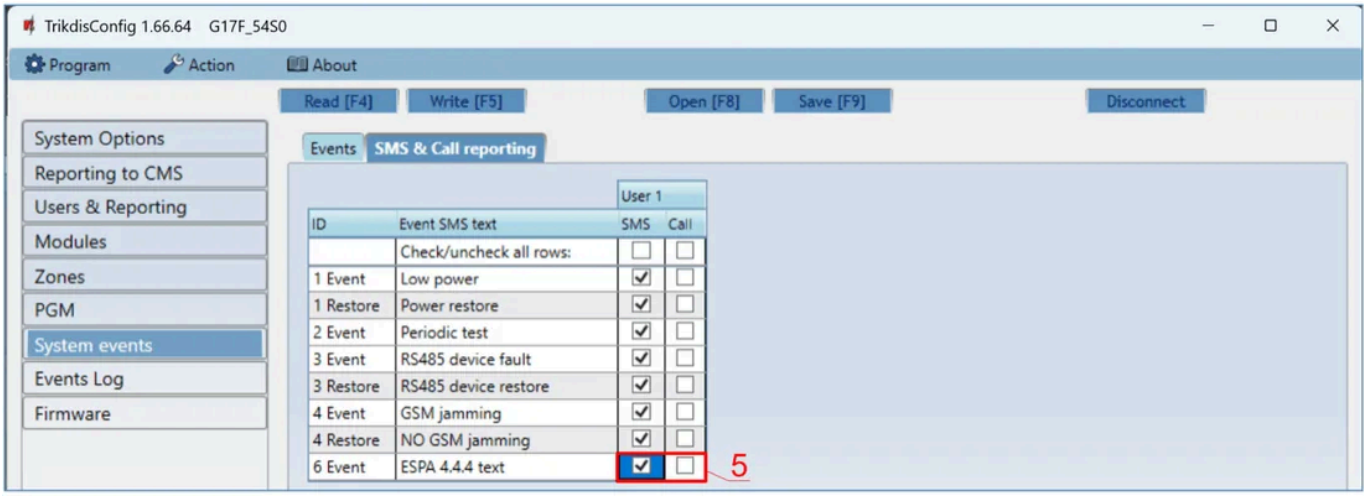


Figura 12. TrikdisConfig – **System events**, scheda **SMS & Call reporting**: per l'utente 1, all'evento **ESPA 4.4.4 text** la casella **SMS** è spuntata.

- 5 le caselle **SMS** e **Call** all'evento **ESPA 4.4.4 text**

6. Se i messaggi devono arrivare anche al ricevitore della centrale di vigilanza, imposta il canale di comunicazione nella pagina **Reporting to CMS** (punti 2.2 e 5.3). I messaggi di evento vengono inviati con il protocollo **SIA DC-09**.

Prova il sistema: provoca un allarme incendio e verifica che i messaggi del G17F arrivino alla centrale di vigilanza e in Protegus 2.

3.4 Centrale antincendio NSC Solution

Collega la centrale antincendio NSC Solution al G17F tramite il bus RS485, secondo lo schema seguente.

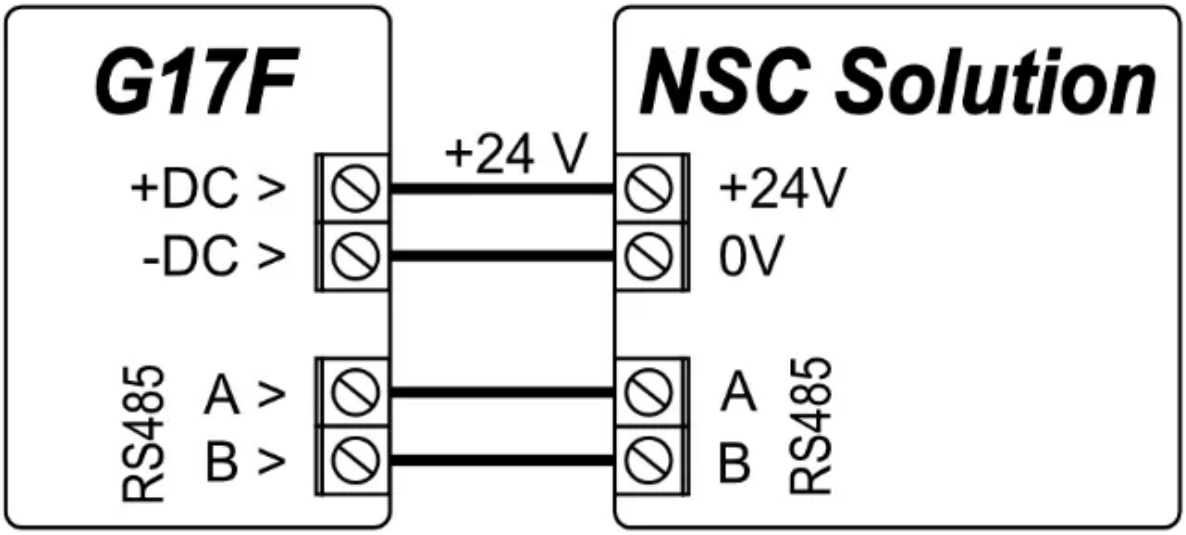


Figura 13. Collegamento tra il G17F e la centrale antincendio NSC Solution. Le scritte dello schema: alimentazione – il morsetto **+DC** del G17F va al morsetto **+24V** (+24 V) della centrale, il **–DC** al morsetto **0V**; RS485 – **A** al morsetto **A**, **B** al **B**.

Configurazione del G17F in TrikdisConfig, se è collegato a una centrale antincendio NSC Solution:

1. Nella pagina **Modules** scegli il modulo **NSC Solution**.

2. L'**NSC slave address** (indirizzo slave del comunicatore) non può coincidere con l'indirizzo dei moduli collegati alla centrale antincendio.

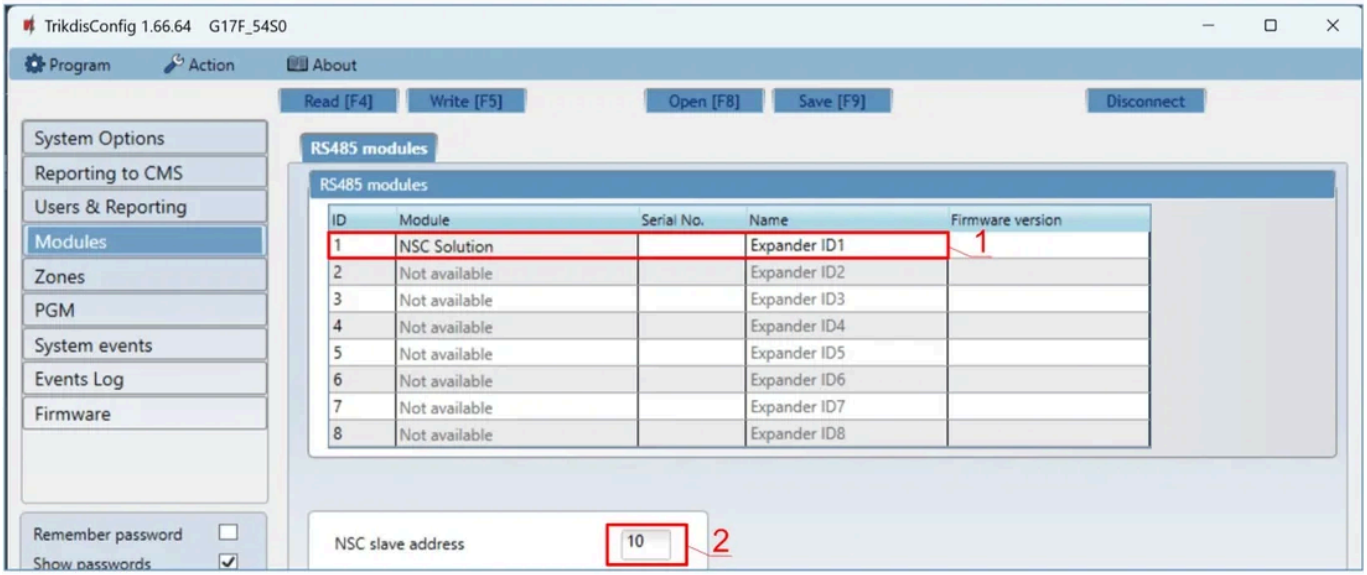


Figura 14. TrikdisConfig – **Modules**: il modulo RS485 n. 1 è **NSC Solution** (nome **Expander ID1**).

- 1 scelta di **NSC Solution**
- 2 **NSC slave address** – nell'immagine 10

3. Nella pagina **Users & Reporting** inserisci i numeri di telefono degli utenti che ricevono i messaggi dal G17F (punto 5.4).
4. Gli utenti ricevono SMS e chiamate sugli eventi spuntati (pagina **Users & Reporting**, scheda **SMS for Panel events**). Nella colonna **CID** puoi aggiungere altri codici evento Contact ID; accanto ai nuovi codici devi scrivere anche il testo dell'SMS. Se vuoi che l'utente riceva un messaggio (o una chiamata) sugli eventi, spunta la casella **SMS** (o **Call**).

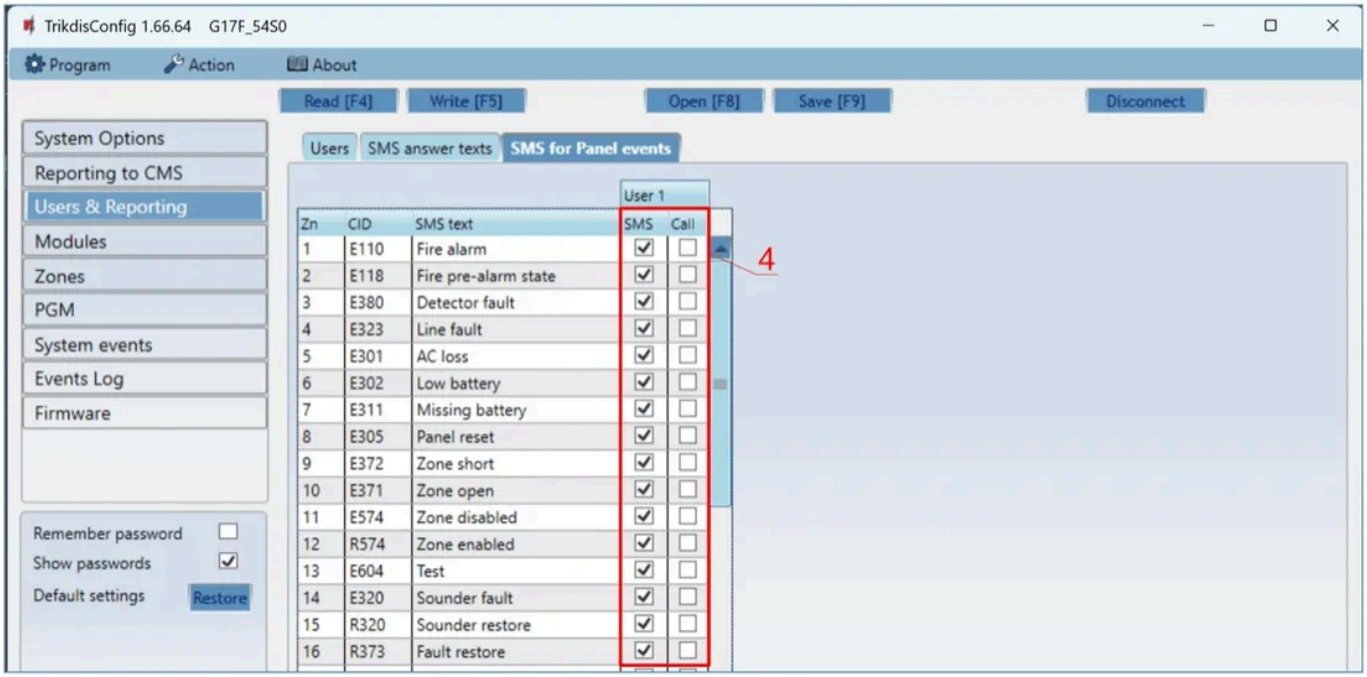


Figura 15. TrikdisConfig – **Users & Reporting**, scheda **SMS for Panel events**: per l'utente 1, nei 16 eventi visibili (dall'allarme incendio **E110 Fire alarm** al ripristino guasto **R373 Fault restore**) la casella **SMS** è spuntata, la **Call** è vuota.

- 4 le colonne **SMS** e **Call** dell'utente 1

5. Se i messaggi devono arrivare anche al ricevitore della centrale di vigilanza, imposta il canale di comunicazione nella pagina **Reporting to CMS** (punti 2.2 e 5.3).

Dopo aver configurato il G17F accendi l'alimentazione della centrale antincendio e attendi che il software della centrale si carichi. Poi sulla centrale bisogna cercare (scansionare) i moduli collegati al bus RS485. Sulla centrale premi: **PROG.** > **INSTALLER** > (inserisci il codice installatore) **00000 OK** > (scegli) **SETTINGS** > **ENTER** > (scegli) **SCAN RS485** > **ENTER**. Attendi la fine della ricerca, poi premendo due volte il pulsante **CANCEL** torna alla schermata principale.

Prova il sistema: provoca un allarme incendio e verifica che i messaggi del G17F arrivino alla centrale di vigilanza e in Protegus 2.

3.5 Centrale antincendio INIM Smartline

Collega la centrale antincendio INIM Smartline al G17F tramite il bus RS485, secondo lo schema seguente.

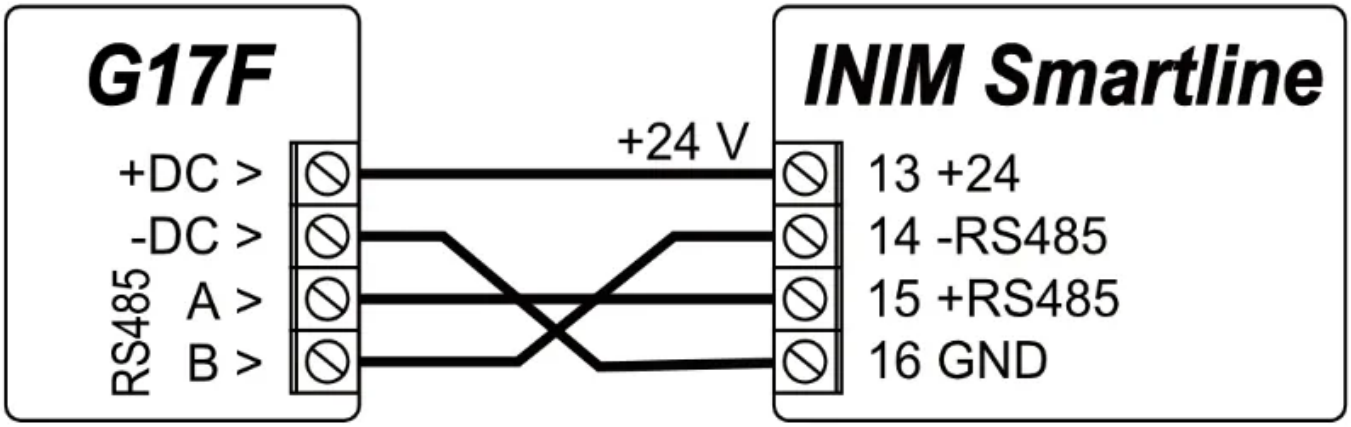


Figura 16. Collegamento tra il G17F e la centrale antincendio INIM Smartline. Le scritte dello schema: alimentazione – il morsetto **+DC** del G17F va al morsetto **13 +24** (+24 V) della centrale, il **–DC** al morsetto **16 GND**; RS485 – l'**A** al morsetto **15 +RS485**, il **B** al morsetto **14 –RS485**. I conduttori che si incrociano non sono in contatto tra loro.

Se colleghi la centrale INIM Smartline al G17F tramite bus RS485, la centrale va impostata in modalità **slave** (subordinata) – lo puoi fare nel programma SmartLeague della centrale.

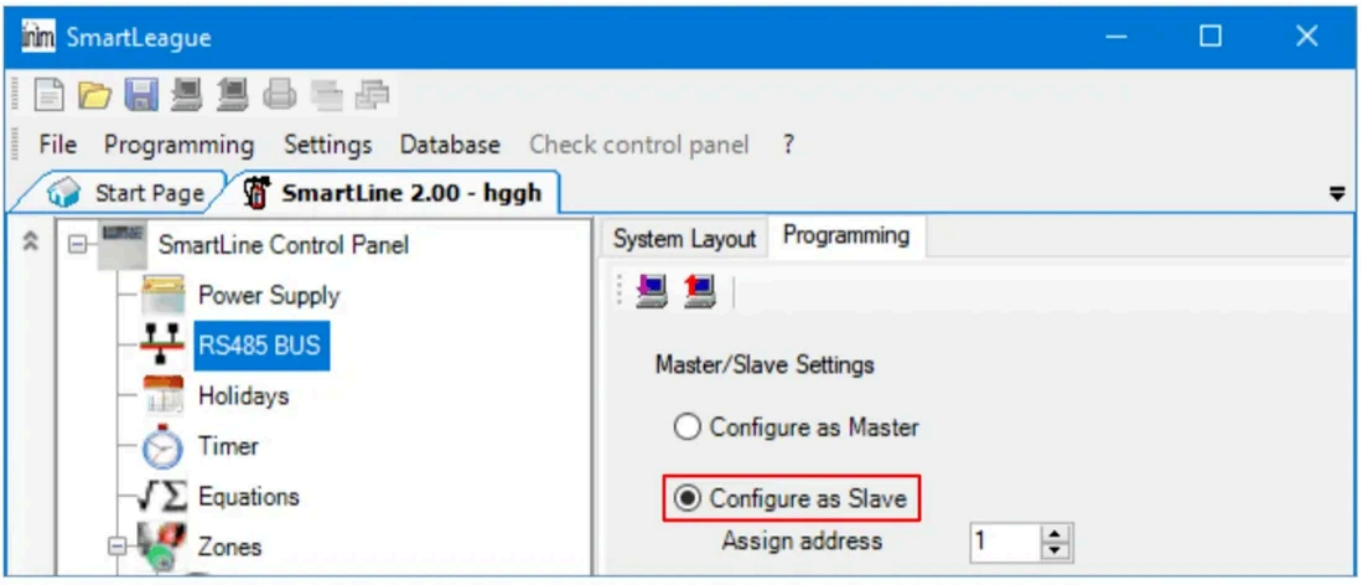


Figura 17. SmartLeague – finestra **RS485 Bus Programming**: nel gruppo **Master/Slave Settings** è selezionato **Configure as Slave**, **Assign address**: 1.

- Se alla centrale INIM Smartline sono collegati dei ripetitori (repeater), il G17F non può essere collegato tramite bus RS485.
- Se il G17F è collegato al bus RS485 della centrale INIM Smartline, i moduli di espansione iO del comunicatore non sono supportati.

Configurazione del G17F in TrikdisConfig, se è collegato a una centrale antincendio INIM Smartline:

1. Nella pagina **Modules** scegli il modulo **Inim Smartline**.

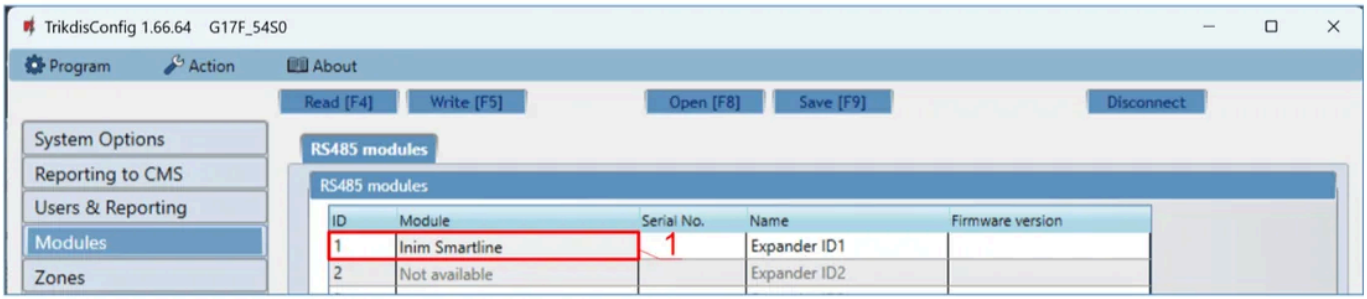


Figura 18. TrikdisConfig – **Modules**: il modulo RS485 n. 1 è **Inim Smartline** (nome **Expander ID1**).

- 1 scelta di **Inim Smartline**

2. Nella pagina **Users & Reporting** inserisci i numeri di telefono degli utenti che ricevono i messaggi dal G17F (punto 5.4).
3. Gli utenti ricevono SMS e chiamate sugli eventi spuntati (pagina **Users & Reporting**, scheda **SMS for Panel events** – l'immagine della scheda è al punto 3.4 e al punto 5.4). Nella colonna **CID** puoi aggiungere altri codici evento Contact ID; accanto ai nuovi codici devi scrivere anche il testo dell'SMS. Se vuoi che l'utente riceva un messaggio (o una chiamata) sugli eventi, spunta la casella **SMS** (o **Call**).
4. Se i messaggi devono arrivare anche al ricevitore della centrale di vigilanza, imposta il canale di comunicazione nella pagina **Reporting to CMS** (punti 2.2 e 5.3).

