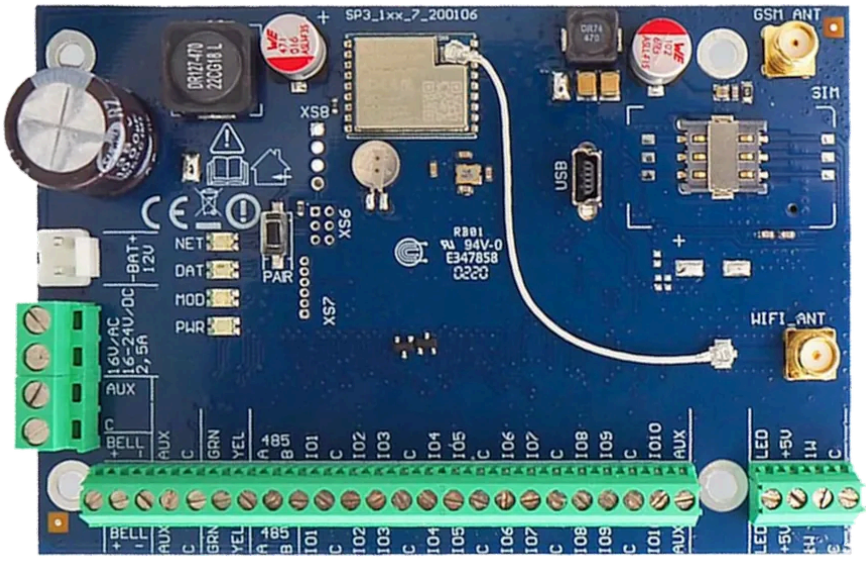
Centrale d'allarme “FLEXi” SP3 – manuale di installazione e programmazione

Manuale di installazione e programmazione della centrale d'allarme Trikdis “FLEXi” SP3: alimentazione, collegamento di zone e uscite PGM, tastiere ed espansioni, programmazione in TrikdisConfig, trasmissione alla centrale di vigilanza, app Protegus 2.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-flexi-sp3

Indice

1. Panoramica

1.1 A cosa serve, come funziona
1.2 Versioni e codici tipo
1.3 Dati tecnici
1.4 Moduli e tastiere compatibili
1.5 Parti della scheda e morsettiere
1.6 Indicazioni LED
1.7 Versioni firmware

2. Alimentazione e messa in servizio rapida

2.1 Alimentatore di rete
2.2 Batteria
2.3 Contenuto della confezione, contenitori: K01 e K02
2.4 I passaggi della messa in servizio in breve

3. Installazione e collegamenti

3.1 Ordine consigliato dell'installazione
3.1.1 Montaggio della scheda nel contenitore
3.1.2 Ordine di collegamento dei dispositivi
3.2 Collegamento dei rivelatori
3.2.1 Schemi di collegamento
3.3 Collegamento dei rivelatori di fumo
3.4 Collegamento della sirena
3.5 Collegamento di tastiere e lettori RFID
3.6 Collegamento dei lettori di chiavi TM17 e CZ-Dallas
3.7 Collegamento dei sensori di temperatura
3.8 Collegamento di relè e spia LED
3.9 Accensione della centrale

4. Collegamento di espansioni e moduli radio

4.1 Modulo Ethernet E485
4.2 Ricevitore radio RF-SH (Crow)
4.3 Ricevitore radio RTX3 (Paradox)
4.4 Ricevitore radio RF-HW (Honeywell)
4.5 Ricevitore radio RF-S8
4.6 Ricevitore radio RF-LORA
4.7 Espansioni LORA
4.8 Espansioni della serie iO
4.9 Trasmettitore radio T16
4.10 Modulo Sigfox SF485
4.11 Misura della tensione continua

5. Protegus 2 e controllo a distanza

5.1 Collegamento all'account Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Inserimento e disinserimento nell'app
5.3 Configurazione e controllo via SMS
5.4 Controllo con chiamata telefonica

6. TrikdisConfig – le impostazioni in dettaglio

- 6.1 La barra di stato
- 6.2 System Options
  - 6.2.1 Scheda System general
  - 6.2.2 Scheda Partitions
  - 6.2.3 Scheda Scheduler
  - 6.2.4 Scheda Holidays
  - 6.2.5 Scheda System troubles
  - 6.2.6 Scheda Access
- 6.3 Reporting to CMS
  - 6.3.1 Scheda Reporting
  - 6.3.2 Scheda Settings
- 6.4 Users & Reporting
  - 6.4.1 Tessere e portachiavi RFID
  - 6.4.2 Chiavi iButton
  - 6.4.3 Scheda Protegus
  - 6.4.4 Scheda SMS answer texts
- 6.5 Modules
- 6.6 Wireless sensors
  - 6.6.1 Registrazione dell'RF-LORA
  - 6.6.2 Accoppiamento dei rivelatori a distanza
  - 6.6.3 Accoppiamento con il pulsante LEARN
  - 6.6.4 RF-SH e dispositivi Crow
- 6.7 Zones
- 6.8 PGM
- 6.9 Sensors
- 6.10 System events
- 6.11 Events log
- 6.12 Ripristino delle impostazioni di fabbrica

7. Programmazione a distanza

8. Verifica del funzionamento del sistema

9. Aggiornamento del firmware

10. Ricerca guasti e domande frequenti

11. Garanzia e norme di sicurezza

- 11.1 Garanzia e limitazione di responsabilità
- 11.2 Norme di sicurezza

Vedi anche

1. Panoramica

La “FLEXi” SP3 è la **centrale d'allarme antintrusione e antincendio** di Trikdis con il comunicatore già integrato: tramite connessione Wi-Fi e/o Ethernet, oppure con un modem 2G / 4G (sulla rete mobile, se è inserita una scheda SIM), trasmette direttamente ogni evento generato alla centrale di vigilanza e all'app Protegus 2 (cloud Protegus). Ha dieci morsetti IO a funzione selezionabile (zona o uscita PGM), gestisce otto aree e, con tastiere, espansioni iO e ricevitori radio, si espande – a seconda della versione firmware – fino a 32 o 64 zone. Le impostazioni si effettuano con il software TrikdisConfig tramite cavo USB o a distanza; l'utente controlla il sistema dalla tastiera cablata o senza fili, con chiave iButton, con tessera RFID, dall'app Protegus 2 e, nelle versioni con modem, anche via SMS e chiamata telefonica – e può cambiare anche a distanza la modalità di protezione delle diverse zone dell'edificio (aree). La centrale è certificata EN 50131 Grado 3.

1.1 A cosa serve, come funziona

A cosa serve soprattutto

- **Impianti d'allarme per edifici piccoli e medi**, preferibilmente collegati a una centrale di vigilanza: accetta sia rivelatori cablati sia senza fili, inoltra gli eventi sia alla centrale di vigilanza sia all'utente, ed entrambi possono controllarla a distanza.
- **Sostituzione di una centrale d'allarme esistente**: il valore delle resistenze di fine linea presenti nei rivelatori si imposta nella centrale uguale a quello della centrale sostituita, quindi non è necessario rimontare i rivelatori uno per uno.
- **Automazione** oltre alla protezione: cancello del garage e del giardino, irrigazione, illuminazione, riscaldamento, ventilazione, raffreddamento e qualsiasi altra cosa che si possa accendere e spegnere – dalle uscite PGM, con logica di funzionamento, programmazione oraria o in modalità termostato.

Come funziona

- **Trasmette alla centrale di vigilanza** tramite la connessione Wi-Fi, Ethernet o di rete mobile integrata; con un modulo aggiuntivo anche su canale Ethernet (E485), radio VHF/UHF (T16) o Sigfox (SF485), con priorità selezionabile. La può ricevere qualsiasi centrale di vigilanza dotata di un ricevitore IP software o hardware Trikdis, oppure di un ricevitore IP che supporti il protocollo SIA DC-09. Può trasmettere in parallelo ai ricevitori di due diversi istituti di vigilanza, ciascuno con ricevitore principale e di riserva.
- **Avvisa l'utente** nell'app Protegus 2 con notifica push e suono dedicato; le versioni con modem anche via SMS fino a 8 numeri di telefono. Con una chiamata con messaggio vocale preregistrato (fino a 8 numeri di telefono) può avvisare solo la vecchia versione SP3_12xx, con firmware fino alla 1.13. Si può impostare che l'evento vada prima alla centrale di vigilanza e solo dopo all'utente.
- **Controllabile a distanza**: inserimento, disinserimento, modalità perimetrale (Stay) e notturna (Sleep), comando dei dispositivi collegati alle uscite PGM e monitoraggio della temperatura dall'app; nelle versioni con modem anche via SMS e chiamata telefonica.
- **Ingressi e uscite**: 10 morsetti IO, ciascuno utilizzabile come ingresso (tipi NC, NO, EOL, ATZ, con valore di resistenza impostabile nei circuiti EOL e ATZ) o come uscita open collector; il numero di ingressi si può portare a 64 con tastiere e con le espansioni iO, iO-8, iO8-LORA, iO-LORA e iO-WL, quello delle uscite a 16 con le stesse espansioni; due uscite dedicate (BELL per la sirena, LED per la spia luminosa); sette modalità di funzionamento delle uscite e, per ogni uscita, si può assegnare una logica di funzionamento, una programmazione oraria preimpostata o ad esempio la modalità termostato; sul bus

1-Wire fino a 8 sensori di temperatura, 1 sensore di temperatura e umidità o un lettore iButton; sul bus tastiere GRN / YEL 8 tastiere dello stesso tipo e il ricevitore radio Paradox RTX3 (4.3); sul bus RS485 espansioni iO, ricevitori radio (RF-LORA, RF-SH, RF-S8, RF-HW), moduli E485, T16 e SF485.

- **Gestione**: 40 codici utente (1 codice master e 39 codici normali, a 4 o 6 cifre), utilizzabili anche come codice sotto coercizione – il codice disinserisce l'allarme, ma la centrale di vigilanza riceve una segnalazione separata che il disinserimento è avvenuto sotto costrizione. Tastiere Trikdis, Paradox e Crow, lettori iButton CZ-Dallas e TM17 (fuori produzione), lettori RFID Wiegand 26/34.
- **Installazione e configurazione**: kit in contenitore metallico con alimentatore integrato, in più dimensioni, con trasformatore riduttore o alimentatore switching; le impostazioni di fabbrica si possono usare senza modifiche nella maggior parte degli edifici piccoli e medi (sette su dieci); la centrale precedente si può sostituire senza cambiare le resistenze dei rivelatori; le impostazioni si possono salvare in un file; due livelli di accesso (installatore e amministratore); a distanza TrikdisConfig non solo configura, ma mostra anche il funzionamento della centrale.

1.2 Versioni e codici tipo

La centrale è un'unica scheda a circuito stampato, disponibile in sei versioni a seconda dei moduli di comunicazione integrati. La versione è indicata dalla prima cifra (**y**) del codice **SP3_yxxz** nel nome del file firmware; la stessa cifra si vede nella barra di stato di TrikdisConfig e, durante l'aggiornamento, si può caricare solo un firmware con la stessa cifra (paragrafo 1.7).