Prova il sistema: provoca un allarme incendio e verifica che i messaggi del G17F arrivino alla centrale di vigilanza e in Protegus 2.

3.6 Centrale antincendio C-TEC Cast ZFP

Collega la centrale antincendio C-TEC Cast ZFP al G17F tramite il bus ABUS RS485, secondo lo schema seguente.

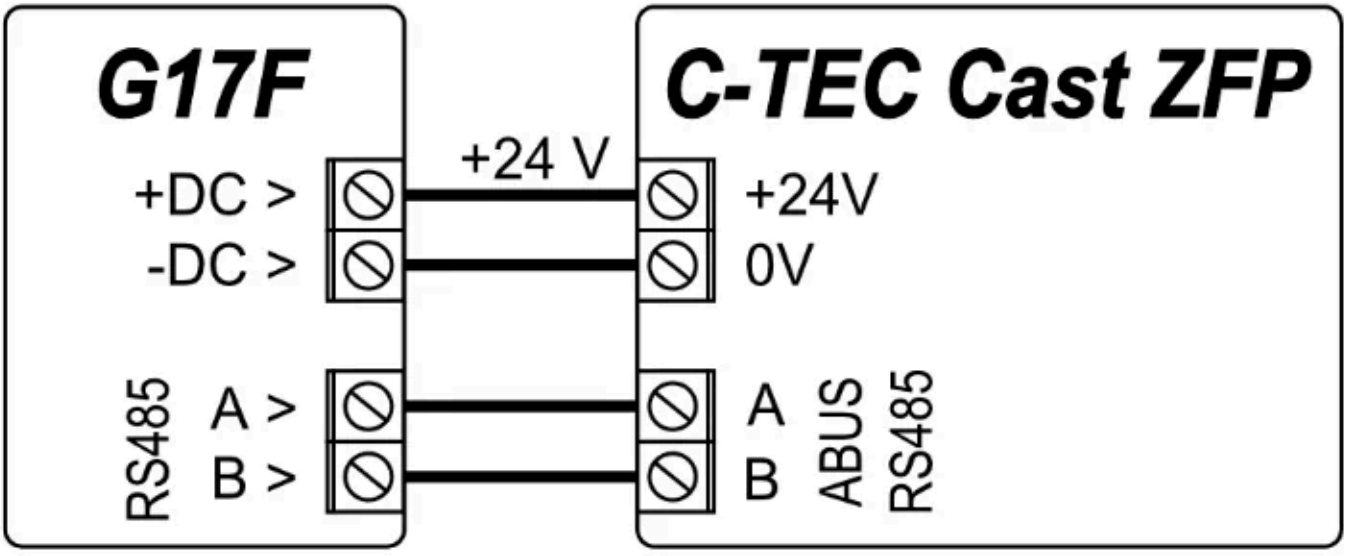


Figura 19. Collegamento tra il G17F e la centrale antincendio C-TEC Cast ZFP. Le scritte dello schema: alimentazione – il morsetto **+DC** del G17F va al morsetto **+24V** (+24 V) della centrale, il **–DC** al morsetto **0V**; **ABUS RS485** – **A** al morsetto **A**, **B** al **B**.

Configurazione del G17F in TrikdisConfig, se è collegato a una centrale antincendio C-TEC Cast ZFP:

1. Nella pagina **Modules** scegli la centrale antincendio **C-TEC Cast ZFP**.

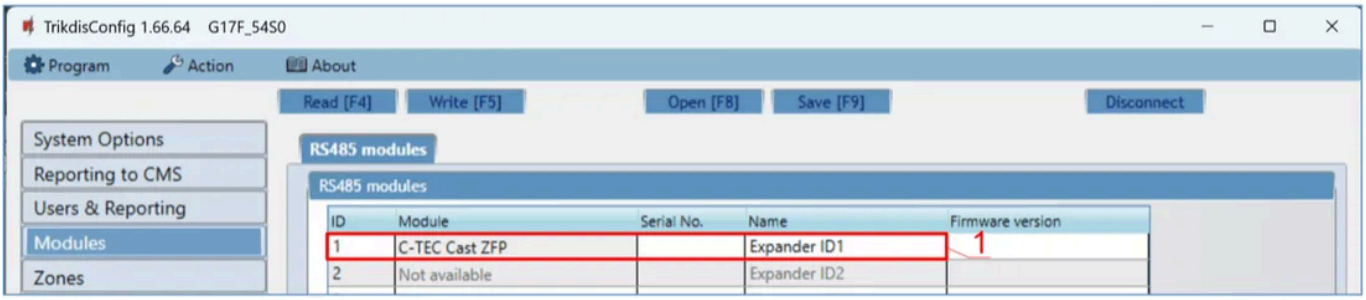


Figura 20. TrikdisConfig – **Modules**: il modulo RS485 n. 1 è **C-TEC Cast ZFP** (nome **Expander ID1**).

- 1 scelta di **C-TEC Cast ZFP**

2. Nella pagina **Users & Reporting** inserisci i numeri di telefono degli utenti che ricevono i messaggi dal G17F (punto 5.4).
3. Gli utenti ricevono SMS e chiamate sugli eventi spuntati (pagina **Users & Reporting**, scheda **SMS for Panel events** – l'immagine della scheda è al punto 3.4 e al punto 5.4). Nella colonna **CID** puoi aggiungere altri codici evento Contact ID; accanto ai nuovi codici devi scrivere anche il testo dell'SMS. Se vuoi che l'utente riceva un messaggio (o una chiamata) sugli eventi, spunta la casella **SMS** (o **Call**).
4. Se i messaggi devono arrivare anche al ricevitore della centrale di vigilanza, imposta il canale di comunicazione nella pagina **Reporting to CMS** (punti 2.2 e 5.3).

3.6.1 Configurazione della centrale C-TEC (ZFPtools)

Installa sul computer il programma **ZFPtools** e avvialo. Accendi l'alimentazione della centrale antincendio e attendi che il software della centrale si carichi. Collega la centrale al computer con un cavo **USB 2.0 A-B**.

1. Apri la scheda **Node View**.

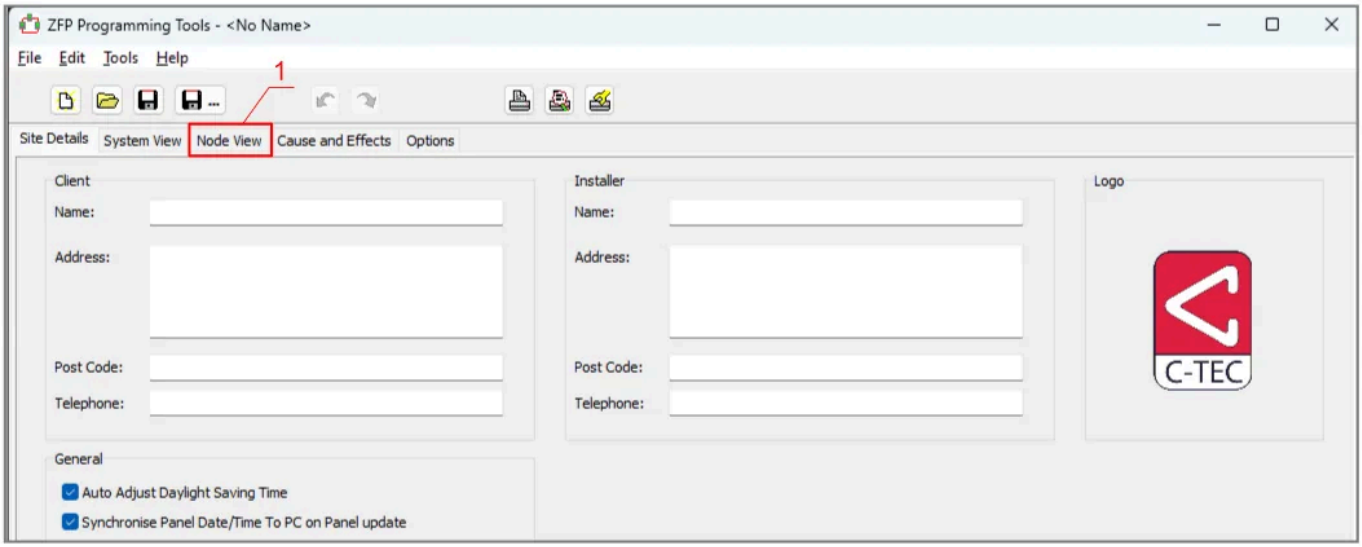


Figura 21. ZFP Programming Tools – finestra **Site Details**.

- 1 la scheda **Node View**

2. Scarica sul computer le impostazioni della centrale antincendio (**Retrieve All Data**).

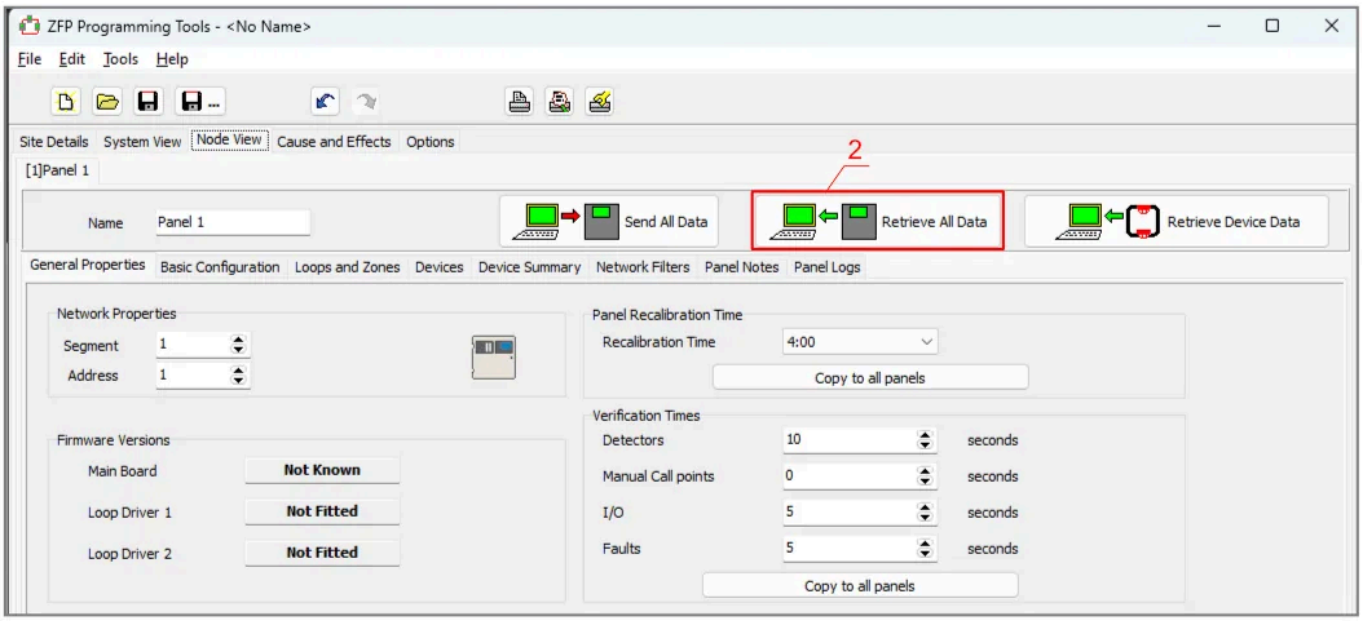


Figura 22. ZFP Programming Tools – **Node View**, **Panel 1**: il pulsante **Retrieve All Data**.

- 2 **Retrieve All Data** – scaricamento delle impostazioni della centrale

3. Inserisci il codice (di fabbrica `4444`).
4. Fai clic sul pulsante **OK** (il segno di spunta verde).

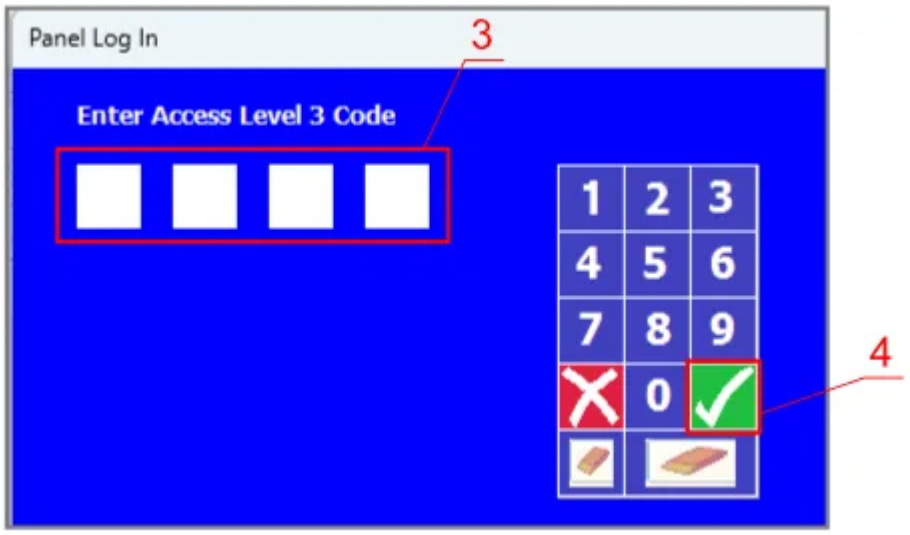


Figura 23. ZFP Programming Tools – finestra **Panel Log In**: **Enter Access Level 3 Code** – codice del livello di accesso 3.

- 3 i quattro campi del codice
- 4 il pulsante **OK** (spunta verde)

5. Scegli il dispositivo **BMS Interface** (**Device Palette**).
6. Fai clic su una posizione libera per l'icona.

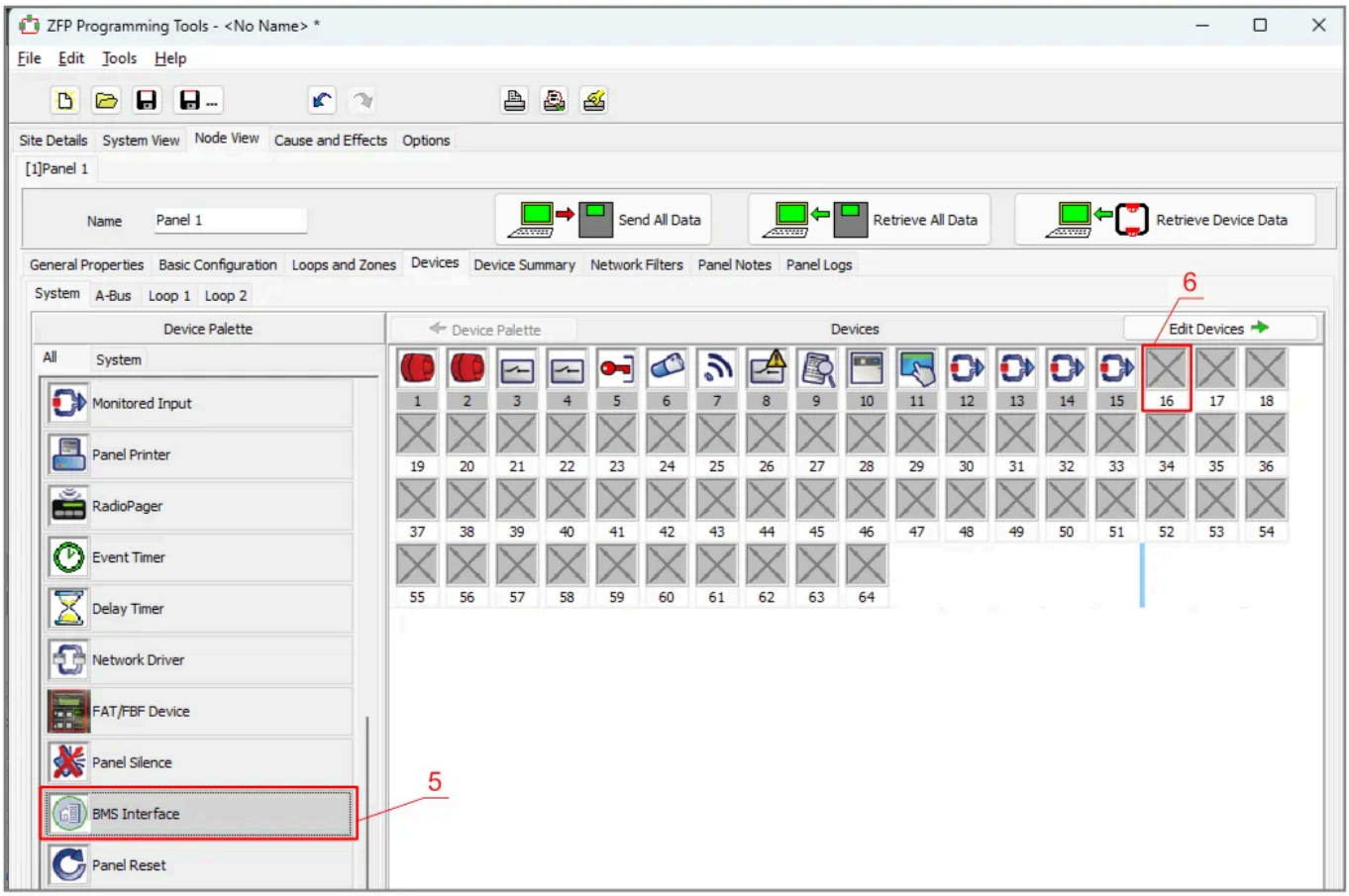


Figura 24. ZFP Programming Tools – **Node View**, **Devices**: nell'elenco **Device Palette** è selezionato **BMS Interface**.

- 5 **BMS Interface** nell'elenco **Device Palette**
- 6 posizione libera per l'icona (nell'immagine la 16ª)

7. Fai clic sul pulsante **Edit Devices**.

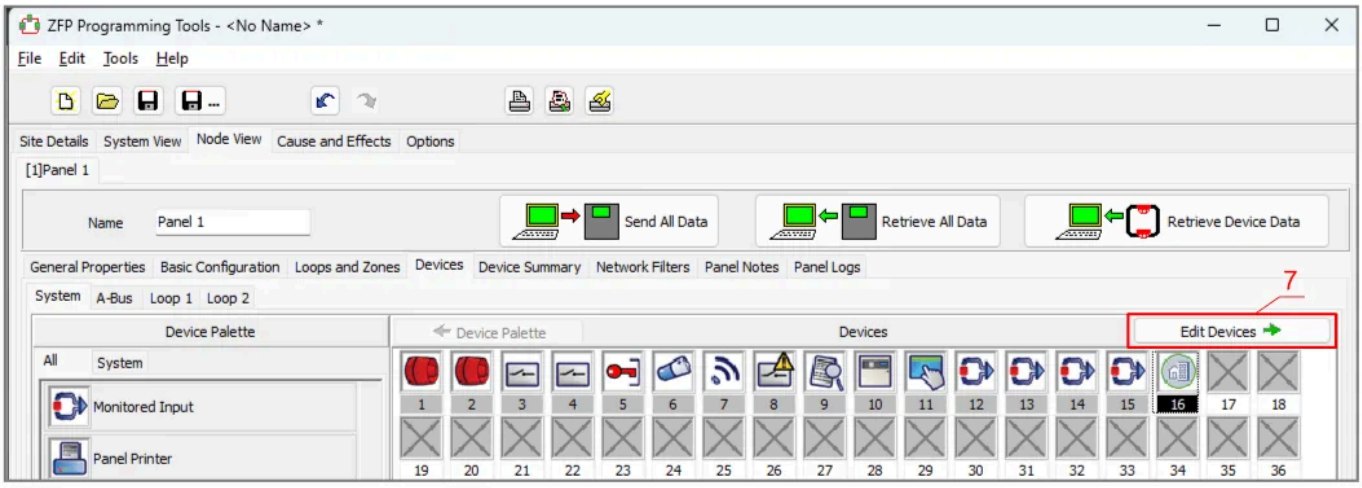


Figura 25. ZFP Programming Tools – **Node View**, **Devices**: nella 16ª posizione il **BMS Interface**; il pulsante **Edit Devices**.

- 7 **Edit Devices**

8. Nella scheda **Device** inserisci il nome del sistema.

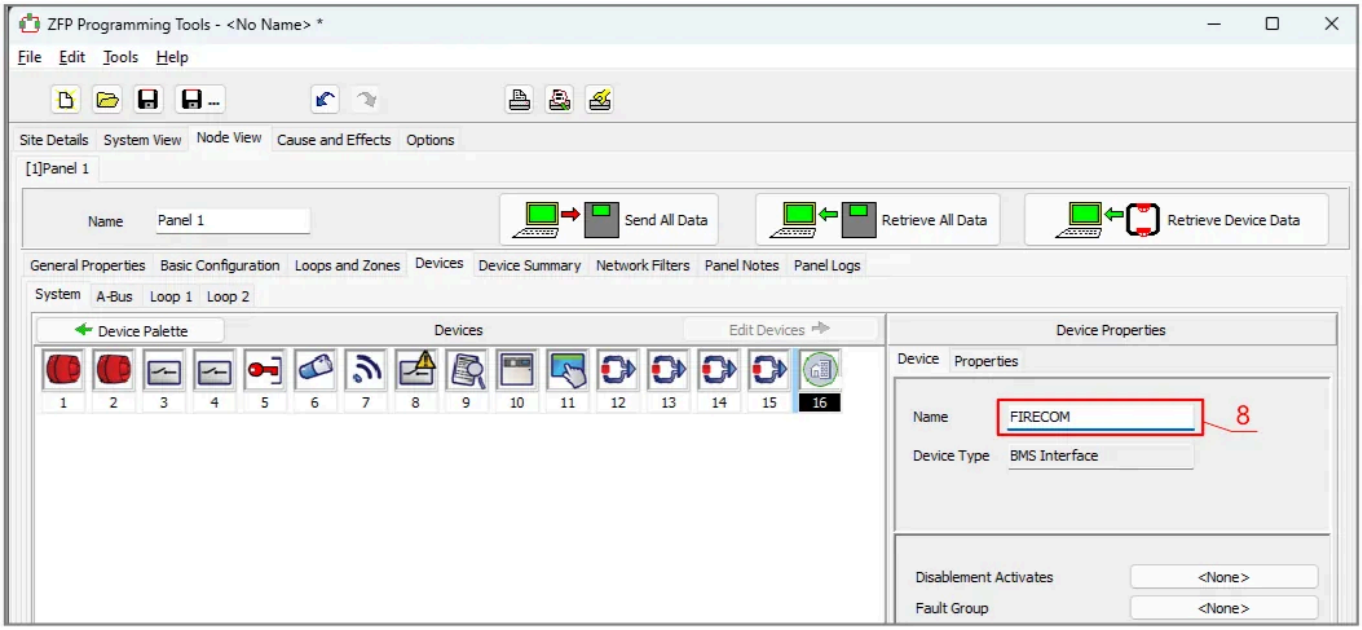


Figura 26. ZFP Programming Tools – **Device Properties**, scheda **Device**: **Name**: FIRECOM, **Device Type**: BMS Interface.

- 8 **Name** – il nome del sistema

9. Nella scheda **Properties** inserisci il nome del sistema.
10. Indica il bus **ABUS RS485** a cui è collegato il G17F.
11. Imposta i messaggi.
12. Scrivi le impostazioni nella centrale antincendio (**Send All Data**).

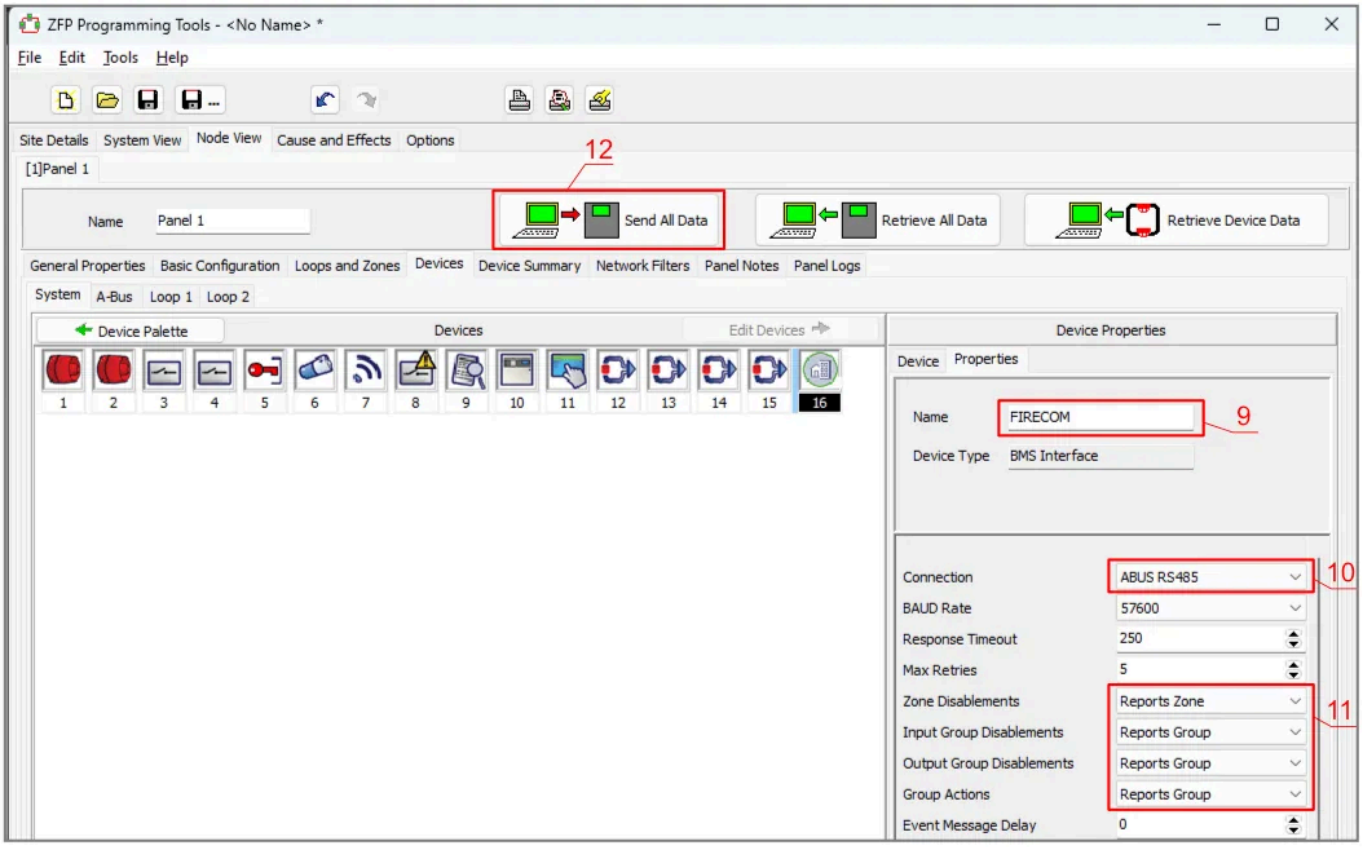


Figura 27. ZFP Programming Tools – **Device Properties**, scheda **Properties**. Nell'immagine: **BAUD Rate** 57600, **Response Timeout** 250, **Max Retries** 5.

- 9 **Name** – il nome del sistema (FIRECOM)
- 10 **Connection** – **ABUS RS485**
- 11 i messaggi: **Zone Disablements** – **Reports Zone**; **Input Group Disablements**, **Output Group Disablements** e **Group Actions** – **Reports Group**
- 12 **Send All Data** – scrittura delle impostazioni nella centrale

13. Inserisci il codice (di fabbrica `4444`) – nella stessa finestra **Panel Log In** del passo 3.
14. Fai clic sul pulsante **OK**.

La centrale antincendio è programmata. Scollega il cavo USB 2.0 A-B dalla centrale.

Prova il sistema: provoca un allarme incendio e verifica che i messaggi del G17F arrivino alla centrale di vigilanza e in Protegus 2.

3.7 Collegamento degli ingressi

Il comunicatore ha sei morsetti di ingresso (**1 IN** – **6 IN**; di cui tre a doppia funzione, IN/OUT), a cui si possono collegare circuiti di tipo NO, NC ed EOL (4,7 kΩ, 10 kΩ). Di fabbrica gli ingressi controllano circuiti di tipo EOL; un altro tipo lo puoi impostare nella pagina **Zones** di TrikdisConfig (punto 5.6).

Collegamento	Riposo (ripristino)	Allarme
NO – contatto normalmente aperto	aperto	cortocircuito
NC – contatto normalmente chiuso	cortocircuito	aperto
NO + EOL – contatto aperto con una resistenza da 10 kΩ in parallelo	10 kΩ	cortocircuito o aperto
NC + EOL – contatto chiuso con una resistenza da 10 kΩ in serie	10 kΩ	cortocircuito o aperto

Gli schemi dei quattro tipi di collegamento; il contatto va tra il morsetto **COM** e il morsetto **INx**, **10k** è la resistenza di fine linea da 10 kΩ.

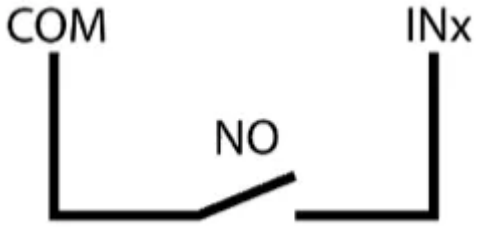


Figura 28. NO – contatto normalmente aperto.

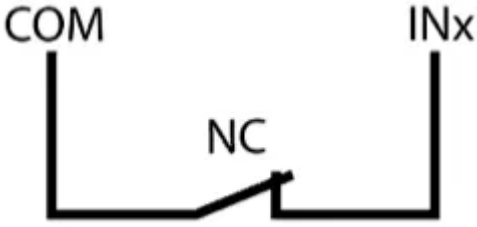


Figura 29. NC – contatto normalmente chiuso.

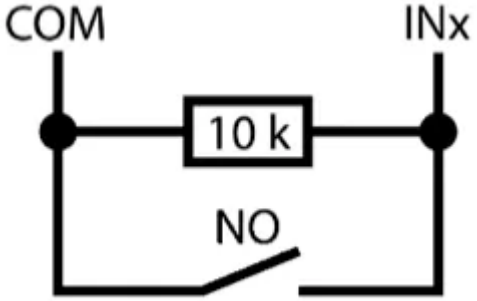


Figura 30. NO + EOL (EOL10k) – contatto normalmente aperto con resistenza da 10 kΩ in parallelo.

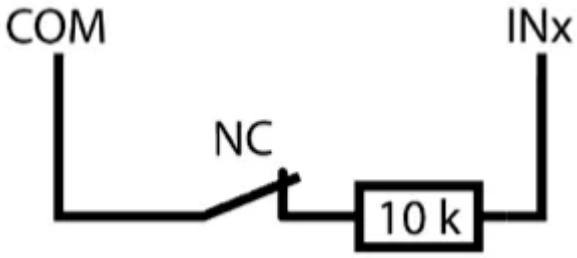


Figura 31. NC + EOL (EOL10k) – contatto normalmente chiuso con resistenza da 10 kΩ in serie.

3.8 Moduli di espansione della serie iO

Se al comunicatore servono più ingressi (IN) o uscite (OUT), collegagli un modulo di espansione di ingressi e uscite Trikdis della serie iO, cablato o senza fili.

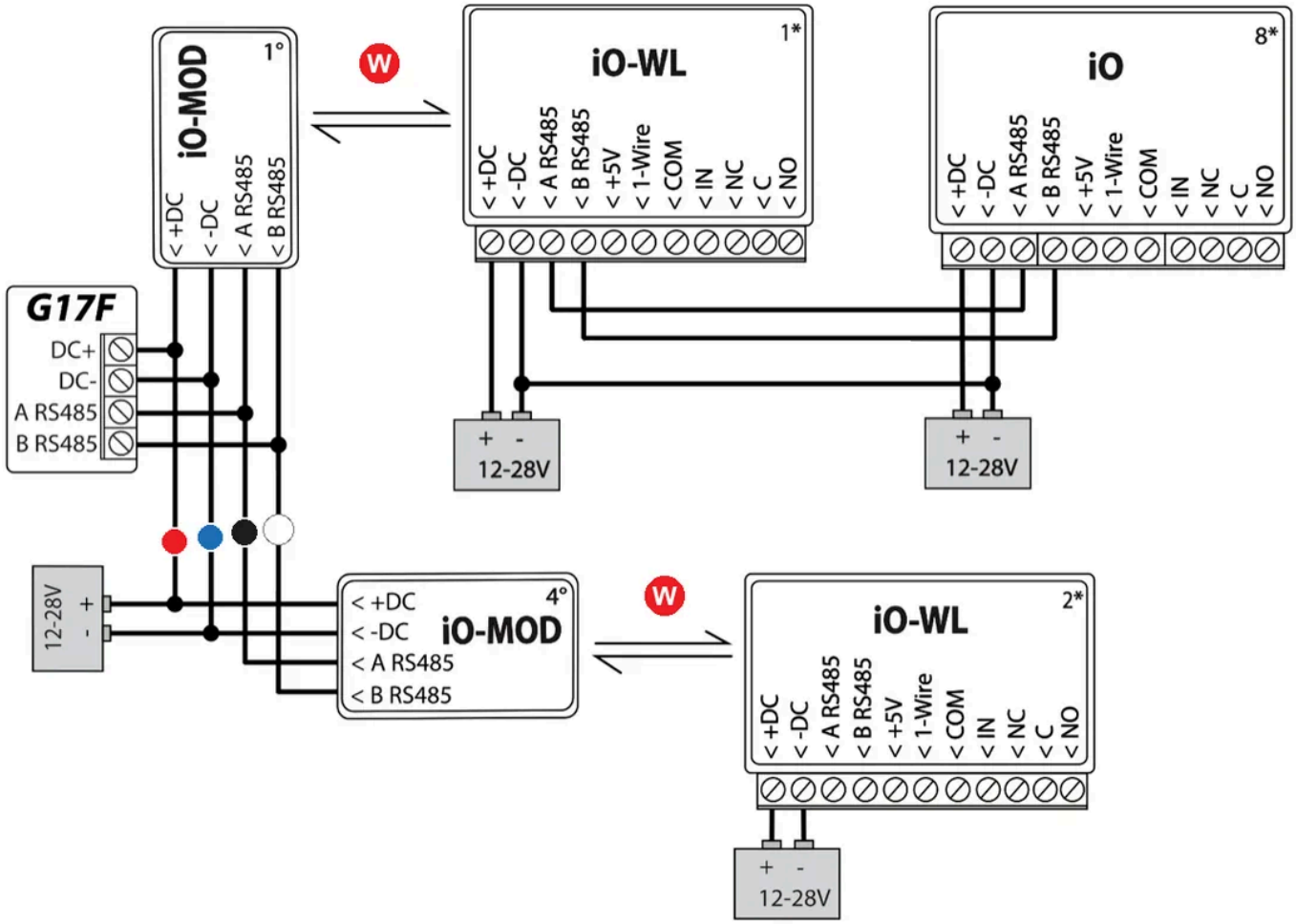


Figura 32. Moduli iO-MOD, iO-WL e iO sul G17F: il morsetto **DC+** del G17F va al morsetto **+DC** dell'iO-MOD (filo rosso), il **DC–** al **–DC** (blu), l'**A RS485** all'**A RS485** (nero), il **B RS485** al **B RS485** (bianco); alimentazione comune 12–28 V; al massimo 4 moduli iO-MOD („up to 4 iO-MOD modules", nello schema indicati con °); ogni iO-MOD si collega via radio a un iO-WL, fino a 300 m; l'iO-WL si collega al modulo iO tramite bus RS485 (A–A, B–B) („RS485 connection"), fino a 300 m („up to 300 m"); al massimo 8 moduli di espansione del sistema („up to 8 system expansion modules", nello schema indicati con *); il polo negativo dell'alimentazione 12–28 V dell'iO-WL e del modulo iO è comune, l'altro iO-WL riceve una propria alimentazione 12–28 V.

- filo rosso („Red wire")
- filo blu („Blue wire")
- filo nero („Black wire")
- filo bianco („White wire")
- W collegamento senza fili („Wireless connection"), fino a 300 m („up to 300 m")

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

3.9 Modulo di espansione iO-8

Se al comunicatore servono più ingressi (IN) o uscite (OUT), collegagli il modulo di espansione cablato **iO-8**. La descrizione dettagliata del modulo di espansione: Modulo di espansione di ingressi e uscite iO8 – manuale di installazione.

Trikdis iO8 modulo di espansione cablato

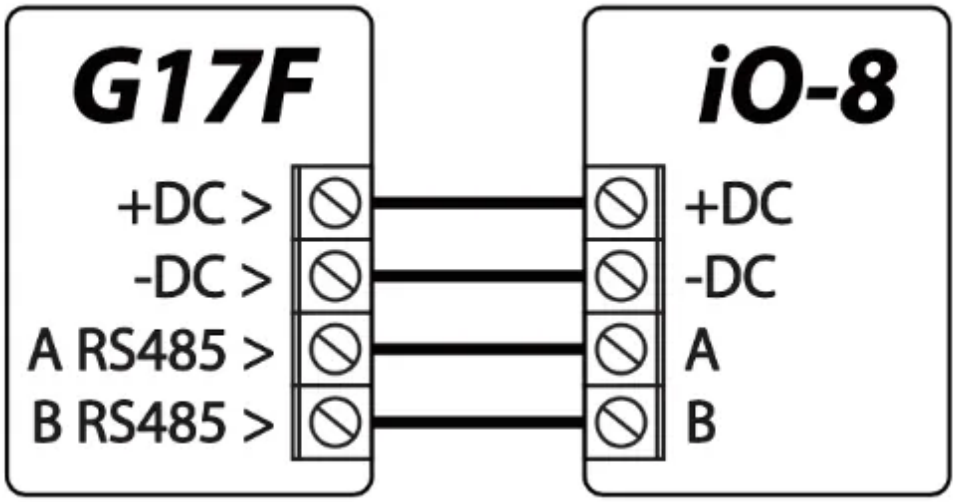


Figura 33. Collegamento del modulo di espansione iO-8: il morsetto **+DC** del G17F va al morsetto **+DC** dell'iO-8, il **−DC** al **−DC**, l'**A RS485** all'**A**, il **B RS485** al **B**.

3.10 Moduli di espansione della serie LORA

I moduli LORA si collegano al G17F via radio: il ricetrasmettitore **RF-LORA** va sul bus RS485 e mantiene il collegamento fino a 5000 m con i moduli di espansione **iO-LORA**, **iO8-LORA** e **REL-LORA** e con il pulsante antipanico **PB-LORA**. I moduli si aggiungono nella pagina **Modules** di TrikdisConfig (punto 5.5).

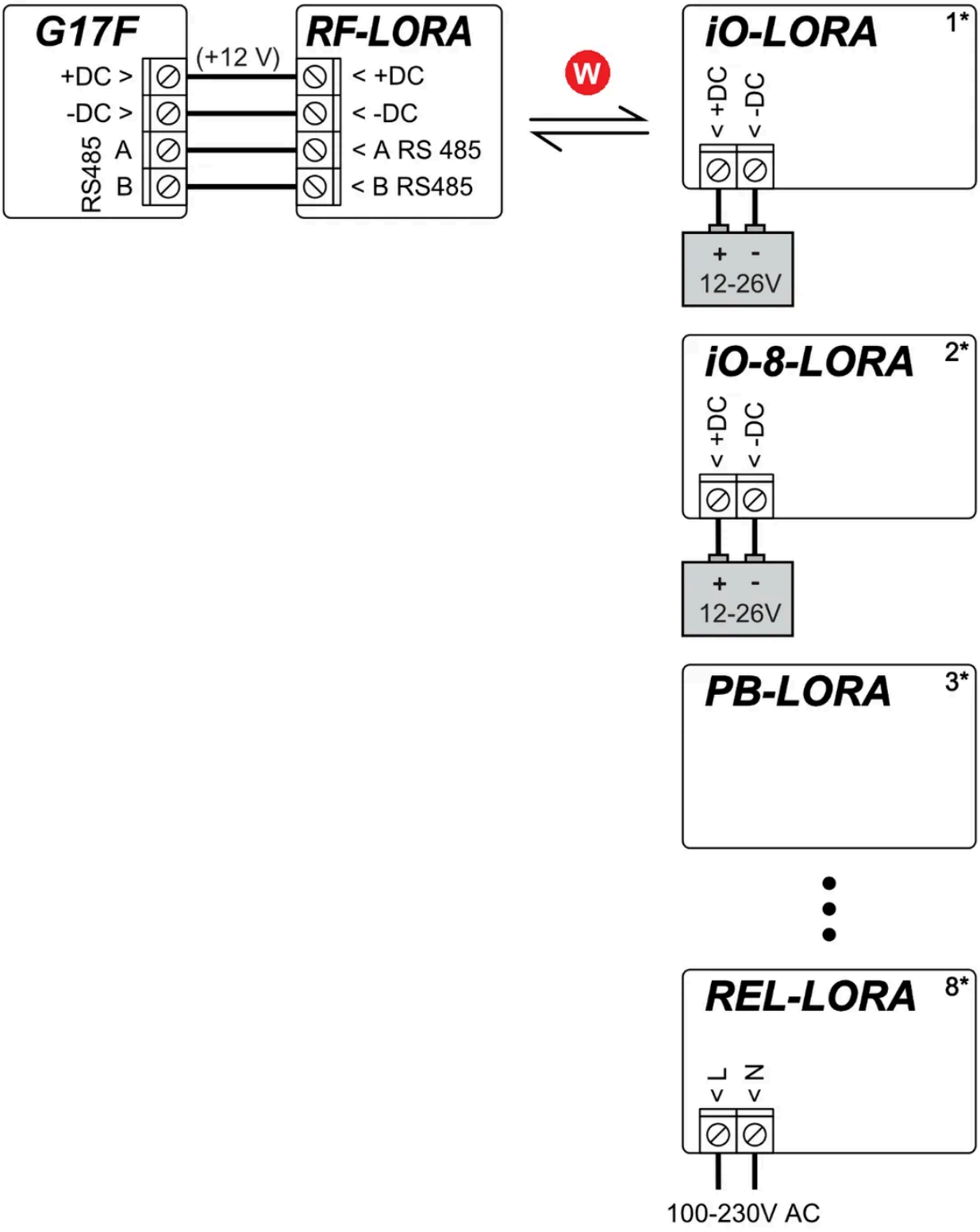


Figura 34. Collegamento dei moduli LORA: il morsetto **+DC** del G17F va al morsetto **+DC** (+12 V) dell'RF-LORA, il **–DC** al **–DC**; RS485 – il morsetto **A** del G17F va al morsetto **A RS 485** dell'RF-LORA, il **B** al **B RS485**; collegamento radio fino a 5000 m con i moduli **iO-LORA**, **iO8-LORA**, **PB-LORA** … **REL-LORA** (nell'angolo dei moduli le indicazioni 1, *2*, 3* … 8*); l'iO-LORA e l'iO8-LORA ricevono una propria alimentazione 12–26 V (**+DC**, **–DC**), il REL-LORA l'alimentazione di rete 100–230 V AC (**L**, **N**).