Versione	Connessione	Codice (y)	Slot SIM
SP3 WiFi	Wi-Fi	2	–
SP3 Ethernet	rete cablata (Ethernet, RJ45)	3	–
SP3 WiFi + 2G	Wi-Fi + modem 2G (GSM/GPRS)	5	1 × nano-SIM
SP3 WiFi + 4G	Wi-Fi + modem 4G (LTE)	1	1 × nano-SIM
SP3 Ethernet + 4G	Ethernet + modem 4G (LTE)	6	1 × nano-SIM
SP3 Ethernet + 2 SIM 4G	Ethernet + modem 4G (LTE), con due slot SIM	verificalo nella barra di stato del dispositivo	2 × nano-SIM

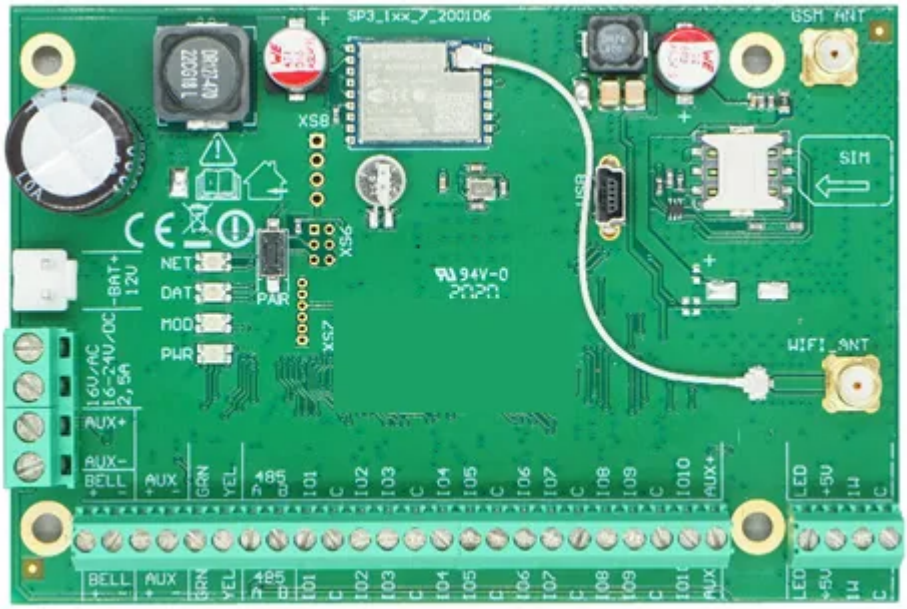


Figura 1. La scheda della versione "FLEXi" SP3 WiFi + 2G: il connettore SMA dell'antenna Wi-Fi e di quella di rete mobile, lo slot nano-SIM e le morsettiere.

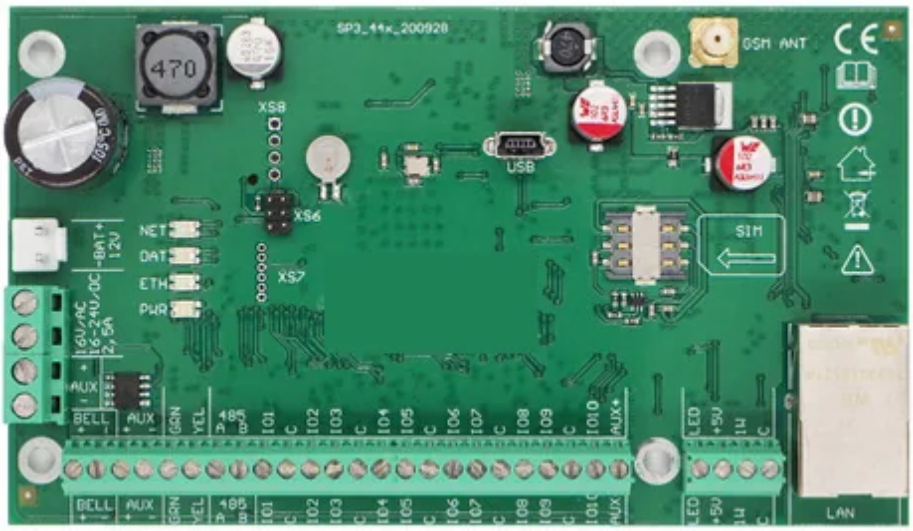


Figura 2. La versione "FLEXi" SP3 Ethernet + 4G: la presa Ethernet RJ45 al posto del connettore dell'antenna Wi-Fi.

Uno o due canali di comunicazione. Le versioni WiFi ed Ethernet comunicano su un solo canale, le versioni con modem su due (dual path): oltre alla connessione cablata, anche sulla rete mobile.

WiFiun canale
Ethernetun canale
WiFi + 2Gdue canali · 1 SIM
WiFi + 4Gdue canali · 1 SIM
Ethernet + 4Gdue canali · 1 SIM
Ethernet + 2 SIM 4Gdue canali · 2 SIM

- Su Wi-Fi ed Ethernet l'accesso dal telefono è rapido e non ci sono costi di dati mobili.
- Se la connessione Internet cablata si interrompe, o il router si spegne durante un'interruzione di corrente, la centrale con modem passa da sola alla rete mobile.
- Grazie ai due canali che si fanno da riserva a vicenda (dual path), la segnalazione arriva a destinazione anche se una delle due vie viene a mancare.

- Sulle connessioni veloci Wi-Fi, Ethernet e 4G la programmazione a distanza e l'aggiornamento del firmware sono comodi.

Il modem **2G** delle versioni con modem funziona sulle bande 850 / 900 / 1800 / 1900 MHz, il modem **4G (LTE)** sulle bande B1 / B3 / B7 / B8 / B20 / B28 usate in Europa (EMEA); per altre regioni (America Latina, Australia, Nord America) Trikdis produce anche versioni con modem a diversa assegnazione di bande (le bande sono indicate nella tabella del paragrafo 1.3). Il Wi-Fi è a 2,4 GHz, 802.11 b/g/n, con crittografia WPA / WPA2.

1.3 Dati tecnici

Caratteristica	Valore
Tensione di alimentazione [AC / DC]	16 V AC oppure 16–24 V DC, 2,5 A
Assorbimento	massimo 50 mA a riposo; massimo 200 mA per breve tempo, durante la trasmissione
Alimentazione di riserva [BAT]	batteria al piombo da 12 V, 4 Ah o 7 Ah
Corrente di carica della batteria	massimo 500 mA
Alimentazione dispositivi esterni [AUX]	12 V DC, massimo 1 A
Uscita sirena [BELL]	1 A
Uscita LED [LED]	0,1 A
Uscita PGM (morsetto IO come uscita)	open collector, massimo 0,1 A
Modulo Wi-Fi	integrato nelle versioni Wi-Fi; 2,4 GHz, 802.11 b/g/n, WPA / WPA2 / WPA misto
Impostazione di rete	DHCP o manuale
Scheda SIM	nelle versioni con modem 1 nano-SIM (nella versione a 2 SIM: 2)
Bande del modem 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Bande del modem 4G (LTE) – “FLEXi” SP3_14E / SP3_24E, EMEA e Thailandia	B1 / B3 / B7 / B8 / B20 / B28
Bande del modem 4G (LTE) – “FLEXi” SP3_24S, America Latina / Australia / Nuova Zelanda	B1 / B3 / B4 / B5 / B7 / B8 / B28
Bande del modem 4G (LTE) – “FLEXi” SP3_24A, Nord America	B2 / B4 / B12
Destinazioni di invio degli eventi	ricevitore principale e di riserva di 2 istituti di vigilanza; al cloud Protegus, all'app Protegus 2 per iOS / Android; via SMS a 8 numeri di telefono; chiamata a 8 numeri di telefono – se l'utente risponde, la centrale comunica con un messaggio vocale cosa è successo (solo la versione SP3_12xx, con firmware fino alla 1.13)
Canali di invio degli eventi	GPRS o 4G, Wi-Fi, Ethernet (integrato o con modulo E485), SMS; chiamata vocale fino a 8 numeri di telefono (solo la versione SP3_12xx, con firmware fino alla 1.13); radio VHF/UHF (con comunicatore T16); Sigfox (con modulo SF485)
Collegamento con la centrale di vigilanza	TCP/IP o UDP/IP, oppure SMS

Caratteristica	Valore
Codifica degli eventi	Contact ID
Crittografia	TRK AES-128, SIA IP AES-128
Orologio interno	sì
Buffer messaggi	60 eventi
Registro eventi	massimo 1000 eventi; quando è pieno, il più vecchio viene cancellato
Codici utente	40 (a 4 o 6 cifre)
Codice sotto coercizione	scelta tra due modalità di inserimento in fase di programmazione
Morsetti a doppia funzione [IO]	10; funzione IN o OUT in fase di programmazione. Come ingresso: NC, NO, EOL, EOL_T, 3EOL, ATZ, ATZ_T. Come uscita: open collector (OC), massimo 100 mA
Aree	8
Zone	10 (20 con raddoppio zone ATZ); con espansioni fino a 64 (paragrafo 1.7)
Uscite PGM	2 (12 se i morsetti IO sono impostati come uscite; 16 con espansioni)
Tastiere	massimo 8 (i tipi sono elencati nel paragrafo 1.4)
Lettori RFID (Wiegand 26/34)	massimo 2
Lunghezza del bus 1-Wire [1 WIRE]	massimo 30 m
Sensori di temperatura	Maxim / Dallas DS18S20, DS18B20; serie AM2301
Numero di sensori di temperatura sul bus 1-Wire	8 (Dallas) o 1 (AM2301)
Chiavi elettroniche (iButton) [1 WIRE]	Maxim / Dallas DS1990A, massimo 40 chiavi
Lunghezza del bus RS485	massimo 100 m
Dispositivi sul bus RS485	massimo 8
Ambiente di funzionamento	−10 °C … +50 °C, umidità relativa massima 80 % a +20 °C, senza condensa
Dimensioni della scheda	117 × 79 × 25 mm; per le versioni Ethernet + 4G 137 × 79 × 25 mm
Peso	0,1 kg

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 Moduli e tastiere compatibili

L'uscita AUX della centrale fornisce al massimo 1 A ai dispositivi esterni; per dimensionare la batteria di riserva (paragrafo 2.1) si deve sommare l'assorbimento complessivo dei moduli collegati. L'elenco di fabbrica:

Modulo	Assorbimento
Tastiera SK-LED TouchPad (Protegus SK232 LED W)	60–150 mA
Tastiera SK-LCD TouchPad (FLEXi SK232LCD – in negozio: tastiera FLEXi LCD)	25–60 mA