- W collegamento senza fili („Wireless connection"), fino a 5000 m („up to 5000 m")

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

servizio.

Trikdis RF-LORA modulo di espansione wireless

Trikdis IO-LORA modulo di espansione wireless

Trikdis IO8-LORA modulo di espansione wireless **Trikdis PB-LORA pulsante panico wireless**

3.11 Modulo Wi-Fi W485

Il modulo **W485** invia i messaggi del G17F tramite Wi-Fi, attraverso il router Internet, alla centrale di vigilanza e all'app Protegus 2. Finché c'è la connessione Wi-Fi, il G17F invia i messaggi di evento tramite il W485; se la connessione Wi-Fi si interrompe, li invia tramite la rete mobile (GPRS) e, quando la connessione Wi-Fi si ripristina, torna al W485. La funzione è disponibile dal firmware **1.08** del G17F. **Con il W485 il G17F si può usare anche senza scheda SIM.** Configurazione del W485 per il G17F: punto 5.5.

Trikdis W485 modulo WiFi (RS485)

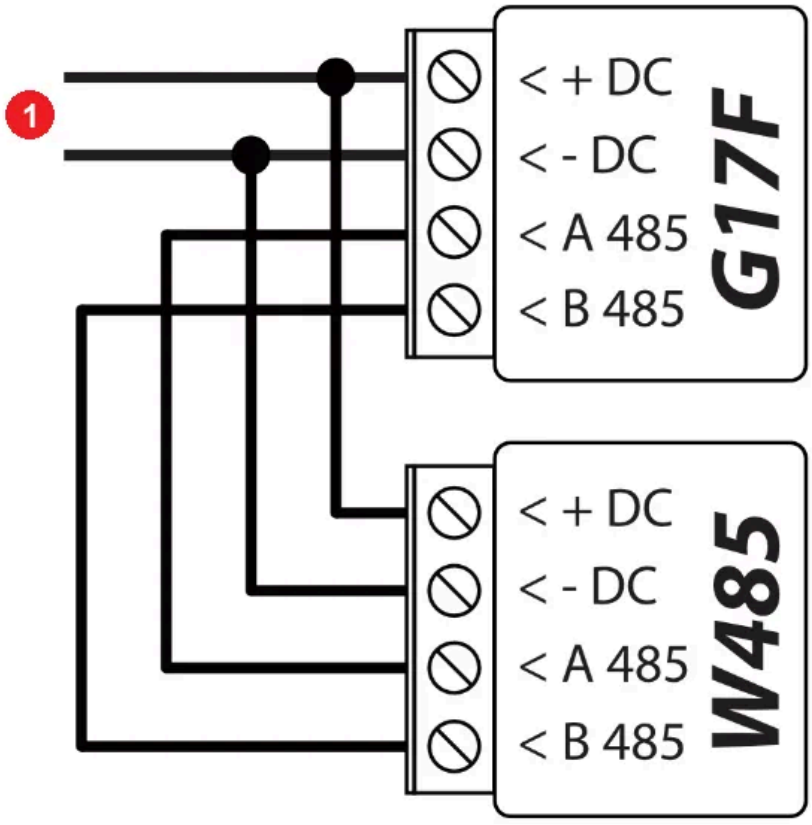


Figura 35. Collegamento del modulo W485: il polo positivo dell'alimentatore va al morsetto **+DC** del G17F e del W485, il negativo al **–DC**; collegamento RS485 („RS485 connection"), fino a 100 m („up to 100 m"): il morsetto **A 485** del G17F va al morsetto **A 485** del W485, il **B 485** al **B 485**.

- 1 alimentatore („Power supply"), 12 V DC, 0,5 A

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.

3.12 Modulo Ethernet E485

Il modulo **E485** invia i messaggi del G17F tramite connessione Internet cablata alla centrale di vigilanza e all'app Protegus 2. Con l'E485 i messaggi passano per l'Internet cablato, il G17F non usa l'Internet mobile. Se la connessione Internet cablata si interrompe, il G17F invia i messaggi tramite Internet mobile e, quando la connessione cablata si ripristina, di nuovo tramite l'E485. La funzione è disponibile dal firmware **1.08** del G17F. **Con l'E485 il G17F si può usare anche senza scheda SIM.** Configurazione dell'E485 per il G17F: punto 5.5.

Trikdis E485 modulo Ethernet (RS485)

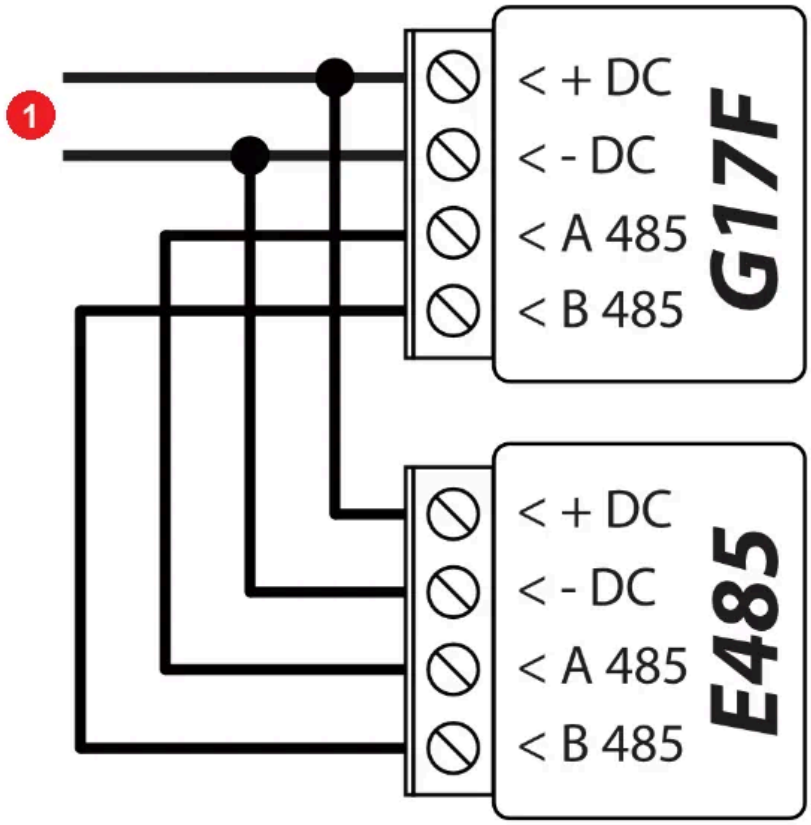


Figura 36. Collegamento del modulo E485: il polo positivo dell'alimentatore va al morsetto **+DC** del G17F e dell'E485, il negativo al **–DC**; collegamento RS485 („RS485 connection"), fino a 100 m („up to 100 m"): il morsetto **A 485** del G17F va al morsetto **A 485** dell'E485, il **B 485** al **B 485**.

- 1 alimentatore („Power supply"), 12 V DC, 0,5 A

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.

3.13 Accensione del comunicatore

Per accendere il comunicatore devi prima garantire l'alimentazione della centrale antincendio (negli schemi il G17F riceve l'alimentazione dall'uscita a 24 V della centrale). Se il comunicatore funziona correttamente, si accendono questi LED:

- il LED **POWER** lampeggia in verde (la tensione di alimentazione è adeguata);
- il LED **NETWORK** è acceso in verde e lampeggia in giallo quando il comunicatore si è connesso alla rete.

- Segnale della rete mobile sufficiente: su rete 2G 5 (cinque lampeggi gialli del LED **NETWORK**), su rete 4G 3 (tre lampeggi gialli).
- Se sul LED **NETWORK** conti meno di 3 lampeggi gialli, il segnale non è sufficiente: scegli un altro punto di installazione oppure usa un'antenna più sensibile (punto 1.7).
- Se la segnalazione è diversa, la spiegazione la trovi al punto 1.6.
- Se nessun LED del G17F si accende, controlla l'alimentazione e i collegamenti.

4. Controllo a distanza

Il G17F si può controllare dall'app **Protegus 2**, con **comando SMS** e con **chiamata telefonica** (durante la chiamata con la tastiera del telefono). Nell'app gli utenti vedono anche lo stato del sistema e ricevono notifiche sugli eventi del sistema; via SMS l'amministratore può modificare anche una parte delle impostazioni.

4.1 Aggiunta del G17F a Protegus 2

In Protegus 2 gli utenti vedono lo stato del sistema e ricevono notifiche sugli eventi del sistema. L'app è disponibile per telefono e per browser (i link per il download sono sotto, alla creazione del sistema).

Prima di aggiungere il sistema

Puoi aggiungere il G17F a Protegus 2 se:

1. contiene una scheda SIM attivata e il codice PIN è stato inserito o disattivato;
2. il servizio Protegus è attivo (**Users & Reporting** → **Enable cloud service**, punto 5.4; via SMS: `CONNECT 123456 PROTEGUS=ON`, punto 4.2);
3. la sua alimentazione è accesa (il LED **POWER** lampeggia in verde);
4. è connesso alla rete (il LED **NETWORK** è acceso in verde e lampeggia in giallo).

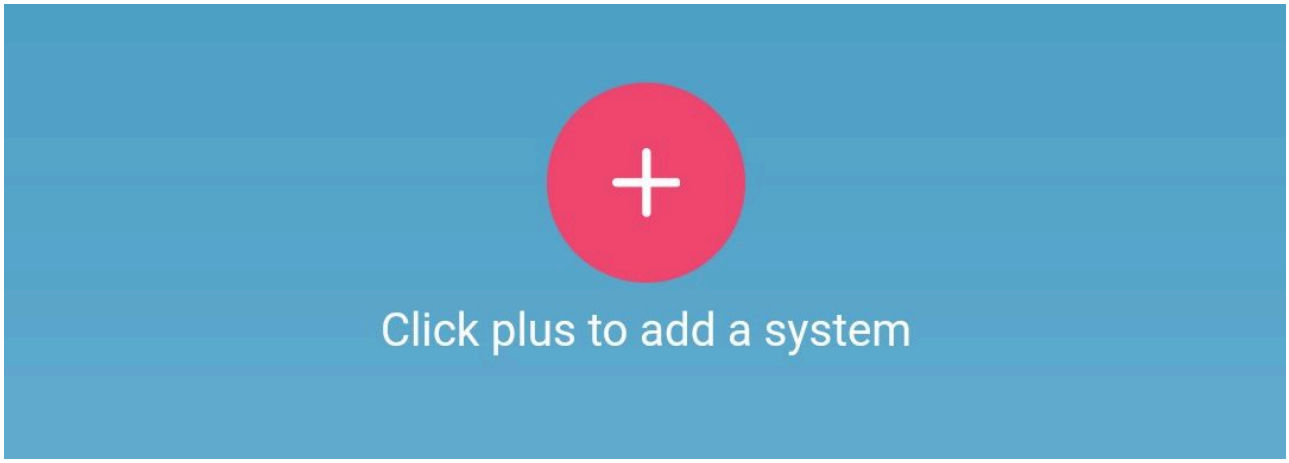
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è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

A rendszer létrehozása a Protegus 2 alkalmazásban

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



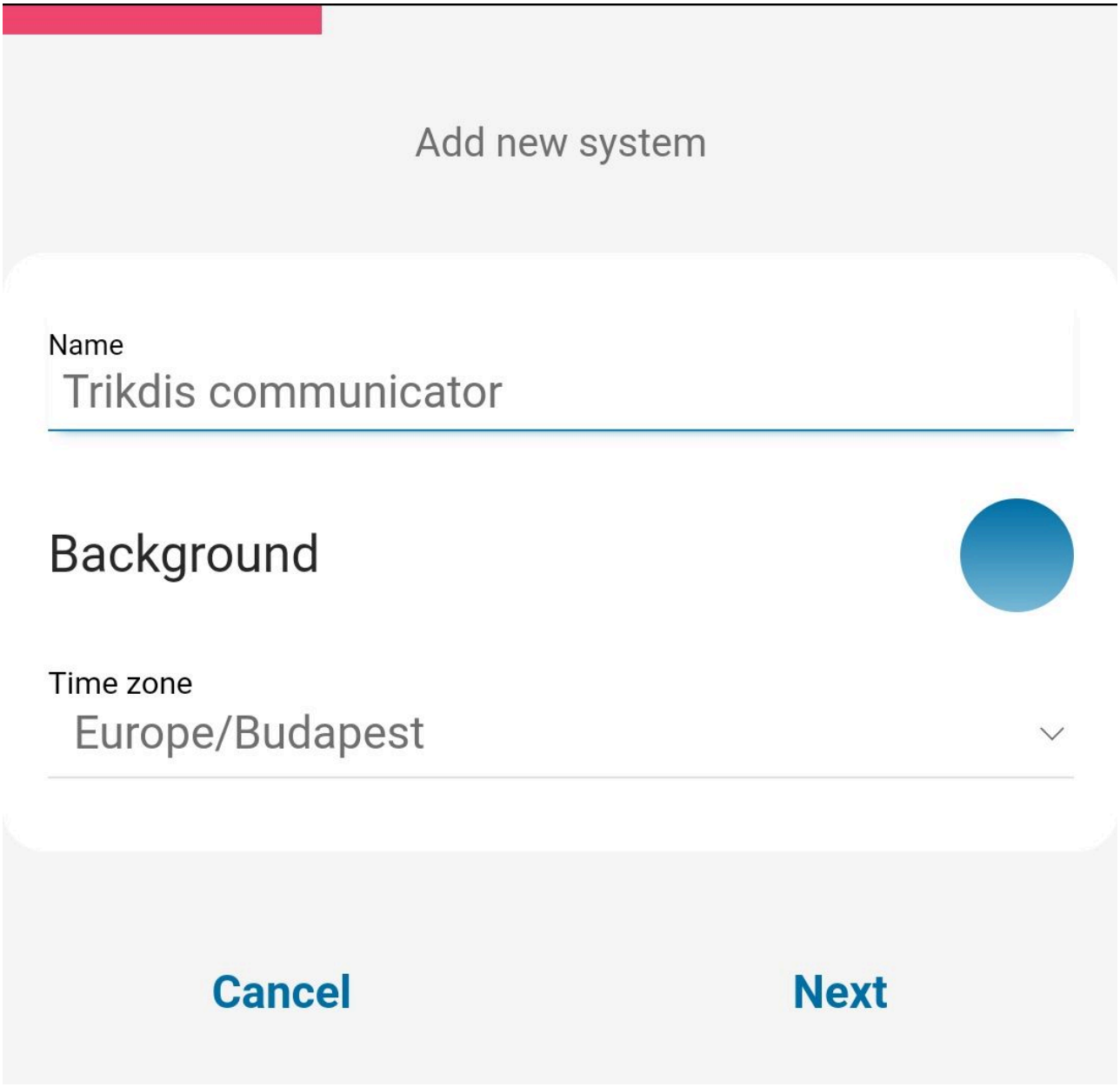
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



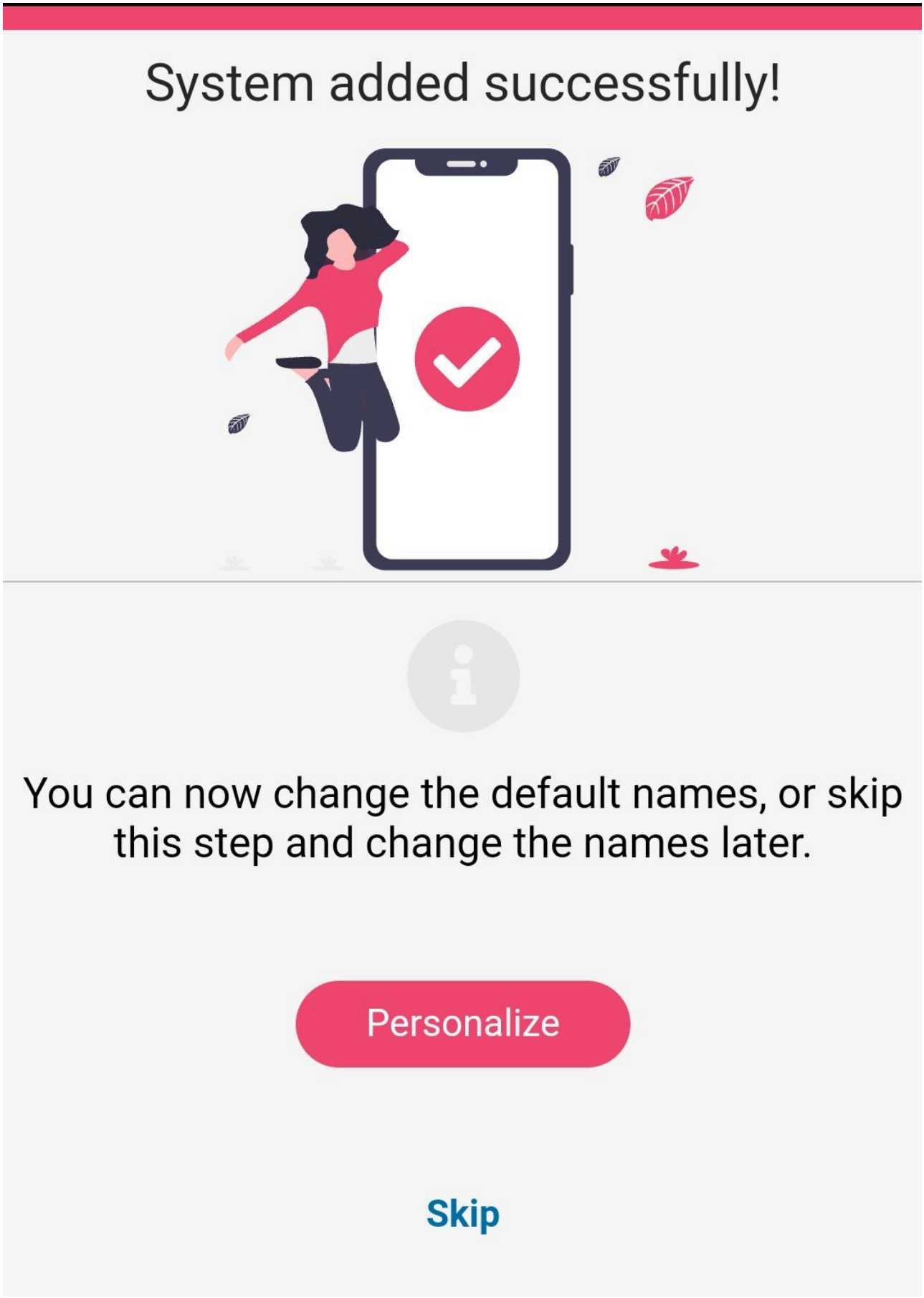
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



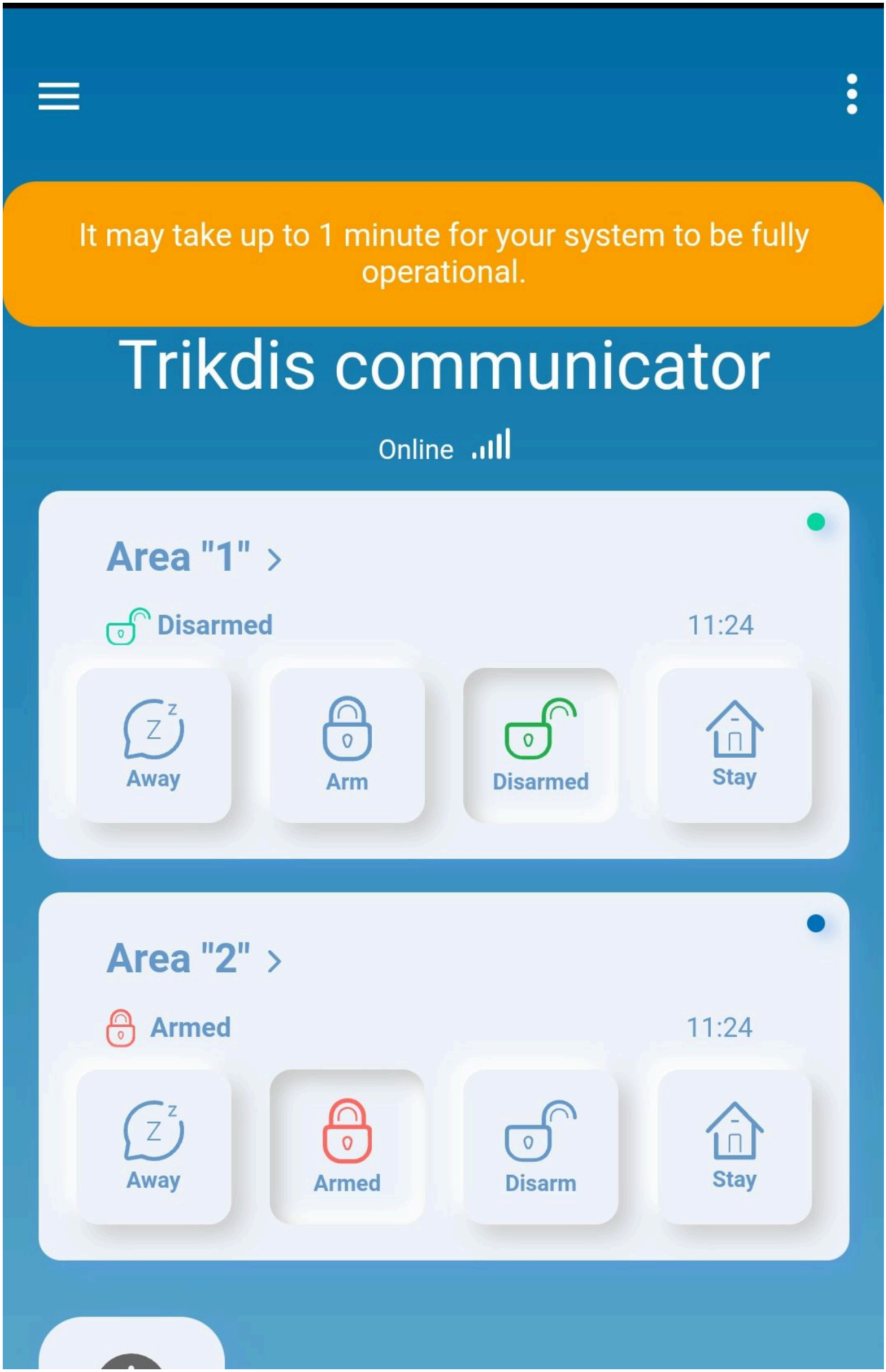
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Per il G17F, durante l'aggiunta fai attenzione a questi punti:

1. Dopo aver inserito l'identificativo univoco (**Unique ID**) fai clic sul pulsante **Next**. L'identificativo lo trovi sull'etichetta presente sul dispositivo e sulla scatola; con la connessione USB lo vedi anche nella barra di stato di TrikdisConfig (**IMEI/Unique ID**, punto 5.1).
2. Se l'installatore ha cambiato il valore di fabbrica `123456` del **Cloud Access Code**, l'app chiede il codice durante l'aggiunta (punto 2.1).

4.2 Configurazione e controllo con messaggio SMS

1. Cambia la password dell'amministratore. Per sicurezza sostituisci la password SMS di fabbrica dell'amministratore. Invia un SMS in questa forma:

`PSW 123456 xxxxxx`

Parte	Significato
`123456`	la password di fabbrica dell'amministratore
`xxxxxx`	la nuova password dell'amministratore di 6 caratteri

2. Autorizza il controllo ad altri utenti. Con SMS e chiamata telefonica il sistema si può controllare solo dai numeri di telefono presenti nell'elenco degli utenti. Dal telefono dell'amministratore invia un SMS con il numero di telefono e il nome delle altre persone, perché anche loro possano controllare il sistema:

`SETN xxxxxx PHONEx=+PHONENR#NAME`

Parte	Significato
`xxxxxx`	la password dell'amministratore di 6 caratteri
`x`	il numero d'ordine dell'utente nell'elenco (se scrivi 1, trasferisci i tuoi diritti di amministratore all'altro utente)
`PHONENR`	il numero di telefono dell'utente
`NAME`	il nome dell'utente

Elenco dei comandi SMS

Comando	Dato	Descrizione
`INFO`		Richiesta di dati sul comunicatore: nella risposta il tipo di comunicatore, il numero IMEI, il numero di serie e la versione del firmware. Esempio: `INFO 123456`
`RESET`		Riavvio del dispositivo. Esempio: `RESET 123456`
`OUTPUTx`	`ON`	Attivazione di un'uscita; „x" è il numero dell'uscita. Esempio: `OUTPUT1 123456 ON`
`OUTPUTx`	`OFF`	Disattivazione di un'uscita; „x" è il numero dell'uscita. Esempio: `OUTPUT1 123456 OFF`

Comando	Dato	Descrizione
`OUTPUTx`	`PULSE=ttt`	Attivazione di un'uscita per alcuni secondi: „x" è il numero dell'uscita OUT, „ttt" un numero di tre cifre, la durata dell'impulso in secondi. Esempio: `OUTPUT1 123456 PULSE=002`
`PSW`	nuova password	Cambio della password. Esempio: `PSW 123456 654123`
`TIME`	`YYYY/MM/DD,12:00:00`	Impostazione della data e dell'ora. Esempio: `TIME 123456 2025/05/09,10:23:00`
`TXTA`	nome dell'impianto	Impostazione del nome dell'impianto. Esempio: `TXTA 123456 House`
`TXTE`	`Z1=` … `Z12=`	Impostazione del testo SMS dell'allarme di zona; Z1…Z12 è il numero della zona di ingresso. Esempio: `TXTE 123456 Z1=ALARM in Zone1`
`TXTR`	`Z1=` … `Z12=`	Impostazione del testo SMS del ripristino di zona; Z1…Z12 è il numero della zona di ingresso. Esempio: `TXTR 123456 Z1=Restore Zone1`
`RDR`	`PhoneNR#SMStext`	Inoltro di un SMS al numero indicato; il numero di telefono deve iniziare con il segno „+" e con il prefisso internazionale del paese. Esempio: `RDR 123456 +37061234567#forwarded text`
`ASKI`		Richiesta via SMS dello stato degli ingressi (IN). Esempio: `ASKI 123456`
`ASKO`		Richiesta via SMS dello stato delle uscite (OUT). Esempio: `ASKO 123456`
`SETN`	`PhoneX=PhoneNR#Name`	Aggiunta del numero di telefono e del nome utente per l'utente „x" („x" è la riga del numero di telefono nell'elenco). Il numero di telefono deve iniziare con il segno „+" e con il prefisso internazionale del paese; il numero di telefono e il nome utente sono separati dal segno #. Esempio: `SETN 123456 PHONE5=+37061234567#JOHN`
`SETN`	`PhoneX=DEL`	Cancellazione dal sistema del numero di telefono e del nome dell'utente. Esempio: `SETN 123456 PHONE5=DEL`
`UUSD`	`*Uusd code#`	Invio di un codice USSD all'operatore (il nome del comando è davvero `UUSD`). Esempio: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON`	Connessione al servizio cloud Protegus. Esempio: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`Protegus=OFF`	Disconnessione dal servizio cloud Protegus. Esempio: `CONNECT 123456 PROTEGUS=OFF`
`CONNECT`	`Code=123456`	Il codice del servizio cloud Protegus. Esempio: `CONNECT 123456 CODE=123456`
`CONNECT`	`IP=0.0.0.0:8000`	Indirizzo IP TCP e porta del canale di collegamento del server principale. Esempio: `CONNECT 123456 IP=0.0.0.0:8000`
`CONNECT`	`IP=0`	Disattivazione del canale principale. Esempio: `CONNECT 123456 IP=0`
`CONNECT`	`ENC=123456`	La chiave di cifratura TRK. Esempio: `CONNECT 123456 ENC=123456`
`CONNECT`	`APN=Internet`	Il nome dell'APN. Esempio: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`USER=user`	Il nome utente dell'APN. Esempio: `CONNECT 123456 USER=User`
`CONNECT`	`PSW=password`	La password dell'APN. Esempio: `CONNECT 123456 PSW=Password`

4.3 Controllo delle uscite PGM con chiamata telefonica

Se al sistema non è ancora stato aggiunto nessun utente, chi chiama per primo il G17F diventa l'amministratore del sistema, e solo lui può controllare il G17F con chiamata e comandi SMS. Se vuoi autorizzare il controllo con chiamata anche ad altri utenti, aggiungili in TrikdisConfig (punto 5.4) oppure dai loro il diritto con un comando SMS (punto 4.2).

Se vuoi controllare un'uscita PGM a distanza:

- L'utente deve avere il diritto di controllare le uscite (OUT) (punto 5.4) e all'uscita (OUT) in TrikdisConfig deve essere assegnato il tipo **Remote control** (pagina **PGM**, **Output definition**, punto 5.7).
- Chiama il numero della scheda SIM del G17F. Il G17F risponde alla chiamata e con la tastiera del telefono puoi digitare i comandi secondo la tabella.

Tasti	Funzione	Descrizione
`[uscita]*[stato]#`	controllo dell'uscita (OUT) scelta	Commuta l'uscita PGM indicata. Stato: **0** – uscita disattivata; **1** – uscita attivata; **2** – disattivata per la durata dell'impulso; **3** – attivata per la durata dell'impulso (la durata dell'impulso si imposta nella tabella **PGM** di TrikdisConfig, punto 5.7). Il **#** indica la fine del comando. Esempi: attivazione dell'uscita 1: `1*1#`; disattivazione dell'uscita 1: `1*0#`; attivazione dell'uscita 2 per la durata dell'impulso indicata nella tabella **PGM**: `2*3#`
`#`	ripresa del comando	Se hai sbagliato il comando, premi il tasto **#** del telefono e digita di nuovo il comando.

5. Le pagine di TrikdisConfig

Questo capitolo descrive le pagine della finestra di programmazione di TrikdisConfig, nell'ordine in cui si susseguono nel menu a sinistra. Collegamento del G17F con cavo USB: capitolo 2; a distanza: capitolo 6.

5.1 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 37. La barra di stato del G17F: **Status: Ready**, **Device: G17F_54S0**, **BL** 2.03, **FW** 1.18, **State: USB**, **Role: Administrator**; a sinistra il campo **IMEI/Unique ID** e il campo del numero di serie. Per il G17F nel campo **Device** deve comparire il tipo **G17F**.

Facendo clic sul pulsante **Read [F4]** il programma legge e mostra le impostazioni attuali memorizzate nel G17F. Imposta i parametri necessari in base alle descrizioni delle pagine che seguono.

5.2 Pagina „System Options”

Le impostazioni generali del dispositivo, in due schede: **System general** e **Access**.

Scheda System general

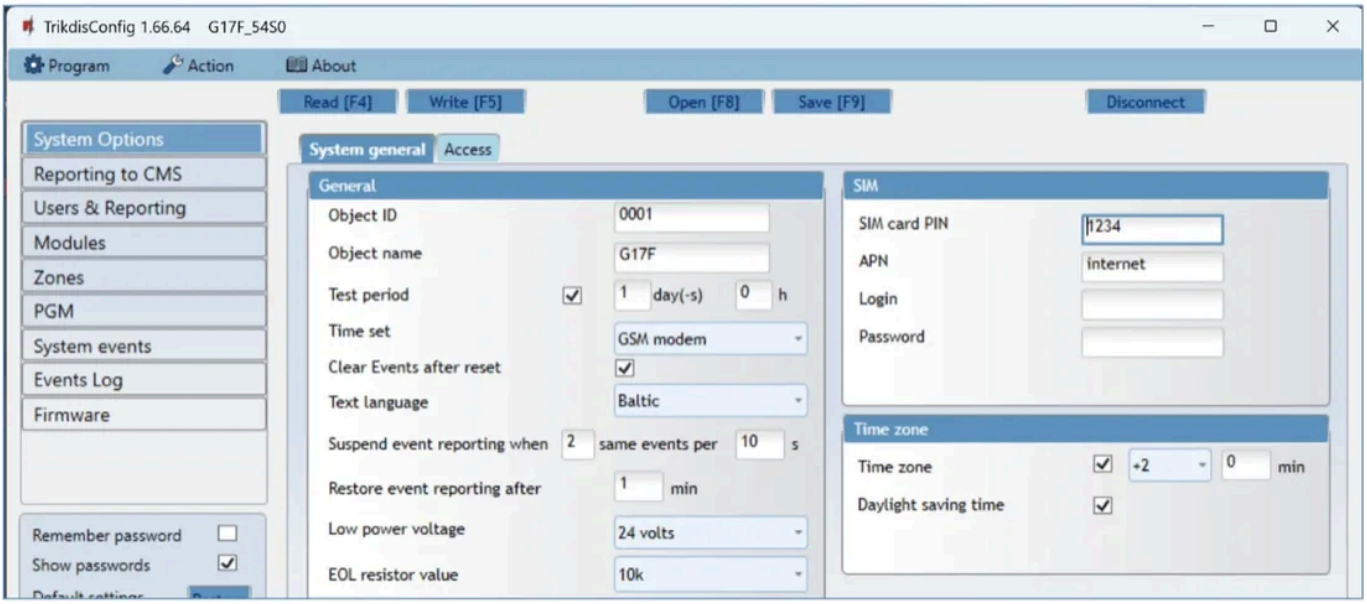


Figura 38. TrikdisConfig – **System Options**, scheda **System general**: i gruppi **General**, **SIM** e **Time zone**. In fondo al gruppo **General** si vede anche il campo **EOL resistor value** (nell'immagine 10k).

Gruppo General

- **Object ID** – se gli eventi vanno alla centrale di vigilanza, inserisci il codice identificativo dell'impianto ricevuto dalla centrale di vigilanza (numero esadecimale di 4 caratteri, 0–9, A–F). Non usare i codici FFFE e FFFF.
- **Object name** – il nome dell'impianto; questo nome compare negli SMS inviati agli utenti.
- **Test period** – se spuntato, il G17F invia un messaggio „Test” all'intervallo impostato.
- **Time set** – la fonte della sincronizzazione dell'ora. **IP server**: l'ora si allinea a quella del ricevitore IP; **Cellular modem** (nell'immagine **GSM modem**): a quella del server dell'operatore mobile.
- **Clear Events after reset** – se spuntato, al riavvio (reset) tutti i messaggi di evento non inviati vengono cancellati.

- **Text language** – la lingua dei messaggi SMS: il dispositivo usa negli SMS i caratteri specifici della lingua scelta.
- **Suspend event reporting when … same events per … s** – sospensione dell'invio degli eventi, se il numero indicato di eventi identici si ripete entro i secondi indicati.
- **Restore event reporting after … min** – dopo questo tempo termina la sospensione dell'invio degli eventi (0–999 minuti).
- **Low power voltage** – indica con quale tensione di alimentazione (12 V o 24 V) funziona il dispositivo; a questa si adeguano i messaggi sulla bassa tensione di alimentazione.

Gruppo SIM

- **SIM card PIN** – il codice PIN della scheda SIM.
- **APN** – il nome del punto di accesso a Internet mobile dell'operatore mobile. Devi inserirlo se i messaggi di evento vanno all'app Protegus 2 o alla centrale di vigilanza tramite connessione dati mobile. I dati degli operatori nazionali ed europei: Impostazione dell'APN – elenco degli operatori mobili europei.
- **Login**, **Password** – il nome utente e la password dell'APN, se l'operatore mobile li richiede.

Gruppo Time zone

- **Time zone** – il fuso orario del paese (Italia: +1).
- **Daylight saving time** – se spuntato, l'orologio interno del dispositivo passa automaticamente all'ora legale e all'ora solare.

Scheda Access

Nella scheda **Access** imposti i codici di accesso e i permessi dell'installatore.

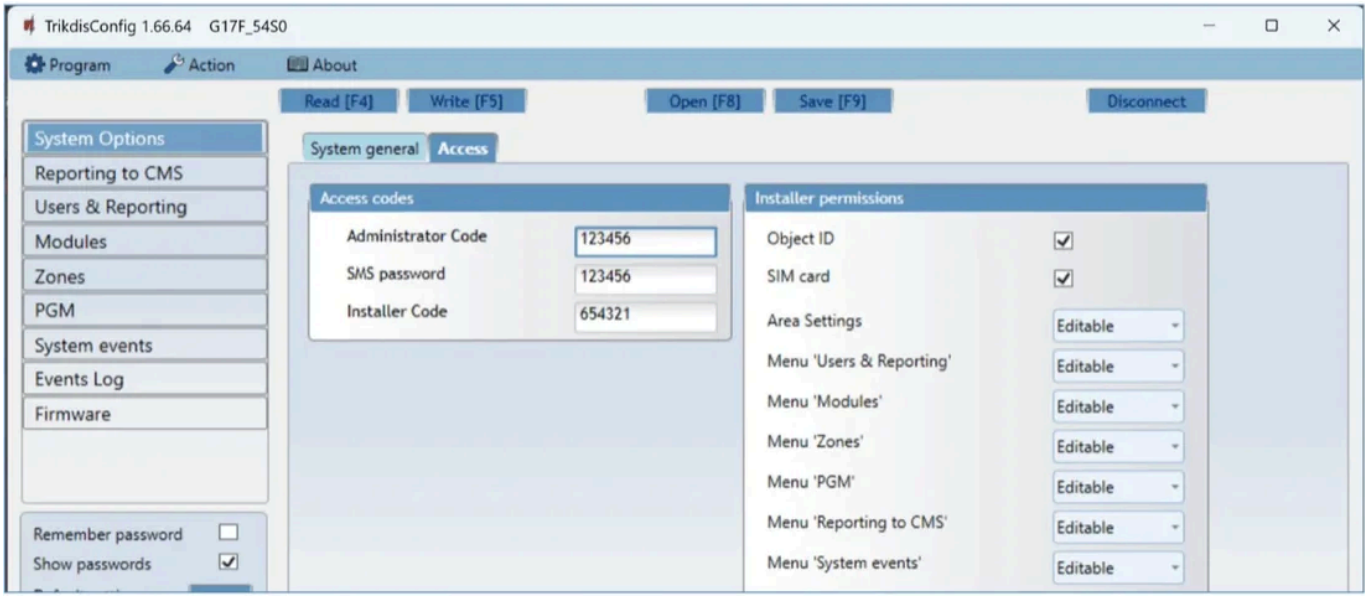


Figura 39. TrikdisConfig – **System Options**, scheda **Access**: il gruppo **Access codes** con i codici di fabbrica e il gruppo **Installer permissions**, in cui l'amministratore indica le impostazioni modificabili dall'installatore.

Gruppo Access codes

- **Administrator Code** – accesso completo alle impostazioni (di fabbrica `123456`).
- **SMS password** – password per il controllo e la programmazione a distanza via SMS (di fabbrica `123456`).
- **Installer Code** – accesso limitato alla modifica delle impostazioni (di fabbrica `654321`).

Gruppo Installer permissions – qui l'amministratore imposta quali parametri può modificare l'installatore.

Per sicurezza cambia i codici di fabbrica. La password SMS la puoi cambiare anche via SMS (`PSW`, punto 4.2).

5.3 Pagina „Reporting to CMS"

Il G17F invia i messaggi alla centrale di vigilanza tramite Internet mobile (IP) o via SMS. Al canale principale si può associare un canale di riserva: il dispositivo lo usa se la connessione sul canale principale si interrompe.