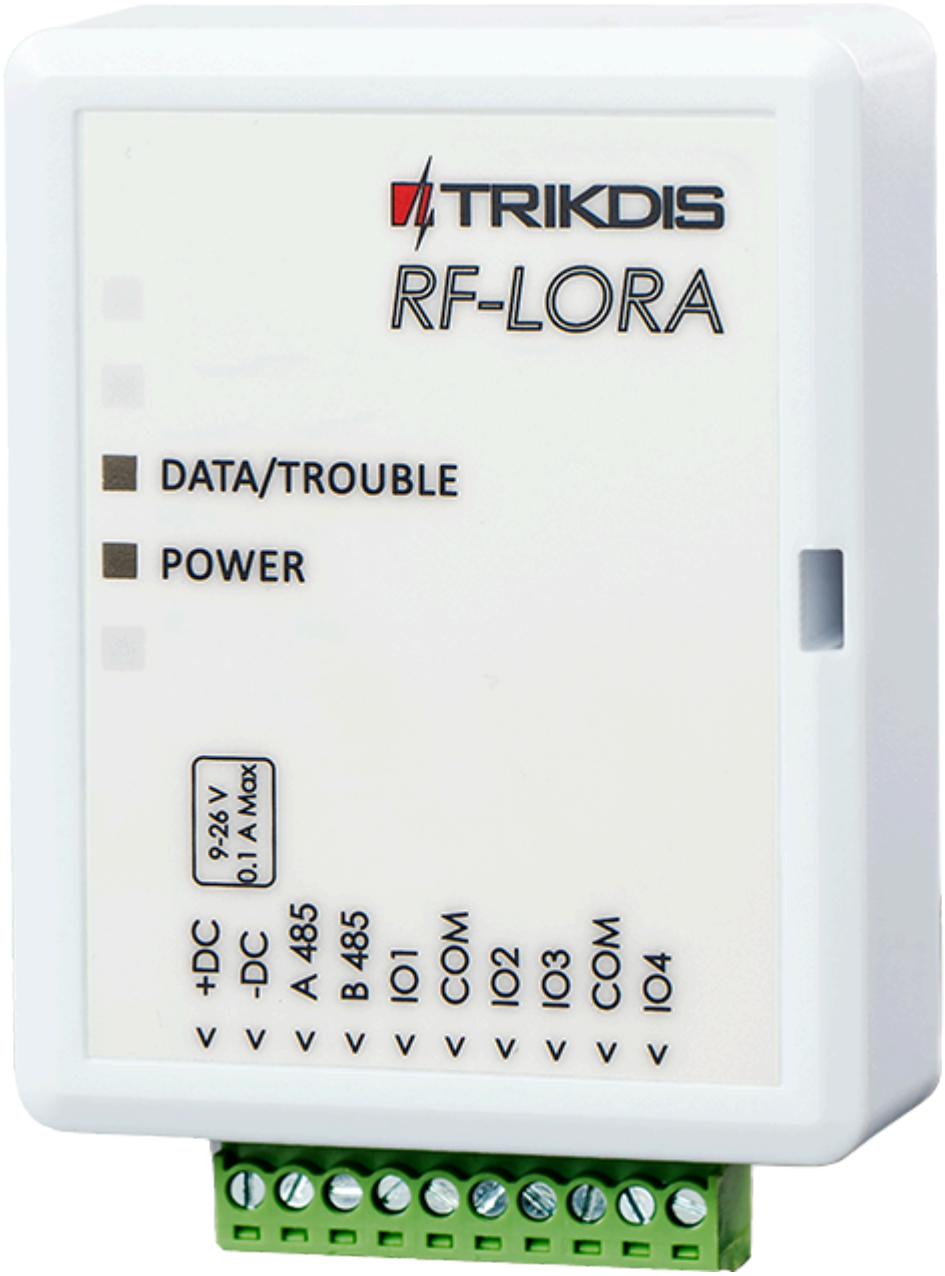
Modulo	Assorbimento
Tastiera SK LCD Button	massimo 70 mA
Tastiera SK LED Button	massimo 70 mA
Tastiera Paradox K636	40–70 mA
Tastiera Paradox K10H(V)	44–72 mA
Tastiera Paradox K32 LED, K32+ LED	49–148 mA
Tastiera Paradox K32LCD+	70–150 mA
Tastiera Paradox K35	30–70 mA
Tastiera Paradox TM50	100–230 mA
Tastiera Paradox TM70	200–330 mA
Tastiera Crow CR16, CR-LCD	40–75 mA
Espansione iO-8	massimo 20 mA
Espansione iO	massimo 50 mA
iO-MOD – ricetrasmettitore radio iO-WL	50–150 mA
Espansione senza fili iO-WL	massimo 200 mA
Ricevitore radio RF-SH (per rivelatori Crow)	massimo 100 mA
Ricetrasmettitore radio Paradox RTX3	massimo 200 mA
Ricetrasmettitore radio RF-HW (per rivelatori Honeywell)	massimo 100 mA
Ricetrasmettitore radio RF-S8 (per rivelatori S8)	massimo 100 mA
Ricetrasmettitore radio RF-LORA (per rivelatori e moduli LORA)	50–150 mA
Espansione iO-LORA, iO8-LORA	massimo 50 mA
Pulsante antipanico PB-LORA	batteria propria, 3 V CR123A
Modulo relè REL-LORA	massimo 45 mA
Modulo Ethernet E485	50–150 mA
Lettore iButton TM17	massimo 50 mA
Lettore iButton CZ-Dallas	massimo 25 mA
Comunicatore radio VHF / UHF T16	100 mA – 1,2 A
Lettore RFID (Wiegand 26/34)	massimo 100 mA

Tastiere. Sul bus GRN / YEL si possono collegare al massimo 8 tastiere dello stesso tipo:

Trikdis PROTEGUS SK232LED, FLEXI LCD, FLEXI LED, SK-LCD Button, SK-LED Button
Paradox K32LCD+, K32+, K32LED, K32+ LED, K35, K10H, K10V, K636, TM50*****, TM70*****
Crow CR16, CR-LCD
A LED-es kezelők csak az első 2 partíció állapotát képesek megjeleníteni, de kezelhetik mind a 8 partíciót.
*Ez a kezelő csak az első 2 partíciót kapcsolhatja ki/be.

Dispositivi senza fili. Il tipo di ricevitore radio dipende dalla versione firmware della centrale (paragrafo 1.7): una centrale lavora con un solo tipo di ricevitore alla volta.

Vezeték nélküli érzékelők és eszközök hozzáadása a FLEXi SP3 riasztórendszerhez





A **TRIKDIS RF-LORA** vagy **Paradox RTX3** vezeték nélküli bővítő modullal a „klasszikus" vezetékes riasztó hibrid vagy teljesen vezeték nélküli módon is működhet. Hasznos, ha nincs lehetőség vezeték kiépítésére és vezeték nélküli érzékelőkre vagy egyéb vezeték nélküli eszközökre van szükség.

A RIKDIS RF-LORA-hoz a Trikdis vezeték nélküli bővítőket, érzékelőket és eszközöket lehet párosítani.

A Paradox RTX3-mal a Paradox vezeték nélküli érzékelőket, eszközöket és billentyűzeteket lehet használni.

1.5 Parti della scheda e morsettiere

Il disegno mostra le parti principali della scheda; la funzione dei morsetti è elencata nella tabella sotto il disegno.

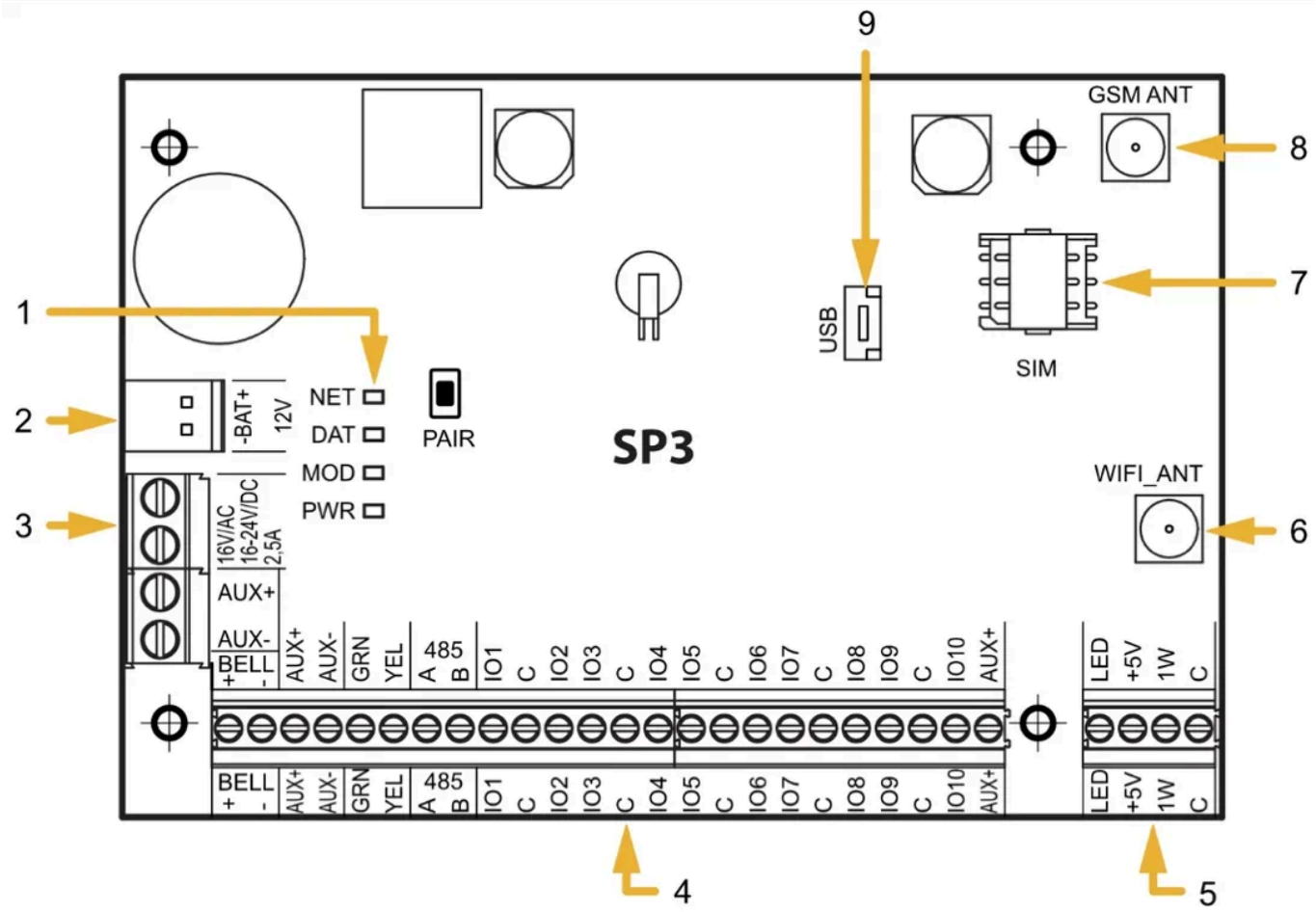


Figura 3. La scheda a circuito stampato della "FLEXi" SP3 (versione Wi-Fi + mobile). Nella versione Ethernet, al posto del 6 c'è una presa Ethernet RJ45.

- 1 LED di connessione e di funzionamento (paragrafo 1.6)
- 2 Morsetto dell'alimentazione di riserva (batteria)
- 3 Morsetto dell'alimentazione principale
- 4 Morsetti dei dispositivi esterni
- 5 Morsetto del bus dati 1-WIRE
- 6 Connettore SMA per l'antenna Wi-Fi
- 7 Slot nano-SIM
- 8 Connettore SMA per l'antenna di rete mobile
- 9 Presa USB Mini-B per la programmazione

Morsetto	Funzione
AC/DC (2 morsetti)	Alimentazione principale: 16 V AC, oppure polo positivo e negativo di 16–24 V DC
BAT+	Polo positivo dell'alimentazione di riserva (batteria da 12 V)
BAT–	Polo negativo dell'alimentazione di riserva
AUX+	+12 V per i dispositivi esterni (massimo 1 A)
AUX–	Negativo comune
BELL+	Uscita sirena: +12 V per la sirena
BELL–	Uscita sirena: polo negativo commutato della sirena (massimo 1 A)
GRN	Bus tastiere (dati)
YEL	Bus tastiere (dati)
A 485	Filo A del bus RS485

Morsetto	Funzione
B 485	Filo B del bus RS485
IO1 – IO9	Ingressi/uscite (impostazione di fabbrica: ingresso)
IO10	Ingresso/uscita (impostazione di fabbrica: uscita PGM, reset rivelatori antincendio)
C	Negativo comune
LED	Uscita PGM (impostazione di fabbrica: indicazione dello stato del sistema)
+5 V	Alimentazione +5 V per i dispositivi 1-Wire
1 WIRE	Bus dati 1-Wire
C	Negativo comune

Le morsettiere sono estraibili, quindi puoi collegare i fili anche senza la scheda, e la scheda si può estrarre per l'assistenza.

1.6 Indicazioni LED

LED	Indicazione	Significato
NET	lampeggia in verde	la scheda SIM si sta registrando sulla rete mobile
	acceso verde	la scheda SIM è registrata sulla rete mobile
	lampeggia in giallo	intensità del segnale di rete mobile con 0–5 lampeggi; 3 sono già sufficienti
DAT	spento	nessun evento non inviato
	acceso verde	invio messaggi in corso
	acceso giallo	eventi non inviati in attesa nel buffer
MOD (versione Wi-Fi)	lampeggia in verde	connessione alla rete Wi-Fi in corso
	acceso verde	connesso alla rete Wi-Fi
ETH (versione Ethernet)	lampeggia in verde	cavo LAN assente o errore DHCP
	acceso verde	connesso alla rete cablata
PWR	lampeggia in verde	nessun guasto di funzionamento
	1 lampeggio rosso	scheda SIM assente
	2 lampeggi rossi	codice PIN della scheda SIM errato
	3 lampeggi rossi	impossibile connettersi alla rete mobile
	4 lampeggi rossi	il ricevitore della centrale di vigilanza non è raggiungibile sul canale 1
	5 lampeggi rossi	il ricevitore della centrale di vigilanza non è raggiungibile sul canale 2
	6 lampeggi rossi	l'orologio interno non è impostato
	7 lampeggi rossi	tensione bassa dell'alimentazione di riserva (batteria)
	8 lampeggi rossi	manca l'alimentazione di rete (AC)

LED	Indicazione	Significato
	9 lampeggi rossi	impossibile connettersi alla rete Wi-Fi

La risoluzione dei guasti è trattata nel capitolo 10.

1.7 Versioni firmware

Il nome del file firmware della centrale ha la forma **SP3_yxxz_NNNN.fw**. La **y** è la versione hardware (paragrafo 1.2) – non si può cambiare durante l'aggiornamento. La **z** indica il tipo di ricevitore radio e quindi il numero di zone gestibili; la scegli tu durante l'aggiornamento, in base al ricevitore radio utilizzato. **NNNN** è il numero di versione del firmware; in genere conviene usare la versione più alta.

Firmware (z)	Ricevitore radio	Rivelatori senza fili	Zone	Tastiere	Moduli
SP3_xxx0	RF-SH (fuori produzione), RF-LORA	Crow	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-SH
SP3_xxx1	Paradox RTX3, RF-LORA	Paradox	32	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA
SP3_xxx2	RF-HW, RF-LORA	Honeywell (345 MHz, non usato in Europa)	64	Trikdis (FLEXi), Paradox, Crow CR Icon / LCD (ST)	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-HW
SP3_xxx4	RF-LORA, RF-S8	MAXIMUM (M4), S8 (Heyi)	64	Trikdis (FLEXi), Paradox	iO, iO-8, iO-WL, iO-MOD, TM17, E485, T16, SF485, RF-LORA, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-S8

Il firmware **SP3_xxx4** serve solo per i rivelatori senza fili: con esso funzionano i dispositivi senza fili MAXIMUM (RF-LORA) e S8 (RF-S8), con 64 zone. Serve almeno la versione 1.21, per i dispositivi S8 la 1.22. Le espansioni LORA collegate tramite RF-LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) funzionano con tutte e quattro le versioni. Per l'espansione Paradox RTX3 serve **SP3_xxx1**, con 32 zone. Carica sempre la versione più recente: a novembre 2026 è la 1.27, con comunicazione migliorata, e non invia più troppi SMS. La codifica e le regole di scelta sono descritte in un articolo a parte: FLEXi SP3 firmware: come scegliere quello giusto?. I passaggi dell'aggiornamento sono nel capitolo 9.

2. Alimentazione e messa in servizio rapida

La centrale e con essa l'intero impianto d'allarme sono alimentati da un alimentatore di rete; la riserva è fornita da una batteria da 12 V. In questo capitolo trovi le regole dell'alimentazione, i kit di fabbrica e la sequenza sintetica dei passaggi di messa in servizio; i dettagli dei collegamenti sono nei capitoli 3 e 4, quelli delle impostazioni nei capitoli 5 e 6.

2.1 Alimentatore di rete

La centrale funziona con una tensione di **16 V AC** o **16–24 V DC**, da una sorgente in grado di erogare almeno **2,5 A**. In corrente alternata è alimentata dalla rete tramite un trasformatore riduttore di Classe II, in corrente continua da un alimentatore switching da 16–24 V (nei contenitori K01 e K02 che vendiamo, un Mean Well APV-35-24). L'alimentazione principale si collega ai due morsetti **AC/DC** della scheda; in corrente continua il polo positivo e quello negativo vanno nell'ordine indicato sui morsetti. In entrambi i casi – con alimentazione in corrente alternata e in corrente continua – è obbligatorio collegare l'alimentazione di riserva, una batteria da 12 V, affinché l'alimentazione resti continua senza interruzioni (paragrafo 2.2).

Interruttore automatico e messa a terra

Nel circuito di alimentazione si deve installare un interruttore automatico bipolare con una distanza di almeno 3 mm tra i contatti aperti; l'interruttore deve trovarsi in un punto noto e accessibile al tecnico che esegue l'assistenza sulla centrale. In caso di contenitore metallico, collega il contenitore a terra. Il contenitore, l'alimentatore, la batteria e il dispositivo di programmazione devono essere conformi alla norma EN 60950.

Calcolo del fabbisogno di corrente. Secondo la EN 50131, l'alimentazione di riserva deve far funzionare il sistema per **12 ore** (Grado 2) o per **60 ore** (Grado 3) dopo la mancanza dell'alimentazione di rete. Per questo somma la corrente a riposo della centrale (50 mA) e l'assorbimento delle tastiere, dei moduli, dei rivelatori e dei segnalatori collegati – i dati dei dispositivi Trikdis e di quelli di terzi supportati sono nella tabella del paragrafo 1.4 – e scegli la capacità della batteria di conseguenza. Il morsetto **AUX+** può fornire in totale al massimo 1 A ai dispositivi esterni; se serve di più, usa un alimentatore separato, con negativo comune.

2.2 Batteria

L'alimentazione di riserva è una **batteria al piombo da 12 V, 4 Ah o 7 Ah** (per il Grado 3 almeno 7 Ah), collegata ai morsetti **BAT+ / BAT–** della scheda con il cavo di collegamento fornito nella confezione. La centrale la carica con al massimo 500 mA.

- Se manca l'alimentazione di rete, la centrale invia l'evento **AC Fault** (guasto rete) e passa alla batteria.
- A 11,5 V viene generato l'evento **Low Battery** (batteria scarica); sotto 9,5 V la centrale **scollega** la batteria per proteggerla dalla scarica profonda.
- Al ritorno dell'alimentazione di rete invia l'evento **AC Restore** e inizia la carica; a 12,6 V invia l'evento **Battery Restore** (batteria a posto).

Per soddisfare il requisito di Classe II la batteria deve ricaricarsi entro 72 ore, per la Classe III entro 24 ore – ciò dipende dalla capacità della batteria insieme alla corrente di carica di 500 mA.

2.3 Contenuto della confezione, contenitori: K01 e K02

La centrale è disponibile da sola (scheda) oppure con contenitore metallico predisposto. La confezione di fabbrica della scheda contiene: la scheda "FLEXi" SP3, un cavo di collegamento della batteria, 20 resistenze da 2,2 kΩ e 10 da 4,7 kΩ, 4 distanziali in plastica per il fissaggio e, per le versioni con modem, l'antenna ME301M con base magnetica e cavo da 2,5 m (2 pezzi secondo la distinta di imballaggio di fabbrica). Il **cavo USB Mini-B** necessario per la programmazione e la batteria non sono inclusi nella confezione.

Nelle versioni con contenitore la centrale è montata in un contenitore metallico dotato di interruttore antimanomissione, con alimentazione predisposta: alimentatore switching Mean Well APV-35-24, punto di collegamento della rete a 230 V con fusibile da 3,15 A, tutto già cablato. Ci sono due dimensioni di contenitore:

Contenitore	Dimensioni	Nota
K01 – contenitore metallico di dimensioni normali	285 × 280 × 80 mm	per tutte le versioni SP3
K02 – contenitore metallico piccolo	200 × 210 × 80 mm	la versione Ethernet + 4G non ci sta

Scatola metallica media con alimentatore per FLEXi SP3

Scatola metallica piccola con alimentatore per FLEXi SP3

In entrambi i contenitori (K01 e K02) c'è un alimentatore switching Mean Well con morsettiera dotata di fusibile da 3,15 A; nei contenitori K01 più vecchi c'era ancora un trasformatore 230 V / 16 V, 40 VA. Con i kit di fabbrica (SP3 KIT, SP3 KITi), oltre alla scheda montata nel contenitore metallico, sono forniti 2 antenne ME301M (con cavo da 2,5 m), un cavo di collegamento della batteria, 20 resistenze da 2,2 kΩ e 10 da 4,7 kΩ e un sensore antimanomissione.

2.4 I passaggi della messa in servizio in breve

Cosa ti servirà

Cavo USB Mini-B · cacciavite a taglio per le morsettiere · le resistenze da 2,2 kΩ e 4,7 kΩ fornite nella confezione · batteria 12 V 7 Ah · per la versione con modem una nano-SIM attiva con servizio dati mobili (disattiva prima la richiesta del PIN in un telefono) · per la versione Wi-Fi il nome e la password della rete · il software TrikdisConfig su un computer Windows.

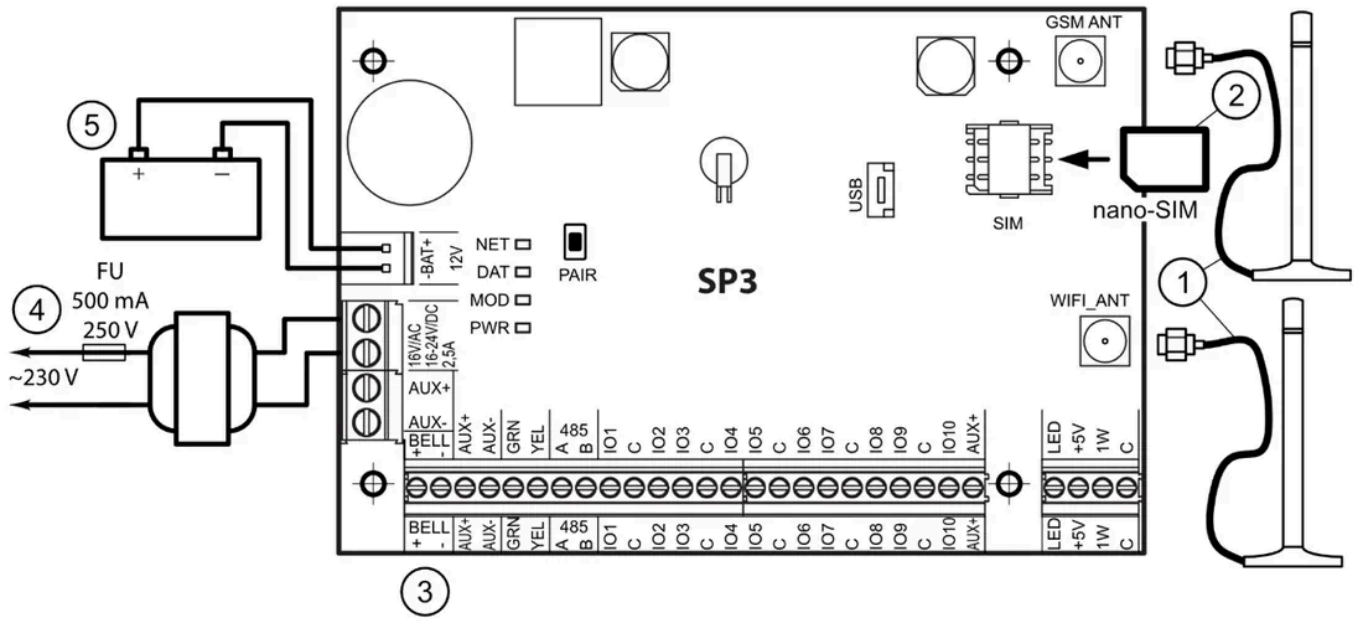


Figura 4. Collegamento dell'alimentazione e ordine di messa in servizio. Alimentazione di rete: trasformatore (“Transformer”), ~230 V / 16 V, 40 VA, 50 Hz, con fusibile da 500 mA / 250 V (FU) sul ramo a 230 V, oppure alimentatore in corrente continua da 16–24 V, 2,5 A (“or DC power supply source 16-24 V, 2,5 A”); alimentazione di riserva: batteria (“Battery”), 12 V, 7 Ah.