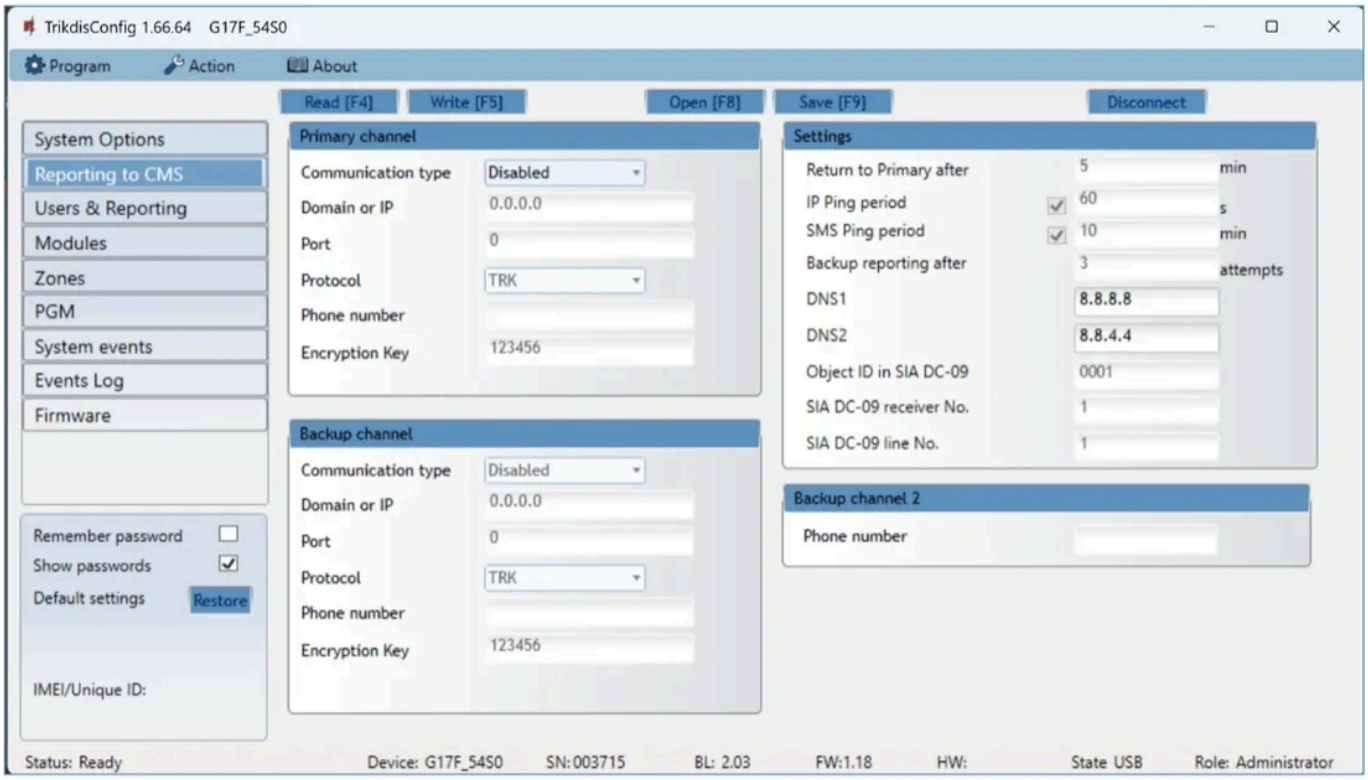


Figura 40. TrikdisConfig – **Reporting to CMS**: i gruppi **Primary channel**, **Backup channel**, **Settings** e **Backup channel 2**. Nell'immagine: **Communication type: Disabled**, **Return to Primary after** 5 minuti, **IP Ping period** 60 s, **SMS Ping period** 10 minuti, **Backup reporting after** 3 tentativi, **DNS1** 8.8.8.8, **DNS2** 8.8.4.4.

I messaggi inviati alla centrale di vigilanza sono codificati e protetti da password. Per ricevere i messaggi e inoltrarli al software della centrale di vigilanza serve un ricevitore Trikdis:

- per i messaggi IP: il programma ricevitore **IPcom** (Windows o Linux), il ricevitore hardware IP/SMS **RL14** o il ricevitore multicanale **RM14**;
- per i messaggi SMS: il ricevitore hardware IP/SMS **RL14**, il ricevitore multicanale **RM14** o il ricevitore SMS **GM14**.

Trikdis IPcom v5 Windows ricevitore software | **Trikdis IPcom v5 Linux ricevitore software**

La connessione SMS come canale di riserva è estremamente utile, perché funziona anche quando nella rete dell'operatore mobile la connessione Internet cade. Come canale principale l'SMS non è consigliato.

Gruppo Primary channel (canale principale)

- **Communication type** – il modo di collegamento con il ricevitore della centrale di vigilanza.
- **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- **Port** – la porta di rete del ricevitore.

- **Protocol** – i ricevitori IP Trikdis ricevono i messaggi inviati con il protocollo **TRK**; per i ricevitori IP in grado di ricevere messaggi SIA DC-09 scegli il protocollo **DC-09_2007** o **DC-09_2012**.
- **Phone number** – (solo per SMS) il numero di telefono del ricevitore SMS Trikdis, che inizia con il prefisso del paese (per esempio 39xxxxxxxxx).
- **Encryption Key** – chiave di cifratura di 6 cifre; deve coincidere con la chiave di cifratura del ricevitore.

Gruppo Backup channel (canale di riserva) – attivalo perché il G17F, quando la connessione si interrompe, invii i messaggi sul canale di riserva. Le sue impostazioni sono le stesse del canale principale.

Gruppo Settings

- **Return to Primary after** – dopo questo tempo il G17F tenta di tornare al canale principale.
- **IP Ping period** – l'intervallo di invio dei segnali PING interni che controllano la connessione. I segnali PING vanno solo sul canale IP; il ricevitore non li inoltra al software della centrale di vigilanza, così non lo appesantiscono. Il software riceve una notifica solo se il ricevitore non riceve PING dal dispositivo per il tempo impostato.
- **SMS Ping period** – l'intervallo in minuti del segnale PING inviato sul canale SMS. Per usare il canale spunta la casella e inserisci l'intervallo.
- **Backup reporting after** – dopo quanti tentativi di invio falliti il G17F deve inviare sul canale di riserva (**Backup channel**).
- **DNS1**, **DNS2** – i server DNS che traducono il nome di dominio in indirizzo IP. Servono se nel campo **Domain or IP** del canale hai scritto un nome di dominio (e non un indirizzo IP). Di fabbrica sono i server DNS di Google.

L'intervallo di PING

Di fabbrica il ricevitore invia al software della centrale di vigilanza il messaggio „Connection lost" (connessione interrotta) se non riceve PING per un tempo pari a tre volte l'intervallo di invio PING del dispositivo: con un **IP Ping period** di 3 minuti, per esempio, dopo 9 minuti. I messaggi PING mantengono attiva anche la connessione tra il dispositivo e il ricevitore – la connessione attiva serve per la configurazione e il controllo a distanza. Consigliamo di impostare l'intervallo di PING al massimo a 5 minuti.

I campi seguenti si vedono solo se nel campo **Protocol** del canale hai scelto il protocollo **DC-09_2007** o **DC-09_2012**:

- **Object ID in SIA DC-09** – il numero dell'impianto; con il protocollo DC-09 questo numero viene inserito nei messaggi. Inserisci il numero esadecimale di 3–16 caratteri ricevuto dalla centrale di vigilanza.
- **SIA DC-09 receiver No.** – il numero del ricevitore.
- **SIA DC-09 line No.** – il numero della linea nel ricevitore.

Gruppo Backup channel 2

- **Phone number** – (solo per SMS) il numero di telefono del ricevitore SMS Trikdis, che inizia con il prefisso del paese (per esempio 39xxxxxxxxx).

5.4 Pagina „Users & Reporting"

Le impostazioni degli utenti, del cloud Protegus e delle risposte SMS, in tre schede: **Users**, **SMS answer texts** e **SMS for Panel events**.

Scheda Users

Nella scheda **Users** indichi gli utenti che ricevono SMS e chiamate, e qui attivi il cloud Protegus.

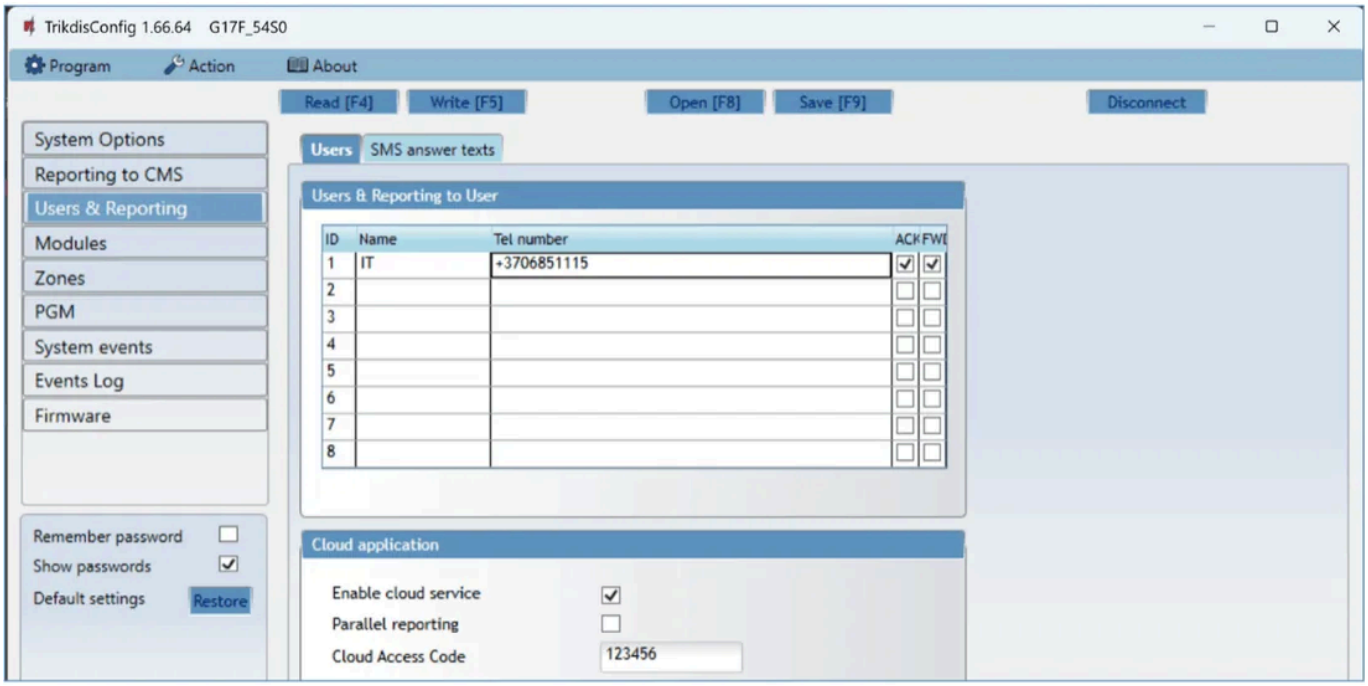


Figura 41. TrikdisConfig – **Users & Reporting**, scheda **Users**: la tabella **Users & Reporting to User** (**ID**, **Name**, **Tel number**, **ACK**, **FWD**) e il gruppo **Cloud application** (**Enable cloud service**, **Parallel reporting**, **Cloud Access Code**).

Gruppo Users & Reporting to User

- **ID** – il numero d'ordine dell'utente nell'elenco.
- **Name** – il nome dell'utente; negli SMS di evento compare questo nome.
- **Tel number** – il numero di telefono dell'utente a cui vanno gli SMS; inseriscilo in formato internazionale (+39…).
- **PGM** – se spuntato, l'utente può controllare le uscite a distanza (nell'immagine sopra questa colonna non si vede).
- **ACK** – se spuntato, il G17F dopo ogni comando SMS ricevuto invia all'utente un SMS di risposta (il testo delle risposte: scheda **SMS answer texts**).
- **FWD** – se spuntato, il G17F inoltra all'utente gli SMS che arrivano da numeri esterni al sistema (per esempio l'avviso sul credito della scheda SIM o i messaggi pubblicitari).

Gruppo Cloud application

- **Enable cloud service** – attivazione del servizio Protegus: così il G17F scambia dati con l'app Protegus 2 e si può configurare anche a distanza con TrikdisConfig (capitolo 6).
- **Parallel reporting** – invio parallelo: i messaggi vanno contemporaneamente sul canale principale e a Protegus 2.
- **Cloud Access Code** – codice di 6 cifre per l'accesso a Protegus 2 (di fabbrica `123456`).

Scheda SMS answer texts

Nella colonna **SMS text** puoi modificare il testo delle risposte inviate ai comandi SMS.

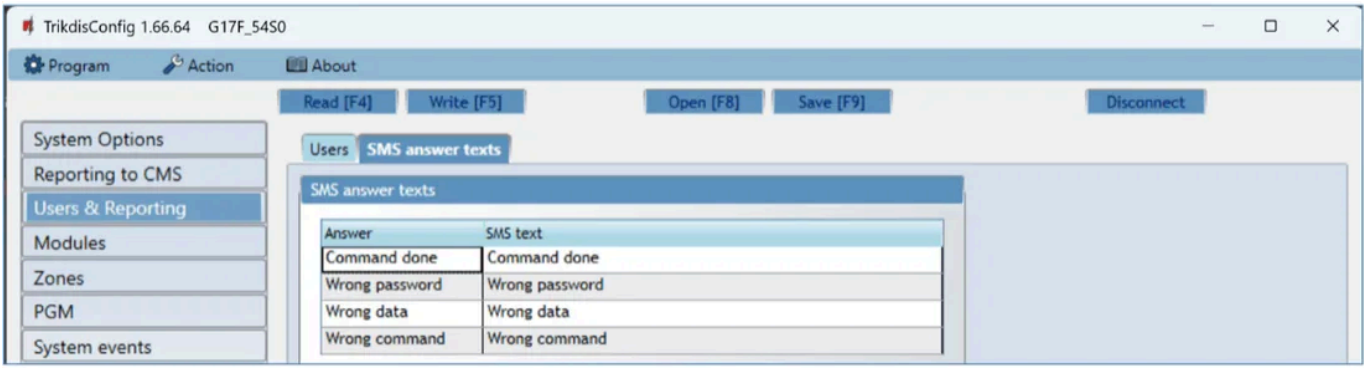


Figura 42. TrikdisConfig – **Users & Reporting**, scheda **SMS answer texts**: **Command done** (comando eseguito), **Wrong password** (password errata), **Wrong data** (dato errato), **Wrong command** (comando errato).

Scheda SMS for Panel events

Questa scheda compare solo se nella scheda **Users** hai inserito almeno un numero di telefono di un utente. Qui imposti se gli utenti devono ricevere SMS e/o chiamate sugli eventi della centrale antincendio.

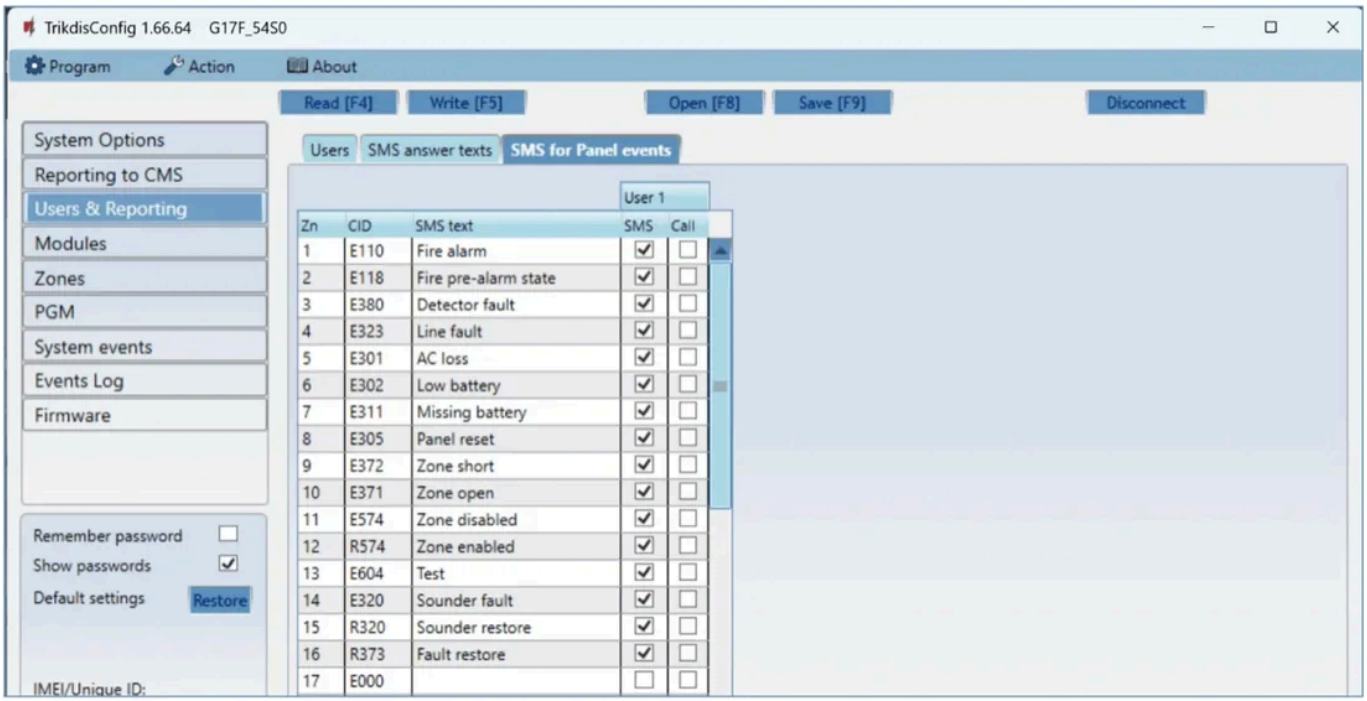


Figura 43. TrikdisConfig – **Users & Reporting**, scheda **SMS for Panel events**: gli eventi della centrale con codice Contact ID, per esempio E110 allarme incendio (**Fire alarm**), E118 preallarme (**Fire pre-alarm state**), E380 guasto rivelatore (**Detector fault**), E301 mancanza di alimentazione di rete (**AC loss**), E302 batteria scarica (**Low battery**); nella colonna **User 1** le caselle **SMS** e **Call**.

- **Zn** – il numero d'ordine dell'evento nell'elenco.
- **CID** – il codice Contact ID dell'evento.
- **SMS text** – il testo SMS dell'evento.
- **User SMS/Call** – per ogni evento puoi scegliere se l'utente deve ricevere un SMS e/o una chiamata.

Il modem effettua la chiamata su 2G o VoLTE. Dove l'operatore ha spento il 2G e non ha approvato il modem per la VoLTE, l'SMS arriva ma il telefono non squilla. Non è un errore di configurazione. In questi casi usa gli SMS e l'app Protegus 2.

5.5 Pagina „Modules”

L'elenco dei moduli e delle centrali antincendio collegati al bus RS485, nonché le impostazioni dei moduli W485 ed E485.

Scheda RS485 modules

Nell'elenco indichi un modulo o una centrale antincendio per riga (al massimo 8).

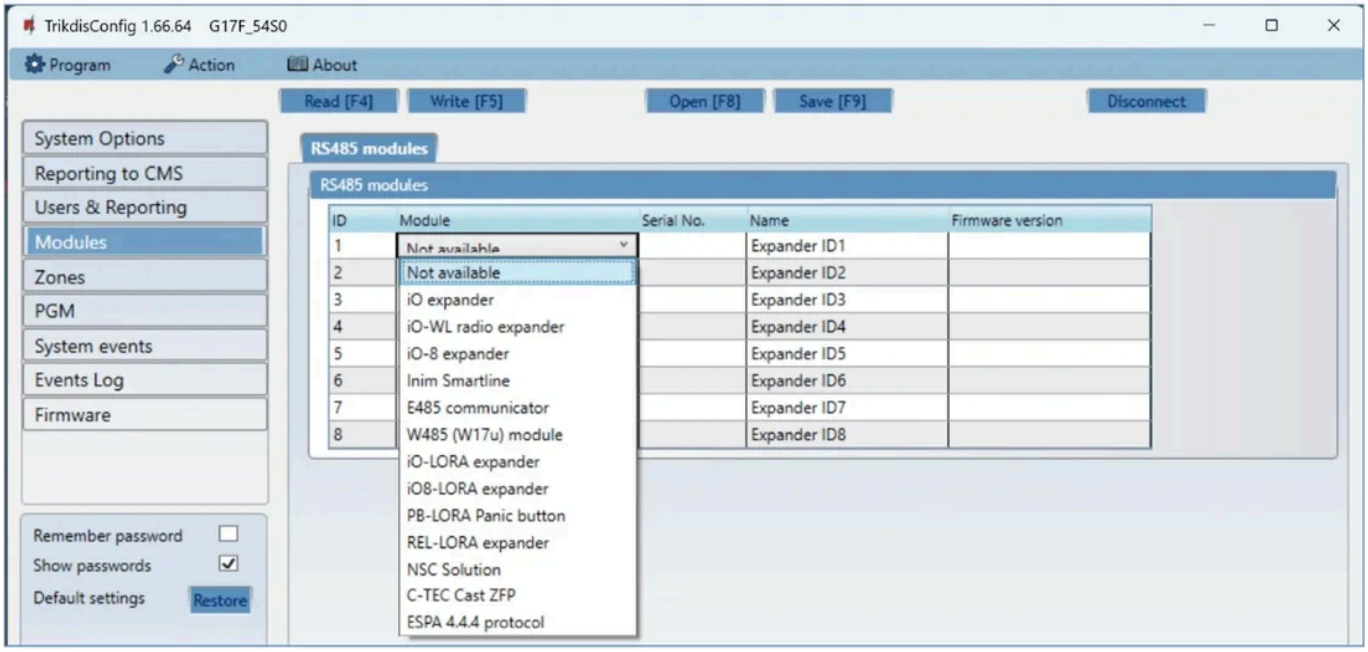


Figura 44. TrikdisConfig – **Modules**, scheda **RS485 modules**: otto righe (ID 1–8); nella prima riga è aperto l'elenco **Module** con i moduli e le centrali antincendio selezionabili.

- **ID** – il numero d'ordine del modulo nell'elenco.
- **Module** – il modulo o la centrale usati: iO, iO-WL, iO-8, INIM Smartline, E485, W485, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, NSC Solution, C-TEC Cast ZFP, ESPA 4.4.4.
- **Serial No.** – numero obbligatorio di 6 cifre; lo trovi sull'involucro e sulla confezione del modulo.
- **Name** – il nome del modulo (a piacere).
- **Firmware version** – la versione del firmware del modulo; compare quando il G17F trova il modulo collegato.

Scheda W485 settings

Le impostazioni del modulo Wi-Fi W485 (W17u) (il collegamento: punto 3.11).

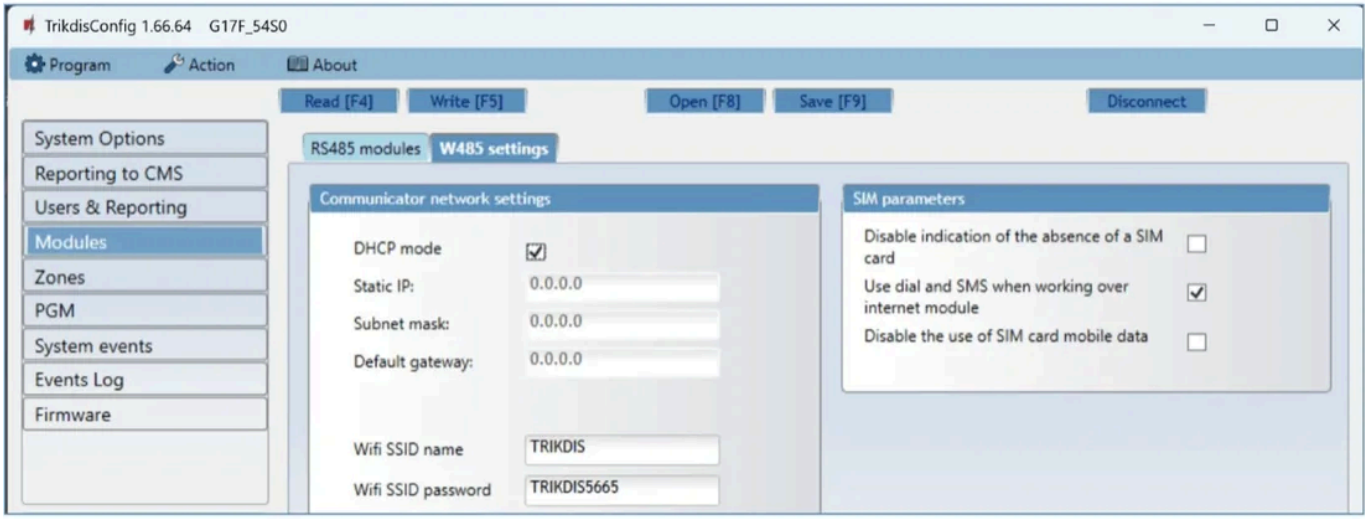


Figura 45. TrikdisConfig – **Modules**, scheda **W485 settings**: il gruppo **Communicator network settings** (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**, **Wifi SSID name**, **Wifi SSID password**) e il gruppo **SIM parameters**.

Gruppo Communicator network settings

- **DHCP mode** – il modo di registrazione in rete del modulo Wi-Fi (manuale o automatico). Se spuntato (modo automatico), il modulo riconosce automaticamente le impostazioni di rete (maschera di sottorete, gateway) e riceve un indirizzo IP.
- **Static IP** – indirizzo IP statico in modo manuale.
- **Subnet mask** – maschera di sottorete in modo manuale.
- **Default gateway** – gateway predefinito in modo manuale.
- **Wifi SSID name** – il nome della rete Wi-Fi a cui si collega il W485 (W17u).
- **Wifi SSID password** – la password della rete Wi-Fi.

Gruppo SIM parameters

- **Disable indication of the absence of a SIM card** – se spuntato, il G17F non segnala l'assenza della scheda SIM.
- **Use dial and SMS when working over internet module** – se spuntato, il G17F si può controllare anche con chiamata e SMS. Se non è spuntato e c'è la rete Wi-Fi, chiamate e SMS non vengono usati; se non è spuntato e non c'è la rete Wi-Fi, il G17F gestisce le chiamate e gli SMS e invia SMS all'utente.
- **Disable the use of SIM card mobile data** – se spuntato, il G17F non usa la connessione dati mobile della scheda SIM: i dati vanno solo tramite il modulo W485. Se la rete Wi-Fi si interrompe, il G17F conserva i dati nella sua memoria e, al ritorno del Wi-Fi, li invia tramite il modulo W485.

Scheda E485 settings

Le impostazioni del modulo Ethernet E485 (il collegamento: punto 3.12).

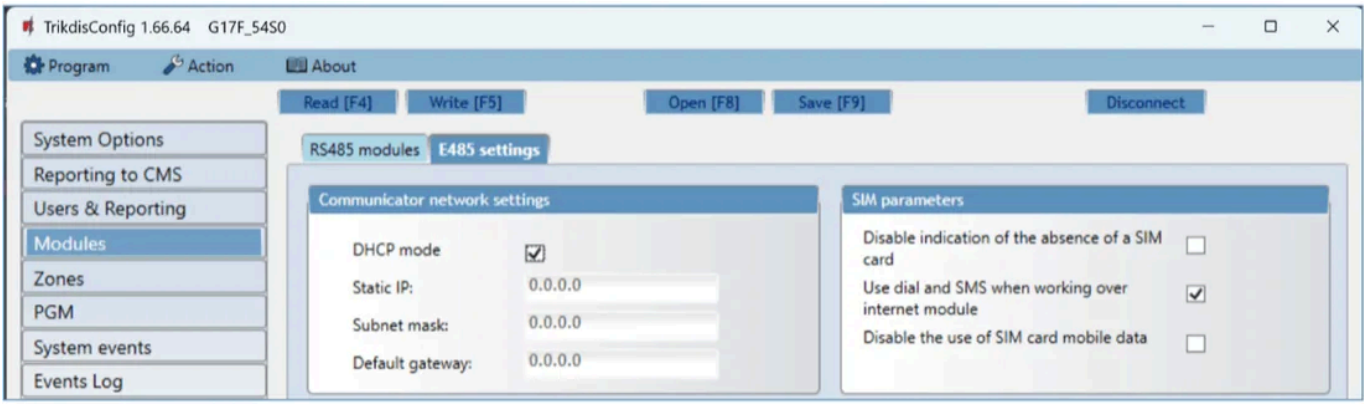


Figura 46. TrikdisConfig – **Modules**, scheda **E485 settings**: il gruppo **Communicator network settings** (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**) e il gruppo **SIM parameters**.

Gruppo Communicator network settings

- **DHCP mode** – il modo di registrazione in rete del modulo Ethernet (manuale o automatico).
- **Static IP** – indirizzo IP statico in modo manuale.
- **Subnet mask** – maschera di sottorete in modo manuale.
- **Default gateway** – gateway predefinito in modo manuale.

Gruppo SIM parameters

- **Disable indication of the absence of a SIM card** – se spuntato, il G17F non segnala l'assenza della scheda SIM.
- **Use dial and SMS when working over internet module** – se spuntato, il G17F si può controllare anche con chiamata e SMS. Se non è spuntato e c'è Internet, SMS e chiamate non vengono usati; se non è spuntato e non c'è Internet, il G17F gestisce le chiamate e gli SMS e invia SMS all'utente.
- **Disable the use of SIM card mobile data** – se spuntato, il G17F non usa la connessione dati mobile della scheda SIM: i dati vanno solo tramite il modulo E485. Se Internet si interrompe, il G17F conserva i dati nella sua memoria e, al ritorno di Internet, li invia tramite il modulo E485.

5.6 Pagina „Zones”

Le impostazioni delle zone (ingressi) in due schede: **Zones settings** e **SMS & Call reporting**.

Scheda Zones settings

Nella tabella imposti una zona per riga.

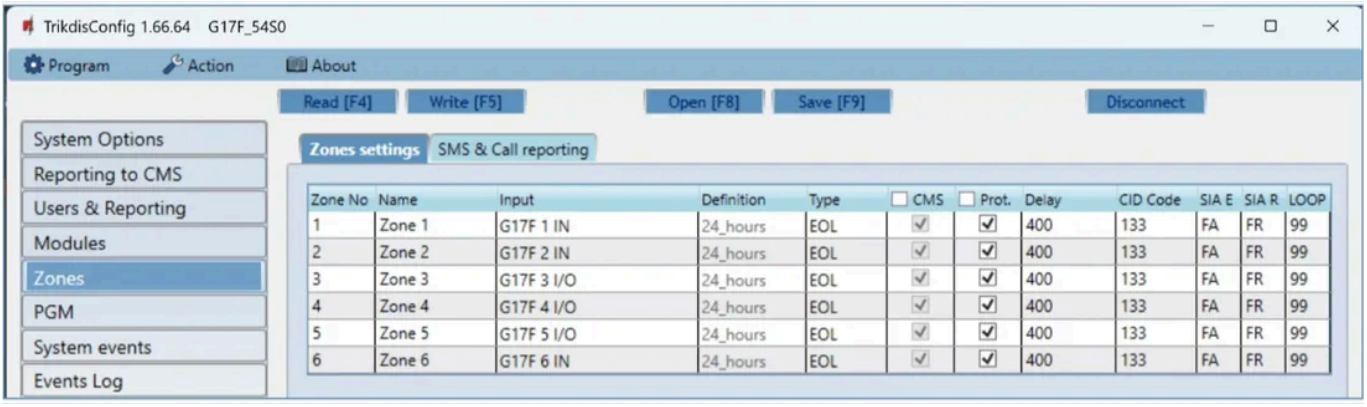


Figura 47. TrikdisConfig – **Zones**, scheda **Zones settings**: nell'immagine sei zone sui sei ingressi del G17F (**1 IN**, **2 IN**, **3 I/O**, **4 I/O**, **5 I/O**, **6 IN**), ciascuna con definizione **24_hours**, tipo **EOL**, caselle **CMS** e **Prot.** spuntate, ritardo di 400 ms e codice CID 133.

- **Zone No** – il numero d'ordine della zona nell'elenco.
- **Name** – il nome della zona; negli SMS compare questo nome.
- **Input** – quale ingresso (IN) del G17F o del modulo di espansione appartiene alla zona.
- **Definition** – ogni zona ha la definizione **24 hours** (24 ore): se la zona viene violata, il messaggio di evento parte immediatamente.
- **Type** – il tipo di circuito collegato all'ingresso: **NC** – contatto normalmente chiuso; **NO** – contatto normalmente aperto; **EOL** – circuito terminato con resistenza di fine linea (4,7 kΩ o 10 kΩ) (punto 3.7).
- **CMS** – se spuntato, gli eventi della zona vanno alla centrale di vigilanza.
- **Prot.** – se spuntato, sugli eventi della zona parte una notifica all'app Protegus 2.
- **Delay** – il tempo di reazione dell'ingresso (IN) in millisecondi.
- **CID Code** – il codice Contact ID dell'evento.
- **SIA E** – il codice evento SIA.
- **SIA R** – il codice di ripristino SIA.
- **LOOP** – il numero del loop; compare nel messaggio SMS.

Scheda SMS & Call reporting

Questa scheda compare solo se nella pagina **Users & Reporting** hai inserito almeno un numero di telefono di un utente.

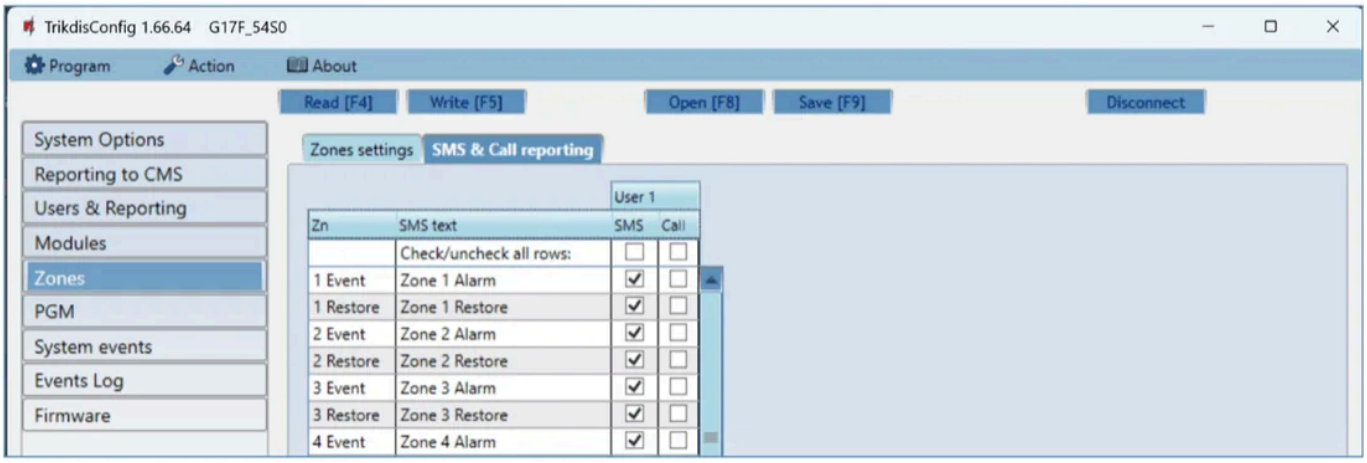


Figura 48. TrikdisConfig – **Zones**, scheda **SMS & Call reporting**: per ogni zona una riga **Event** e una riga **Restore** (per esempio Zone 1 Alarm, Zone 1 Restore); nella colonna **User 1** le caselle **SMS** e **Call**.

- **Zn** – il numero della zona con la parola che indica l'evento: **Event** (evento) o **Restore** (ripristino).
- **SMS text** – la descrizione dell'evento di zona; finisce nell'SMS di evento inviato agli utenti.

- **User SMS/Call** – per ogni evento di zona puoi scegliere se l'utente deve ricevere un SMS e/o una chiamata.

5.7 Pagina „PGM”

Le impostazioni delle uscite PGM in due schede: **Outputs** e **SMS & Call reporting**.

Scheda Outputs

Nella tabella imposti un'uscita PGM per riga.

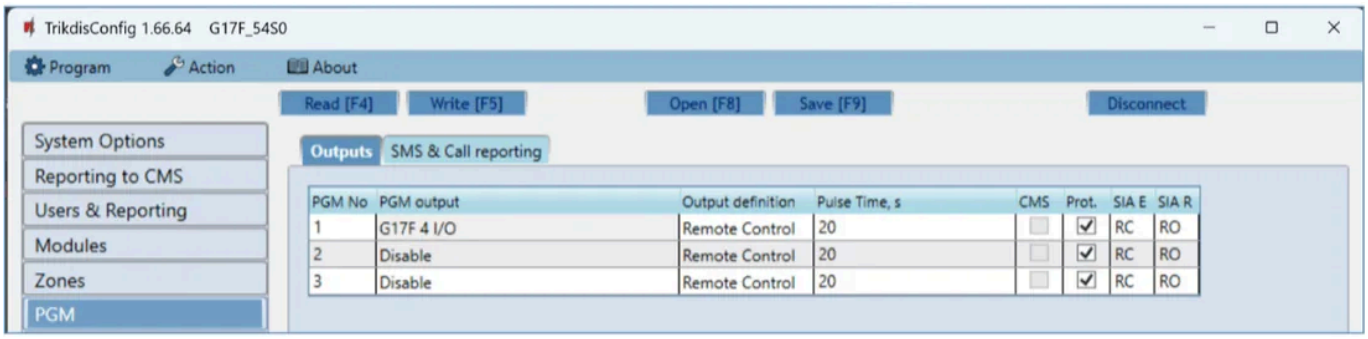


Figura 49. TrikdisConfig – **PGM**, scheda **Outputs**: nell'immagine la PGM 1 sul morsetto **4 I/O** del G17F, le PGM 2 e 3 disattivate (**Disable**); in tutte e tre le righe la definizione di uscita **Remote Control**, durata dell'impulso di 20 s e casella **Prot.** spuntata.

- **PGM No** – il numero d'ordine dell'uscita PGM nell'elenco.
- **PGM output** – l'uscita (OUT) assegnata alla PGM: del G17F o di un dispositivo esterno.
- **Output definition** – il modo di funzionamento dell'uscita (OUT).
- **Pulse time, s** – la durata dell'attivazione dell'uscita (OUT), 0–9999 secondi.
- **CMS** – se spuntato, gli eventi scelti vanno alla centrale di vigilanza.
- **Prot.** – se spuntato, sugli eventi dell'uscita parte una notifica all'app Protegus 2.
- **SIA E** – il codice evento SIA.
- **SIA R** – il codice di ripristino SIA.

Scheda SMS & Call reporting

Questa scheda compare solo se nella pagina **Users & Reporting** hai inserito almeno un numero di telefono di un utente.

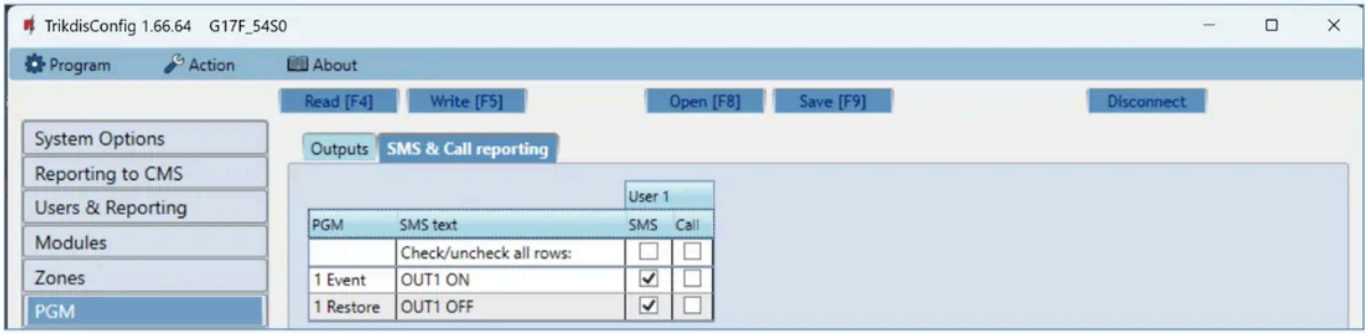


Figura 50. TrikdisConfig – **PGM**, scheda **SMS & Call reporting**: nella riga **Event** della PGM 1 il testo SMS **OUT1 ON**, nella riga **Restore** il testo SMS **OUT1 OFF**; nella colonna **User 1** la casella **SMS** è spuntata.

- **PGM** – il numero dell'uscita (OUT) e il tipo di evento: **Event** – attivazione dell'uscita; **Restore** – disattivazione dell'uscita.
- **SMS text** – il nome dell'evento di attivazione o disattivazione dell'uscita; finisce nell'SMS di evento.

- **User SMS/Call** – puoi scegliere quali utenti devono ricevere un SMS e/o una chiamata all'attivazione e alla disattivazione dell'uscita (OUT).

5.8 Pagina „System events”

Le impostazioni degli eventi propri (di sistema) del comunicatore in due schede: **Events** e **SMS & Call reporting**.

Scheda Events

Nella tabella imposti un evento di sistema per riga.

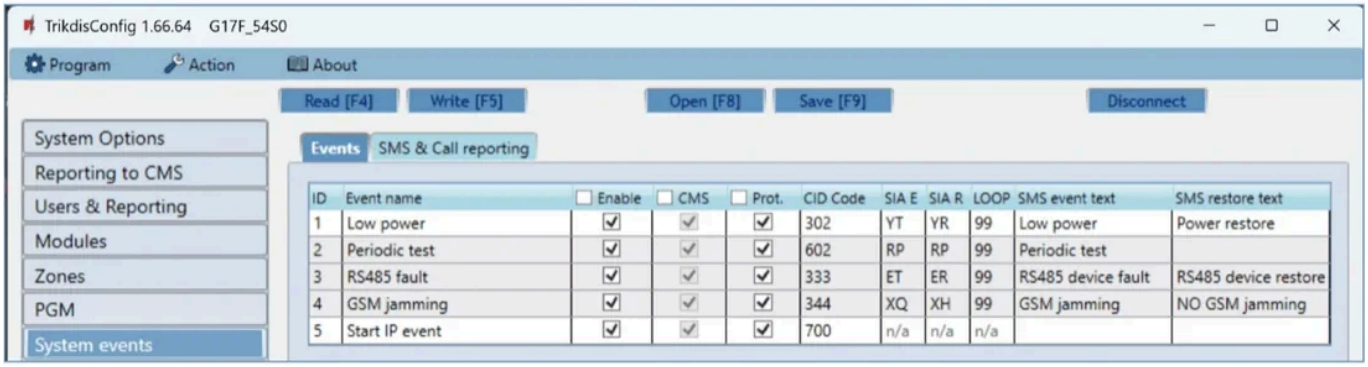


Figura 51. TrikdisConfig – **System events**, scheda **Events**: bassa tensione di alimentazione (**Low power**, CID 302), test periodico (**Periodic test**, 602), guasto RS485 (**RS485 fault**, 333), disturbo della rete mobile (**GSM jamming**, 344) e **Start IP event** (700).