- 1 Avvitare le antenne mobile e Wi-Fi sui connettori d'antenna
- 2 Inserire la scheda nano-SIM nello slot SIM
- 3 Collegare i dispositivi alle morsettiere
- 4 Collegare l'alimentazione di rete ai morsetti AC/DC
- 5 Collegare la batteria ai morsetti BAT+ / BAT–

1. **Progetta il sistema.** Stabilisci la posizione del contenitore, delle tastiere, dei segnalatori acustici e luminosi e dei dispositivi comandati; in base all'area da proteggere e alle caratteristiche dei rivelatori decidi numero, tipo e posizione dei rivelatori.
2. **Monta la scheda nel contenitore** con i distanziali in plastica e collega a terra il contenitore metallico (paragrafo 3.1).
3. **Avvita le antenne** (mobile e Wi-Fi) e inserisci la scheda nano-SIM attivata (versione con modem).
4. **Collega i dispositivi** secondo gli schemi di collegamento: contatti magnetici, rivelatori di movimento, antincendio e altri (3.2–3.3), sirena (3.4), tastiere e lettori (3.5–3.6), sensore di temperatura (3.7), relè e spia luminosa (3.8), l'interruttore antimanomissione del contenitore; espansioni e ricevitori radio secondo il capitolo 4.
5. **Collega l'alimentazione di rete** ai morsetti AC/DC. All'accensione la centrale riconosce le tastiere, le espansioni e i lettori collegati correttamente al bus 1-WIRE e GRN / YEL (paragrafo 3.9).
6. **Collega la batteria** ai morsetti BAT+ / BAT−.
7. **Configura la centrale con TrikdisConfig** tramite cavo USB (capitolo 6). Le impostazioni di fabbrica vanno bene per la maggior parte degli edifici piccoli e medi; cosa va tipicamente controllato: aree e dati di base del sistema (**System Options**, 6.2), tipo e comportamento delle zone (**Zones**, 6.7), utenti, i loro codici e numeri di telefono (**Users & Reporting**, 6.4), l'ora esatta (6.2), i dati della scheda SIM (6.2), i ricevitori della centrale di vigilanza – disattivati di fabbrica (**Reporting to CMS**, 6.3) –, il cloud Protegus – attivato di fabbrica – e le notifiche SMS (6.4, 6.10), il funzionamento delle uscite PGM (6.8). Le impostazioni consigliate in dettaglio:
    - **Sistema.** Se vuoi inserire i gruppi di zone separatamente, dividi il sistema in aree e imposta le proprietà delle aree (6.2.2). Imposta ogni zona secondo le caratteristiche del rivelatore e il comportamento d'allarme desiderato per l'evento della zona (6.7); in un sistema diviso in aree, assegni ogni zona all'area desiderata. Per la gestione dalla tastiera, con chiave iButton o dal telefono (via SMS) occorre creare gli utenti e assegnare loro i permessi (6.4).
    - **Invio dei messaggi.** L'ora esatta va impostata affinché i messaggi ricevano la marca temporale corretta (6.2.1). La segnalazione degli eventi è abilitata di fabbrica per tutti gli eventi: quando si verifica un evento, la sua segnalazione va ai destinatari impostati sui canali impostati; la segnalazione di singoli eventi si può disabilitare nella finestra **System events** (6.10). Se la centrale trasmette sulla rete mobile, inserisci i dati della scheda SIM (6.2.1). La trasmissione alla centrale di vigilanza è disattivata di fabbrica (6.3). Il cloud Protegus è attivato di fabbrica, le notifiche SMS e le chiamate sono disattivate; l'impostazione dell'invio al telefono dell'utente è nel paragrafo 6.10.
    - **Controllo a distanza.** Con chiamata e SMS può controllare il sistema chi ha il proprio numero di telefono nell'elenco utenti (6.4). Con una chiamata non si può solo inserire e disinserire l'intero sistema o una sua parte, ma anche accendere e spegnere le apparecchiature collegate alle uscite PGM – cosa impostare sull'uscita a questo scopo è descritto nel paragrafo 5.4. Via SMS si possono anche modificare alcuni parametri di funzionamento della centrale, inserire e disinserire l'intero sistema o una sua parte e comandare le apparecchiature collegate alle uscite PGM – l'elenco dei comandi è nel paragrafo 5.3.
8. **Sostituisci i codici di fabbrica** con valori noti solo a te: il codice master nella finestra **Users & Reporting**, la password SMS nel campo **SMS Password** del gruppo **System Options** → **Access**, i codici di accesso a TrikdisConfig nello stesso gruppo **Access**.
9. **Collega il sistema all'app Protegus 2** (paragrafo 5.1).
10. **Verifica il funzionamento** secondo il capitolo 8: evento dalla tastiera, ricezione presso la centrale di vigilanza e in Protegus 2, uscite, inserimento a distanza.

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.

Questo capitolo descrive il montaggio della scheda, l'ordine dei collegamenti e poi il collegamento dei rivelatori, dei rivelatori di fumo, delle sirene, delle tastiere e dei lettori, dei sensori di temperatura e dei relè. Il significato dei morsetti è indicato nella tabella del paragrafo 1.5; il collegamento delle espansioni e dei moduli radio è nel capitolo 4. Nei disegni i nomi dei morsetti dell'SP3 sono a sinistra, quelli del dispositivo collegato a destra.

3.1 Ordine consigliato dell'installazione

Progettazione del sistema:

- Disegna la pianta dei locali e segna dove andranno il contenitore della centrale, la tastiera o le tastiere, i segnalatori acustici e luminosi e le apparecchiature comandate dalla centrale automaticamente o a distanza.
- In base al luogo, alle esigenze di protezione e alle caratteristiche dei rivelatori presi in considerazione, decidi numero, tipo e posizione dei rivelatori.

3.1.1 Montaggio della scheda nel contenitore

La scheda va in un contenitore in cui sono già presenti il trasformatore riduttore (con fusibile da 500 mA) e il posto per la batteria di riserva. Fissa la scheda nel contenitore in plastica o metallo scelto con **distanziali in plastica**; **il contenitore metallico deve essere collegato a terra**. Il contenitore deve soddisfare i requisiti delle norme EN 60950 ed EN 50131.

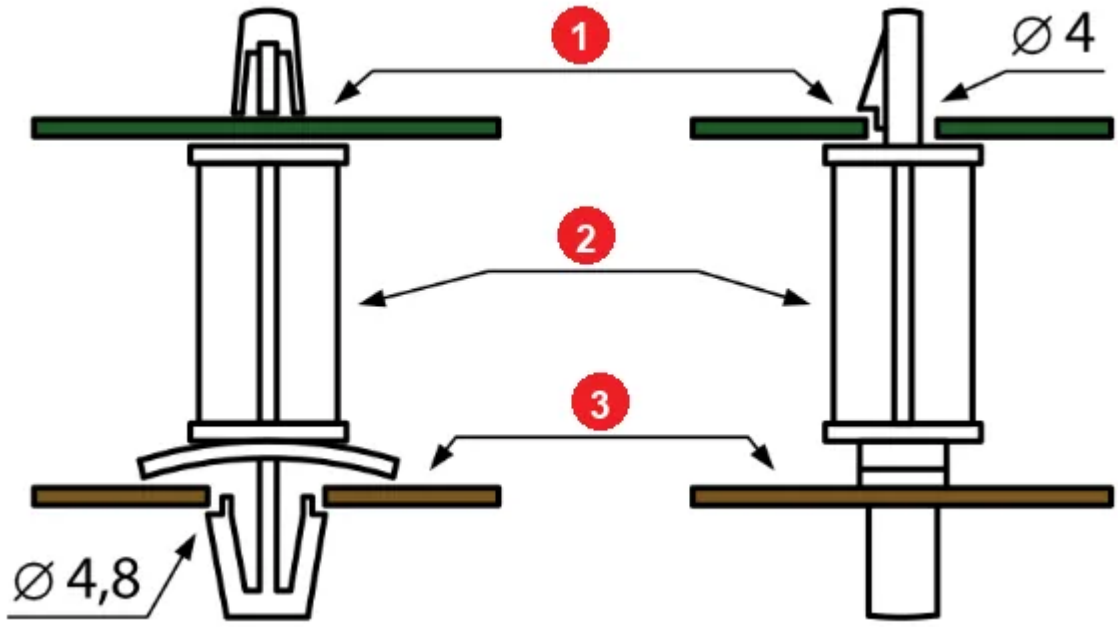


Figura 5. Fissaggio della scheda con distanziale in plastica (a sinistra vista frontale – “Front view”, a destra vista laterale – “Side view”). Il foro della scheda è Ø4 mm, quello del contenitore Ø4,8 mm.

- 1 la scheda a circuito stampato dell'SP3 (“SP3 circuit board”)
- 2 distanziale (“Spacer”)
- 3 il contenitore (“Box housing”)

Le dimensioni della scheda sono 116,5 × 78,5 mm. I centri dei quattro fori di fissaggio da Ø4 mm distano tra loro 93 mm in orizzontale e 61 mm in verticale; i fori di sinistra sono a 5 mm dal bordo sinistro, quelli in basso a 10 mm dal bordo inferiore.

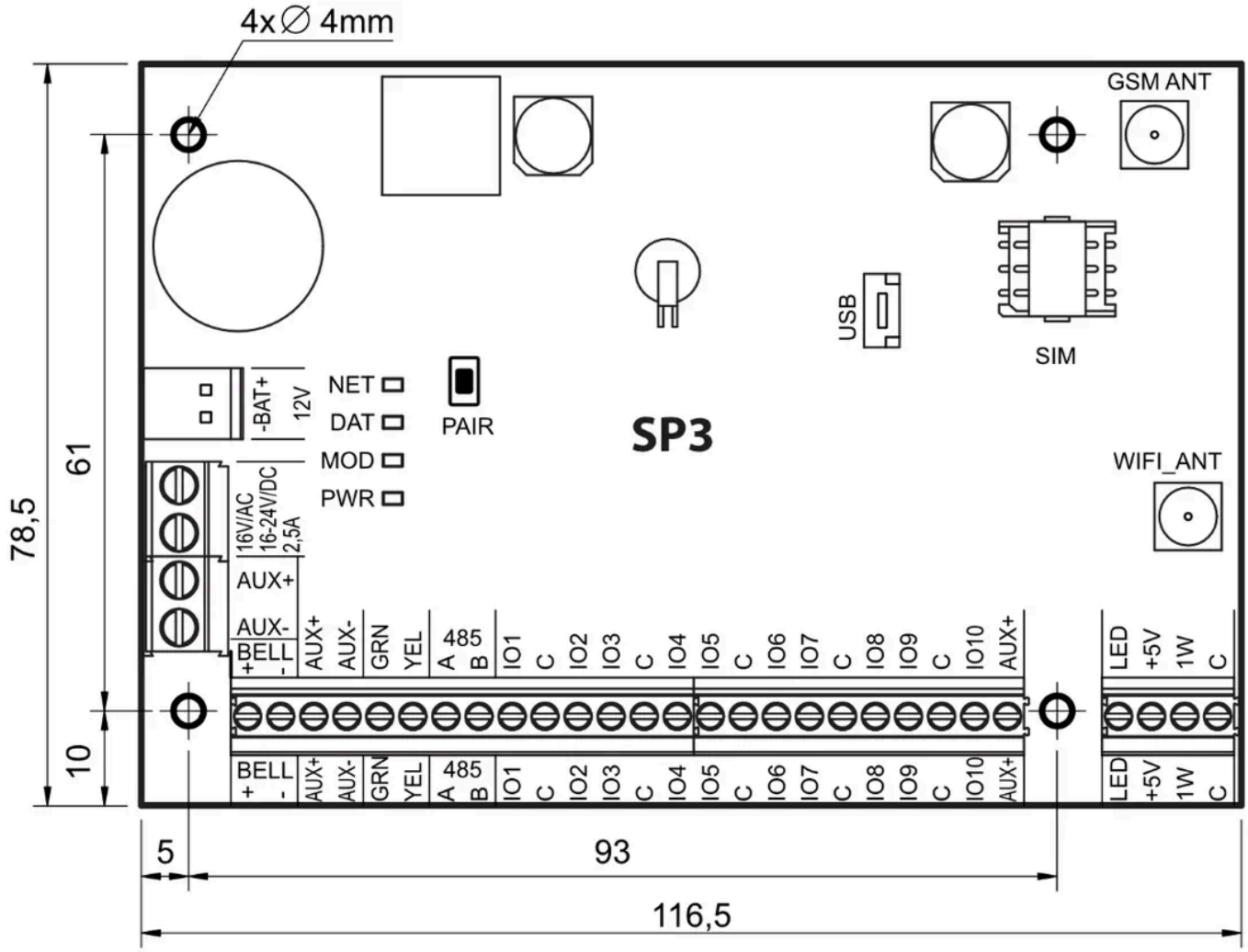


Figura 6. Dimensioni della scheda e dei fori di fissaggio in millimetri.

3.1.2 Ordine di collegamento dei dispositivi

Collega i dispositivi nell'ordine seguente; l'alimentazione e la batteria sempre per ultime.

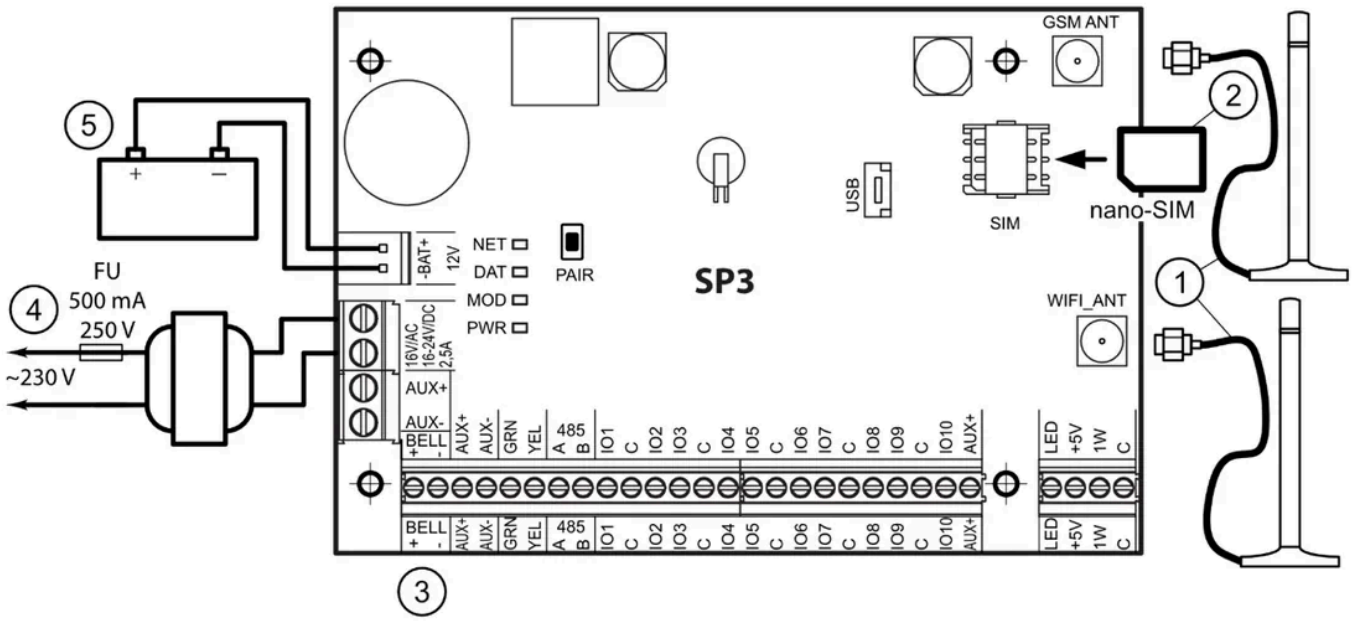


Figura 7. Panoramica dell'alimentazione e dei collegamenti. Alimentazione di rete: trasformatore ~230 V / 16 V, 40 VA, 50 Hz ("Transformer"; con fusibile da 500 mA, 250 V sul lato a 230 V) oppure alimentatore in corrente continua da 16–24 V, 2,5 A ("or DC power supply source 16-24 V, 2,5 A"); batteria di riserva ("Battery"), 12 V, 7 Ah.

- 1 antenna GSM e Wi-Fi sui connettori d'antenna
- 2 scheda nano-SIM nello slot SIM
- 3 i dispositivi sulla morsettiera esterna
- 4 alimentazione di rete sui morsetti AC/DC
- 5 batteria sui morsetti BAT+ / BAT−

1. Avvita l'**antenna GSM** e l'**antenna Wi-Fi** sui connettori d'antenna (a seconda della versione una o entrambe, paragrafo 1.2).
2. Nella versione con modem inserisci nello slot la **scheda nano-SIM attivata**. Conviene disattivare prima la richiesta del PIN in un telefono.
3. Nella versione Ethernet (SP3_3E, SP3_44E) inserisci il **cavo LAN** nel connettore RJ45.
4. In base agli schemi di collegamento riportati qui, agli schemi propri dei dispositivi collegati e al progetto, collega i contatti di apertura di porte e finestre, i rivelatori di movimento, antincendio e altri, i segnalatori acustici e luminosi, le tastiere e i dispositivi comandati. Collega ai morsetti della scheda anche l'**interruttore antimanomissione** dell'apertura dello sportello del contenitore e della rimozione dal muro.
5. Collega i fili dell'alimentatore di rete ai morsetti **AC/DC** della scheda e accendi l'alimentazione. La centrale riconosce le tastiere, le espansioni e le interfacce collegate correttamente al bus 1-WIRE e YEL/GRN.
6. Metti la batteria nel contenitore e collega i suoi capicorda ai morsetti **BAT+ / BAT−**.

La batteria deve ricaricarsi entro 72 ore perché il sistema soddisfi il livello di sicurezza 2 (Grado 2), ed entro 24 ore per il livello 3 (Grado 3).

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

L'ordine consigliato delle impostazioni (aree, zone, utenti, ora, trasmissione, controllo a distanza, sostituzione dei codici) è riassunto nel paragrafo 2.4, i dettagli nel capitolo 6.

3.2 Collegamento dei rivelatori

Sulla scheda **10 morsetti IO** (IO1–IO10) accolgono i circuiti dei rivelatori. Di fabbrica IO1–IO9 sono ingressi, IO10 è un'uscita PGM (reset rivelatori antincendio, vedi 3.3). Il numero di ingressi si può portare al massimo a 64 con le espansioni (iO, iO-8, iO-WL, RF-SH, iO-LORA, iO8-LORA). Qualsiasi morsetto può essere impostato come ingresso (zona), e nella pagina **Zones** (6.7) si possono definire le proprietà della zona: il tipo di circuito (**NO, NC, EOL, EOL_T, 3EOL, ATZ, ATZ_T**), la sensibilità agli eventi di breve durata sul circuito e la funzione della zona (ritardata, istantanea, istantanea stay, a seguire, a seguire stay, incendio, a chiave, 24 ore, silenziosa, silenziosa 24 ore). Le espansioni iO-8 e iO8-LORA supportano tutti i tipi di circuito della centrale.

Resistenze di fine linea. Per i circuiti EOL, EOL_T, 3EOL, ATZ e ATZ_T puoi scegliere in TrikdisConfig tra sette set di resistenze (**System Options** → **System general** → **EOL Type**, 6.2.1); per questo, quando sostituisci una vecchia centrale, le resistenze esistenti possono restare nei rivelatori. RT è la resistenza del circuito antimanomissione, R1 quella del primo rivelatore, R2 quella del secondo (con 3EOL quella del circuito di mascheramento). Accanto a ogni set sono indicate le centrali d'allarme i cui valori di resistenza di fabbrica coincidono con esso:

Set	RT	R1	R2
1 – predefinito Trikdis: Bosch AMAX, Risco LightSYS Plus, Satel INTEGRA (EOL)	**2,2 kΩ**	**2,2 kΩ**	**4,7 kΩ**
2 – Paradox, Honeywell Galaxy Flex, Hikvision AX Hybrid PRO (3EOL)	1 kΩ	1 kΩ	2,2 kΩ
3 – DSC PowerSeries, Eldes ESIM364	5,6 kΩ	5,6 kΩ	3,3 kΩ
4 – Eldes ESIM364 (modalità a 6 zone, con antimanomissione)	5,6 kΩ	3,3 kΩ	5,6 kΩ
5	3,3 kΩ	6,8 kΩ	3,3 kΩ
6 – Crow Runner, Texecom Premier Elite, Pyronix Enforcer	2,2 kΩ	4,7 kΩ	8,2 kΩ
7	4,7 kΩ	4,7 kΩ	2,2 kΩ

Per i produttori indicati coincidono la resistenza antimanomissione e quella del rivelatore (RT, R1), per la Satel INTEGRA il collegamento a una resistenza (EOL). Con il raddoppio zone (ATZ) e il collegamento 3EOL deve coincidere anche R2: ciò vale nel set 2 per Paradox e Hikvision AX Hybrid PRO, nel set 3 per Eldes ESIM364, nel set 6 per Crow Runner. Dove nella vecchia centrale il valore della resistenza era impostabile (ad esempio Crow, Risco, Honeywell Galaxy, Pyronix, Texecom), decide la resistenza presente nei rivelatori. Il collegamento Honeywell VISTA (2 kΩ) e quello Satel a due resistenze (2EOL, 2 × 1,1 kΩ) non coincidono con nessun set.