- **ID** – il numero d'ordine dell'evento nell'elenco.
- **Event name** – il nome dell'evento.
- **Enable** – attivazione del monitoraggio dell'evento.
- **CMS** – gli eventi scelti vanno alla centrale di vigilanza.
- **Prot.** – sugli eventi scelti parte una notifica all'app Protegus 2.
- **CID Code** – il codice Contact ID dell'evento.
- **SIA E** – il codice evento SIA.
- **SIA R** – il codice di ripristino SIA.
- **LOOP** – il numero del loop; compare nel messaggio SMS.
- **SMS event text** – il testo SMS dell'evento.
- **SMS restore text** – il testo SMS del ripristino.

Scheda SMS & Call reporting

Questa scheda compare solo se nella pagina **Users & Reporting** hai inserito almeno un numero di telefono di un utente.

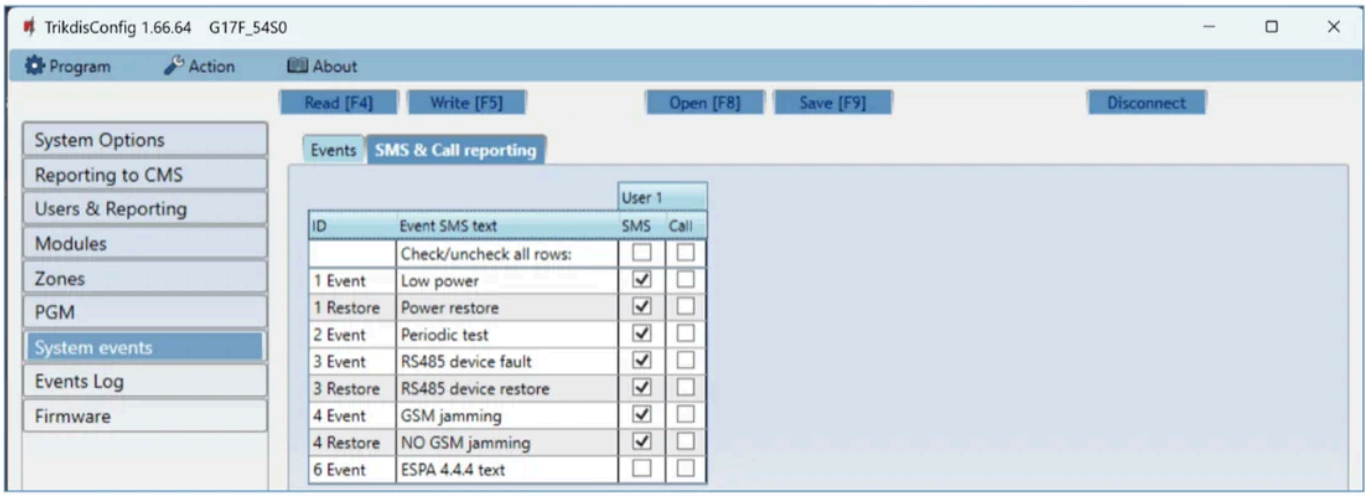


Figura 52. TrikdisConfig – **System events**, scheda **SMS & Call reporting**: le righe **Event** e **Restore** degli eventi di sistema (per esempio Low power, Power restore, Periodic test, GSM jamming); nella colonna **User 1** le caselle **SMS** e **Call**.

- **ID** – il numero d'ordine dell'evento e la parola che lo indica (**Event**, **Restore**).
- **Event SMS text** – il testo dell'evento che finisce nel messaggio SMS.
- **User SMS/Call** – per ogni evento puoi scegliere se l'utente deve ricevere un SMS e/o una chiamata.

5.9 Pagina „Events Log”

Qui puoi leggere e cancellare il registro eventi del dispositivo.

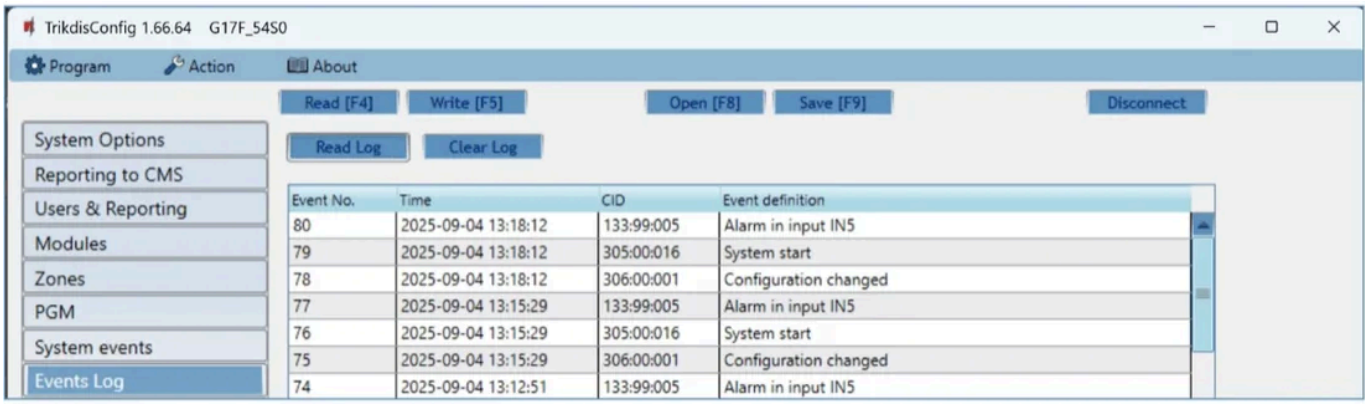


Figura 53. TrikdisConfig – **Events Log**: i pulsanti **Read Log** e **Clear Log**; nella tabella il numero d'ordine, l'ora, il codice CID e la descrizione dell'evento – nell'immagine per esempio allarme sull'ingresso IN5 (**Alarm in input IN5**), avvio del sistema (**System start**) e modifica della configurazione (**Configuration changed**).

- **Read Log** – il pulsante legge il registro eventi dalla memoria del dispositivo.
- **Clear Log** – il pulsante cancella le voci del registro dalla memoria del dispositivo.
- Nella tabella si vedono il numero d'ordine (**Event No.**), l'ora (**Time**), il codice **CID** e la descrizione (**Event definition**) dell'evento. Il registro mostra fino a 1000 eventi memorizzati nel G17F.

5.10 Ripristino delle impostazioni di fabbrica

Per ripristinare le impostazioni di fabbrica del G17F fai clic sul pulsante **Restore** di TrikdisConfig (nella parte in basso a sinistra della finestra di programmazione, nella riga **Default settings**).



Figura 54. TrikdisConfig – il pulsante **Restore** della riga **Default settings**; sotto il campo **IMEI/Unique ID** e la barra di stato.

Se le impostazioni attuali potranno servirti anche in seguito, prima del ripristino salvale in un file con il pulsante **Save [F9]** (punto 5.1).

6. Programmazione a distanza

Le impostazioni del G17F le puoi leggere e modificare anche a distanza tramite il cloud Protegus con TrikdisConfig – non devi recarti sul posto.

Condizioni per la programmazione a distanza

La configurazione a distanza funziona solo se nel G17F:

1. c'è una scheda SIM attivata e il codice PIN è stato inserito o disattivato;
2. il servizio Protegus è attivo (**Users & Reporting** → **Enable cloud service**, punto 5.4);
3. l'alimentazione è accesa (il LED **POWER** lampeggia in verde);
4. è connesso alla rete (il LED **NETWORK** è acceso in verde e lampeggia in giallo).

Se il LED **NETWORK** o **DATA** è acceso fisso in giallo, il dispositivo non riesce a connettersi alla rete mobile e/o a Protegus 2.

1. Avvia TrikdisConfig sul computer.
2. Nella sezione **Remote access**, nel campo **Unique ID**, inserisci l'identificativo univoco del G17F (**Unique ID**). Questo numero lo trovi sul retro del dispositivo e sulla confezione.

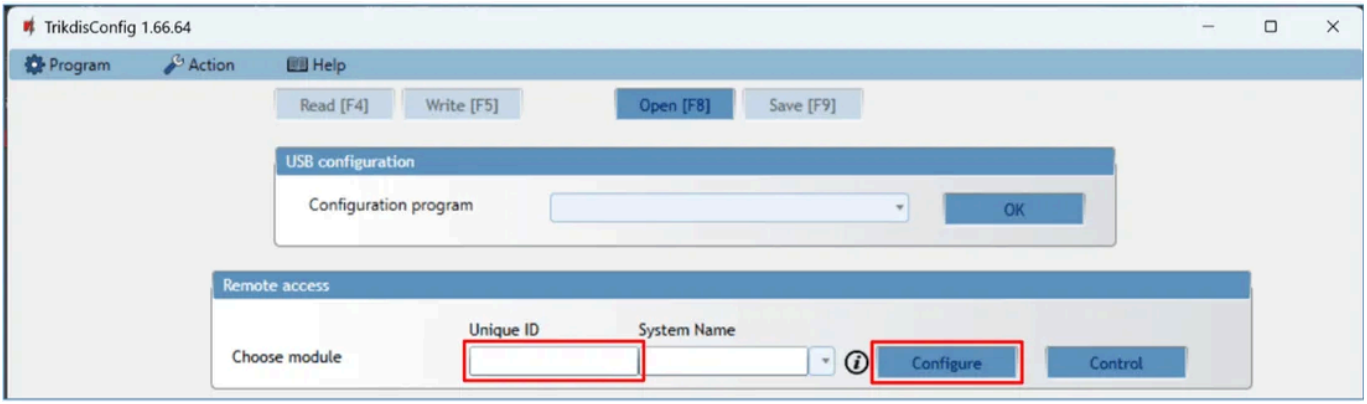


Figura 55. TrikdisConfig – la sezione **Remote access** della finestra iniziale: il campo **Unique ID**, accanto il campo **System Name**, e il pulsante **Configure**.

3. (Facoltativo) Nel campo **System Name** scrivi un nome per il dispositivo (per esempio il nome dell'impianto).
4. Fai clic sul pulsante **Configure**.
5. Nella finestra che si apre fai clic sul pulsante **Read [F4]**. Se il programma lo chiede, inserisci il codice amministratore o installatore.

6. Al termine delle impostazioni fai clic sul pulsante **Write [F5]**. Quando hai finito con TrikdisConfig, fai clic sul pulsante **Disconnect**.

7. Verifica del funzionamento

Al termine della configurazione e dell'installazione prova tutto il sistema:

1. Per verificare un ingresso, attivalo (violalo). Controlla che l'evento sia arrivato alla centrale di vigilanza e/o all'app Protegus 2.
2. Per verificare le uscite, attivale a distanza e controlla il loro funzionamento. Assicurati che gli eventi siano arrivati alla centrale di vigilanza e/o all'app Protegus 2.
3. Esegui una prova di allarme incendio e verifica che la centrale di vigilanza riceva correttamente gli 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.

I dati del comunicatore e lo stato degli ingressi e delle uscite li puoi richiedere anche via SMS: `INFO 123456`, `ASKI 123456`, `ASKO 123456` (al posto di `123456` scrivi la tua password SMS; punto 4.2).

8. Aggiornamento del firmware

Quando colleghi il G17F a TrikdisConfig e c'è un firmware più recente, il programma propone da solo l'aggiornamento – per questo il computer deve essere connesso a Internet. L'antivirus, il firewall o impostazioni di accesso a Internet restrittive possono bloccare l'aggiornamento automatico.

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.

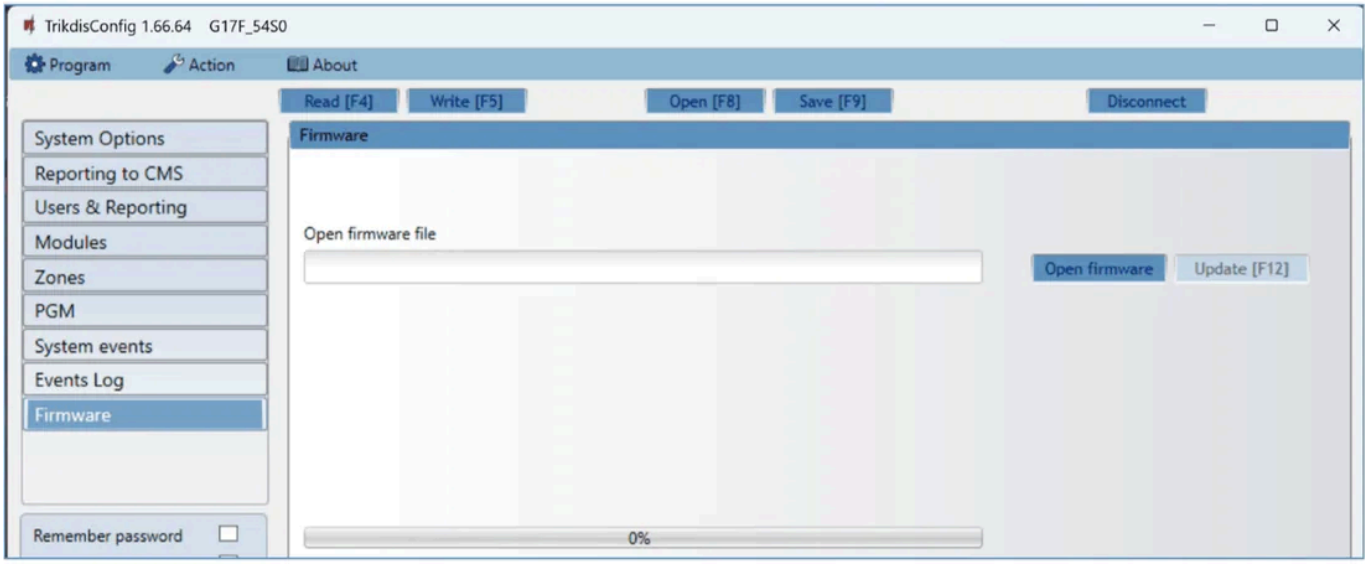


Figura 56. TrikdisConfig – G17F, pagina **Firmware**: il campo **Open firmware file**, il pulsante **Open firmware**, il pulsante **Update [F12]** e l'indicatore di avanzamento.

Per usare i moduli W485 ed E485 serve almeno il firmware **1.08** del G17F (punti 3.11 e 3.12); la versione attuale la vedi nel campo **FW** della barra di stato (punto 5.1).

9. Risoluzione dei problemi e domande frequenti

Se il comunicatore non fa quello che ti aspetti, guarda prima i LED (punto 1.6), poi i punti qui sotto.

Il LED TROUBLE lampeggia – che cosa significa il numero di lampeggi?

Il numero di lampeggi indica la causa del guasto: **1** – nessuna scheda SIM; **2** – il codice PIN della scheda SIM è errato (**System Options** → **SIM card PIN**, punto 5.2); **3** – non riesce a connettersi alla rete mobile; **4** – non riesce a connettersi al ricevitore IP sul canale principale (**Reporting to CMS**, punto 5.3); **5** – non riesce a connettersi al ricevitore IP sul canale di riserva; **6** – l'orologio interno non è impostato (**Time set**, punto 5.2; via SMS: `TIME`, punto 4.2); **7** – la tensione di alimentazione non è adeguata (9–32 V DC; **Low power voltage**, punto 5.2); **9** – errore nella comunicazione con il modulo RS485 (collegamenti: punti 3.3–3.12; **Modules**, punto 5.5).

Quanti lampeggi gialli servono sul LED NETWORK?

Il numero di lampeggi gialli indica il livello del segnale: su rete 2G (GPRS) bastano già 5 lampeggi, su rete 4G 3. Se conti meno di 3 lampeggi gialli, il segnale non è sufficiente: scegli un altro punto per il comunicatore oppure usa un'antenna più sensibile da posizionare all'esterno (punto 1.7). Se i LED non si accendono affatto, controlla l'alimentazione e i collegamenti (punto 3.13).

Protegus 2 non trova il comunicatore

- Controlla le condizioni per l'aggiunta: scheda SIM attivata, codice PIN inserito o disattivato, servizio Protegus attivo (**Users & Reporting** → **Enable cloud service**, punto 5.4), LED **POWER** lampeggiante in verde, LED **NETWORK** acceso in verde e lampeggiante in giallo (punto 4.1).
- Se il LED **NETWORK** o **DATA** è acceso fisso in giallo, il dispositivo non riesce a connettersi alla rete mobile e/o a Protegus 2 (capitolo 6). Controlla l'impostazione dell'**APN** (punto 5.2).
- Se il **Cloud Access Code** non è quello di fabbrica `123456`, durante l'aggiunta inserisci il codice corretto (punto 2.1).

Non riesco a controllare le uscite con chiamata o SMS

- Con SMS e chiamata si può controllare solo dai numeri di telefono presenti nell'elenco degli utenti (punto 4.2). Se non è ancora stato aggiunto nessun utente, chi chiama per primo diventa l'amministratore (punto 4.3).
- L'utente deve avere il diritto di controllare le uscite (casella **PGM**, punto 5.4) e all'uscita deve essere assegnata la definizione **Remote Control** (**Output definition**, punto 5.7).
- Con il modulo W485 o E485 controlla la casella **Use dial and SMS when working over internet module** (punto 5.5): se non è spuntata e c'è la connessione Internet, chiamate e SMS non vengono usati.

Non ricevo risposta ai miei comandi SMS

Per l'SMS di risposta, per l'utente deve essere spuntata la casella **ACK** (**Users & Reporting**, punto 5.4). Il testo delle risposte lo puoi modificare nella scheda **SMS answer texts**.

Dove finiscono gli SMS dell'operatore (credito, pubblicità)?

Se per l'utente la casella **FWD** è spuntata, il G17F gli inoltra gli SMS che arrivano da numeri esterni al sistema (per esempio l'avviso sul credito della scheda SIM) (punto 5.4).

INIM Smartline: a cosa devo fare attenzione?

La centrale va impostata in modalità **slave** nel programma SmartLeague. Se alla centrale sono collegati dei ripetitori (repeater), il G17F non può essere collegato tramite bus RS485; se invece il G17F è collegato al bus RS485 della centrale, i moduli di espansione iO del comunicatore non sono supportati (punto 3.5).

NSC Solution: la centrale non vede il comunicatore

Dopo aver configurato il G17F, sulla centrale bisogna cercare (scansionare) i moduli collegati al bus RS485 (**SCAN RS485**, punto 3.4). L'**NSC slave address** non può coincidere con l'indirizzo degli altri moduli collegati alla centrale.

Quale intervallo devo impostare per il PING?

Consigliamo un intervallo di PING al massimo di 5 minuti. Di fabbrica il ricevitore segnala l'interruzione della connessione al software della centrale di vigilanza dopo tre volte l'intervallo di PING; la connessione attiva serve anche per la configurazione e il controllo a distanza (punto 5.3).

Il G17F si può usare senza scheda SIM?

Sì, con il modulo Wi-Fi W485 o con il modulo Ethernet E485 (con firmware del G17F almeno 1.08): in questo caso i messaggi passano tramite il modulo (punti 3.11 e 3.12). Se il Wi-Fi o l'Internet cablato cade, il G17F invierebbe tramite la rete mobile – per questa riserva serve la scheda SIM. Le impostazioni del modulo, per esempio la segnalazione dell'assenza della scheda SIM e il divieto della connessione dati mobile: punto 5.5.

10. 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.

- Il comunicatore può essere installato e mantenuto solo da personale qualificato.
- Prima dell'installazione leggi attentamente questo manuale, per evitare errori che possono portare a un funzionamento scorretto o perfino al danneggiamento dell'apparecchiatura.
- **Prima di ogni collegamento elettrico scollega l'alimentazione.**
- Modifiche, aggiornamenti o riparazioni non autorizzati dal produttore comportano la perdita della garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare l'apparecchio e i suoi componenti nei rifiuti domestici – consegna il dispositivo dismesso come rifiuto elettronico.

Vedi anche

- Modulo di espansione di ingressi e uscite iO8 – manuale di installazione – il modulo di espansione iO-8 per il G17F.
- Impostazione dell'APN – elenco degli operatori mobili europei – se la connessione dati mobile non si stabilisce.
- App Protegus per Android / iPhone e web – sull'app.
- Account aziendale Protegus 2 (Business Account) – gestione di più sistemi come installatore.
- Versione in inglese: docs.trikdis.com – LTE communicator for fire alarm control panels G17F.

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

Prodotti correlati

Trikdis G17F 4G GSM / IP comunicatore antincendio

Trikdis G17F 2G GSM / IP comunicatore antincendio

Trikdis iO8 modulo di espansione cablato **Trikdis RF-LORA modulo di espansione wireless**

Trikdis IO-LORA modulo di espansione wireless

Trikdis IO8-LORA modulo di espansione wireless **Trikdis PB-LORA pulsante panico wireless**

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

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

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

Trikdis IPcom v5 Windows ricevitore software **Trikdis IPcom v5 Linux ricevitore software**

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-g17f