3.2.1 Schemi di collegamento

Nelle figure **IOx** è il morsetto IO scelto, **C** il morsetto negativo comune; NC è il contatto normalmente chiuso, NO quello normalmente aperto.

Simboli nei disegni. R1, R2, RT – resistenza (resistore); RT è la resistenza del circuito antimanomissione. La **T** rossa indica il contatto antimanomissione, il numero blu il numero d'ordine del rivelatore; il significato di ogni simbolo è riportato anche sotto il rispettivo disegno.

NO – normalmente aperto, senza resistenza di fine linea. Quando il rivelatore interviene, chiude il circuito tra IOx e C.

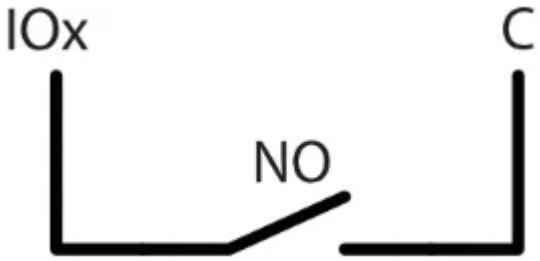


Figura 8. Zona NO: il contatto normalmente aperto tra il morsetto IOx e il morsetto C.

NC – normalmente chiuso, senza resistenza di fine linea. Quando il rivelatore interviene, interrompe il circuito tra IOx e C.

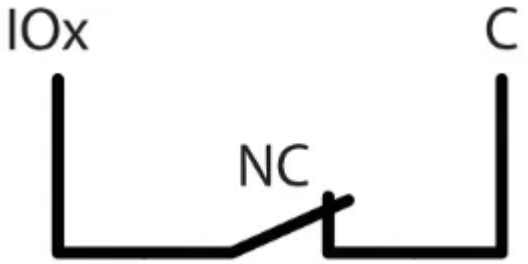


Figura 9. Zona NC: il contatto normalmente chiuso tra il morsetto IOx e il morsetto C.

EOL – con resistenza di fine linea. Con un rivelatore NO la R1 è in parallelo al contatto, con un rivelatore NC in serie con esso, tra IOx e C; così la centrale rileva anche il taglio e il cortocircuito del cavo.

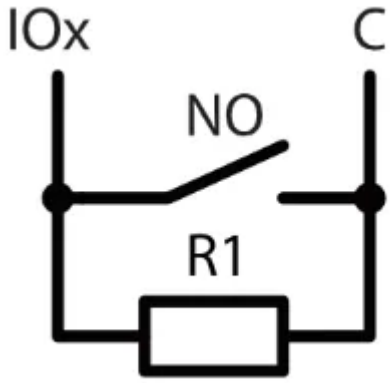


Figura 10. Zona NO con resistenza di fine linea (EOL): la R1 in parallelo al contatto aperto, tra IOx e C.

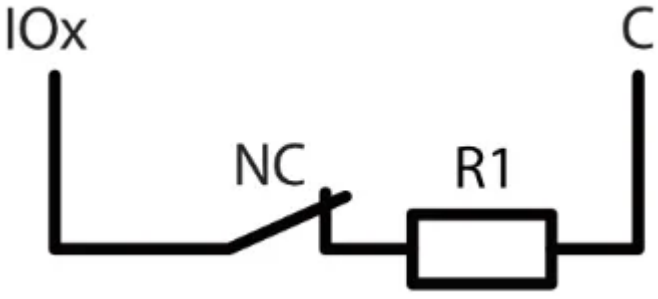


Figura 11. Zona NC con resistenza di fine linea (EOL): la R1 in serie con il contatto chiuso, tra IOx e C.

EOL_T – con resistenza di fine linea, rilevamento manomissione e guasto del cavo. Partendo da IOx, il contatto antimanomissione NC e la RT in serie, poi il contatto d'allarme NC in parallelo con R1 tra RT e C.

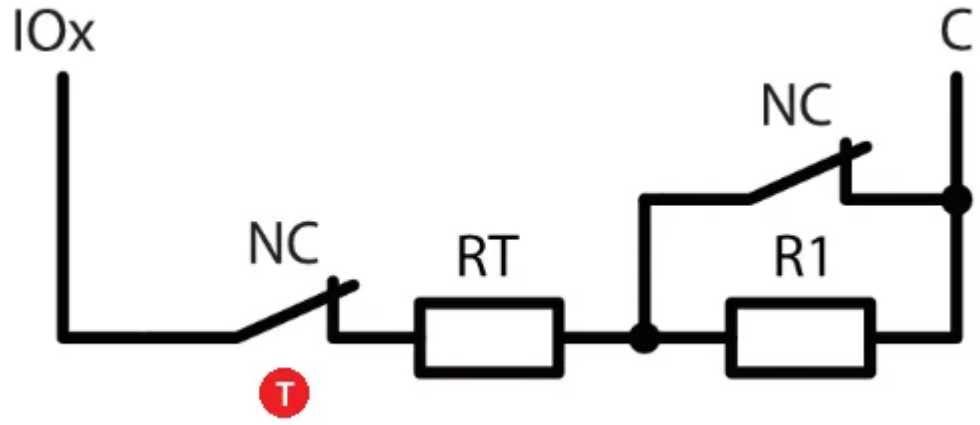


Figura 12. Zona EOL_T: IOx → contatto antimanomissione NC → RT → (contatto d'allarme NC in parallelo con R1) → C.

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

ATZ – raddoppio zone. Due rivelatori su un solo morsetto: tra IOx e C due circuiti in serie, nel primo un contatto NC in parallelo con R1, nel secondo un contatto NC in parallelo con R2. Così con 10 morsetti si gestiscono 20 zone.

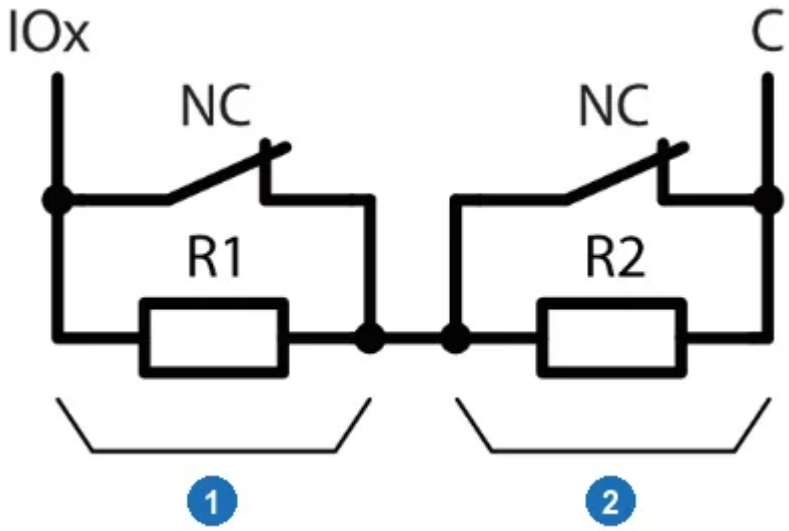


Figura 13. Zona ATZ: il contatto NC del 1° rivelatore in parallelo con R1, in serie con esso il contatto NC del 2° rivelatore in parallelo con R2, tra IOx e C.

- 1 il circuito del 1° rivelatore (“Detector terminal 1”)
- 2 il circuito del 2° rivelatore (“Detector terminal 2”)

ATZ_T – raddoppio zone con rilevamento manomissione e guasto del cavo. Come ATZ, ma nel circuito di entrambi i rivelatori è in serie anche il contatto antimanomissione NC, nel primo circuito insieme alla resistenza RT.

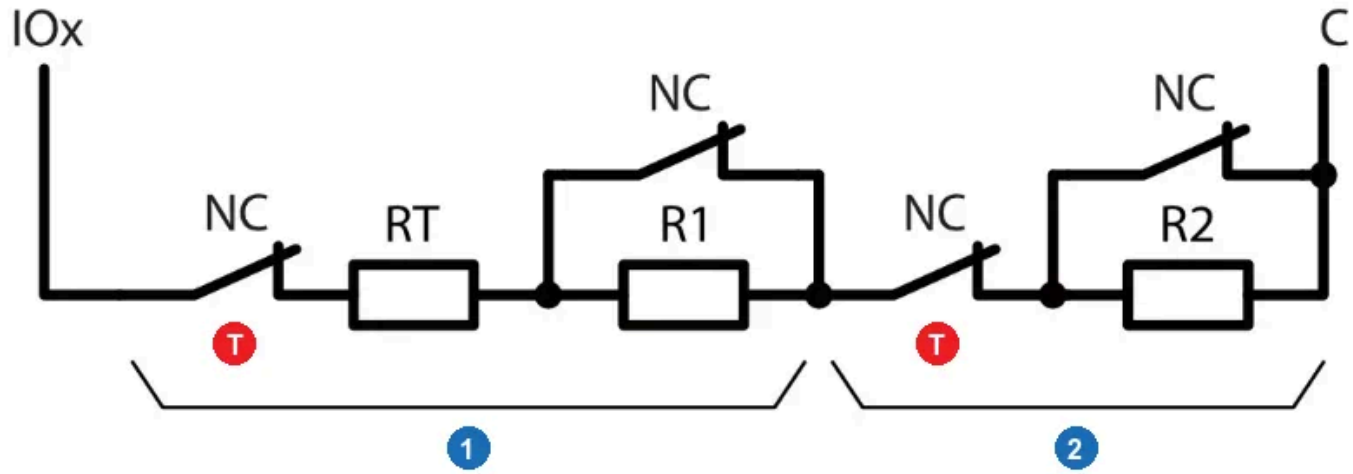


Figura 14. Zona ATZ_T: 1° rivelatore – contatto antimanomissione NC e RT in serie, poi contatto NC in parallelo con R1; 2° rivelatore – contatto antimanomissione NC in serie, poi contatto NC in parallelo con R2; i due circuiti in serie tra IOx e C.

- T contatto antimanomissione (“Tamper”), segnala l'apertura dell'involucro del rivelatore
- 1 il circuito del 1° rivelatore (“Detector terminal 1”)
- 2 il circuito del 2° rivelatore (“Detector terminal 2”)

3EOL – tre resistenze di fine linea: allarme, manomissione e mascheramento. All'interno di un solo rivelatore si riconoscono separatamente il circuito antimanomissione, quello d'allarme e quello antimascheramento (anti-masking).

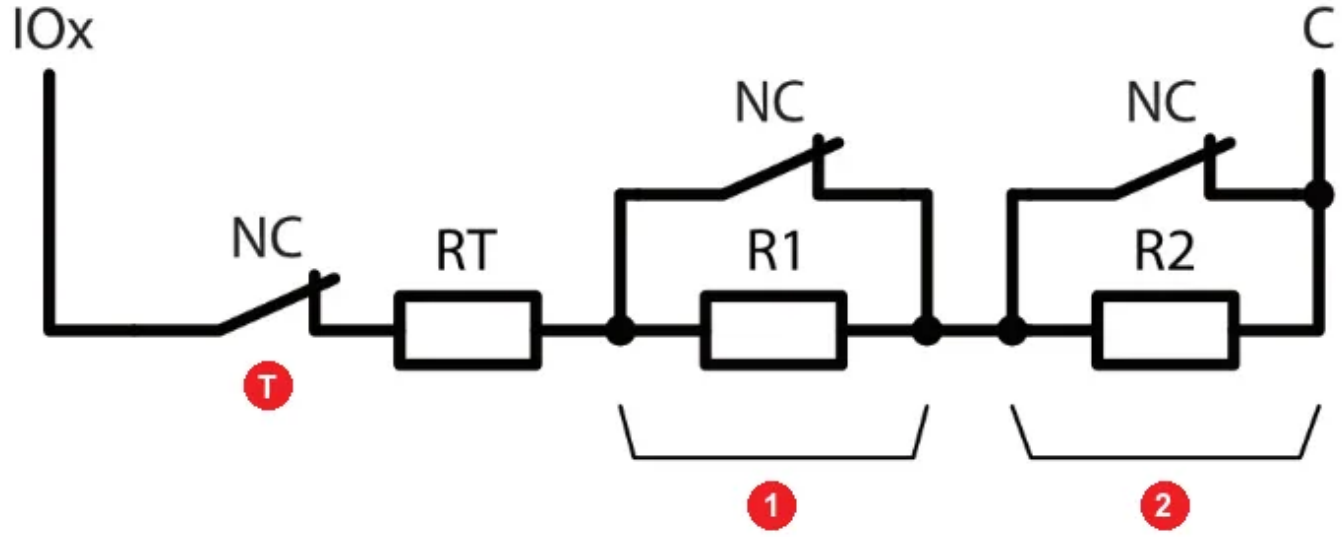


Figura 15. Zona 3EOL: IOx → contatto antimanomissione NC e RT in serie → circuito d'allarme (contatto NC in parallelo con R1) → circuito di mascheramento (contatto NC in parallelo con R2) → C.

- T contatto antimanomissione (“Tamper”), segnala l'apertura dell'involucro del rivelatore
- 1 circuito d'allarme (“Alarm”)
- 2 circuito antimascheramento (“Anti-masking”), segnala la copertura del rivelatore

3.3 Collegamento dei rivelatori di fumo

Rivelatori di fumo a due fili sull'uscita LED. Se colleghi i rivelatori d'incendio in questo modo, nella pagina **System Options** spunta la casella **LED out as 2Wire fire** (6.2).

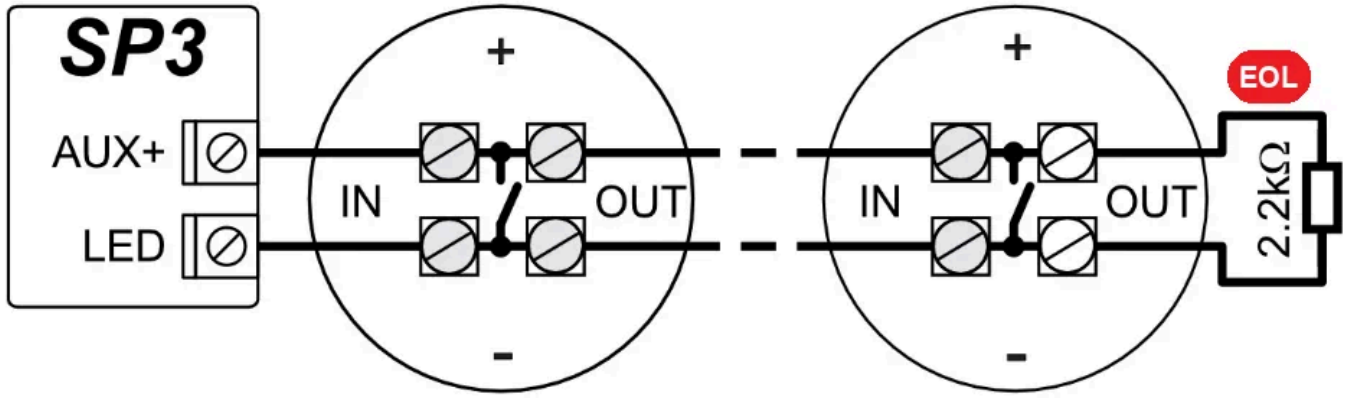


Figura 16. Rivelatori di fumo a due fili sull'uscita LED: AUX+ → morsetto + IN del primo rivelatore, LED → − IN; i morsetti + OUT e − OUT di ogni rivelatore sullo stesso morsetto IN del rivelatore successivo; dopo l'ultimo rivelatore una resistenza di fine linea da 2,2 kΩ tra il filo + e il filo −.

- EOL resistenza di fine linea da 2,2 kΩ (“End of line resistor”)

Rivelatori di fumo a quattro fili. All'ingresso del circuito dei rivelatori di fumo (IOx) assegna la funzione di zona **incendio** (6.7). L'alimentazione dei rivelatori a quattro fili è commutata dall'uscita PGM IO10, a cui è associata la funzione **Fire Sensor Reset** (reset rivelatori antincendio) (6.8) – questa è l'impostazione di fabbrica di IO10. Il relè K1 segnala il taglio del cavo e la rimozione del rivelatore.

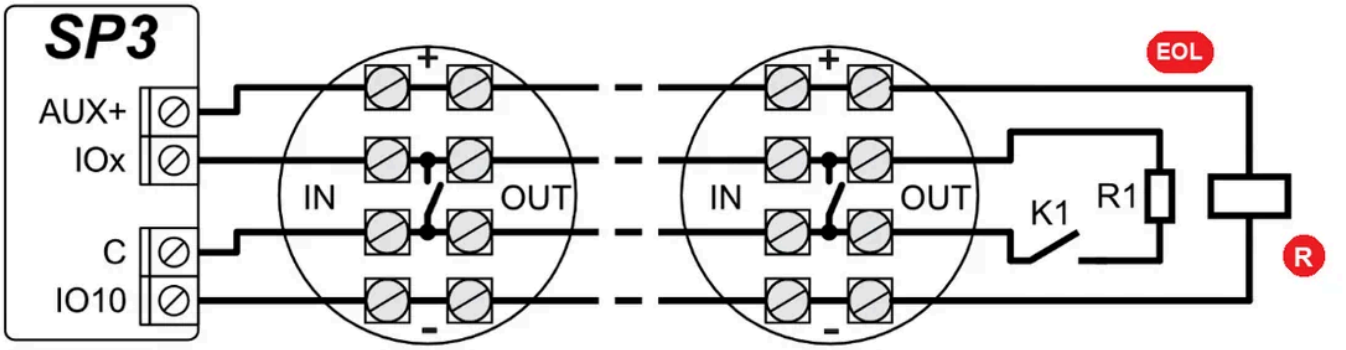


Figura 17. Rivelatori di fumo a quattro fili con relè K1. Dall'alto verso il basso: AUX+ → morsetto + del primo rivelatore, IOx → contatto superiore, C → contatto inferiore, IO10 → − IN; i quattro morsetti OUT sullo stesso morsetto IN del rivelatore successivo; dopo l'ultimo rivelatore il contatto di K1 e la resistenza di fine linea R1 in serie tra il filo IOx e il filo C; la bobina di K1 tra il filo AUX+ e il filo IO10.

- R relè **K1** (“Relay”)
- EOL la resistenza di fine linea **R1** (“End of line resistor”)

Rivelatori di fumo a due fili con interfaccia SM1. Con l'interfaccia SM1 i rivelatori a due fili si possono collegare a un ingresso IO; anche qui il relè K1 segnala il taglio del cavo e la rimozione del rivelatore. Il circuito di supervisione si può realizzare in due modi:

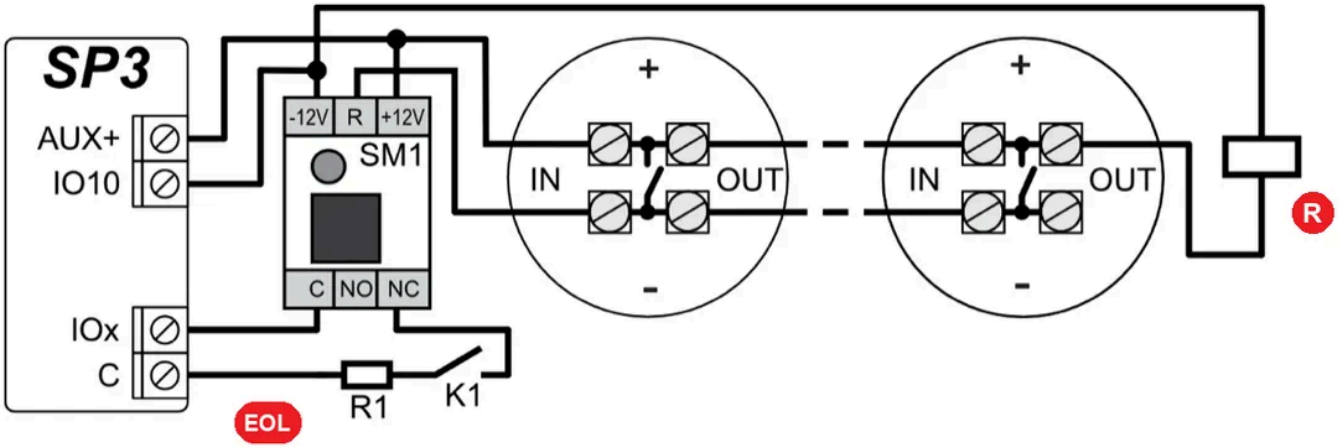


Figura 18. Rivelatori di fumo a due fili con interfaccia SM1: AUX+ → SM1 +12V e + IN del primo rivelatore; IO10 → SM1 −12V e la bobina di K1; SM1 R → − IN del rivelatore; i morsetti IN/OUT dei rivelatori in catena, l'ultimo + OUT su K1. Circuito di supervisione: IOx → SM1 C; morsetto C dell'SP3 → resistenza di fine linea R1 → contatto K1 → SM1 NC.

- R relè **K1** (“Relay”)
- EOL la resistenza di fine linea **R1** (“End of line resistor”)

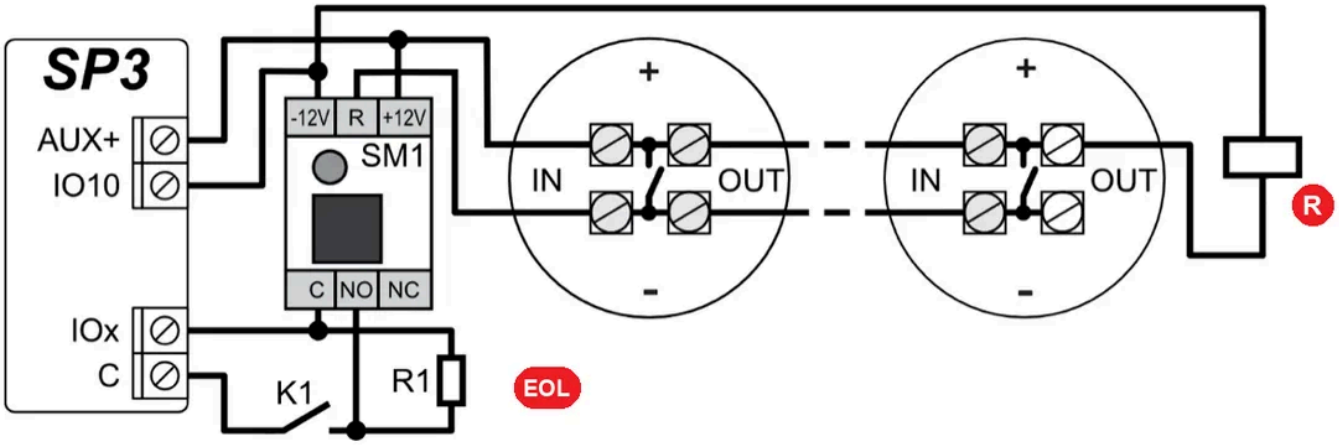


Figura 19. Lo stesso con l'altro circuito di supervisione: la R1 tra i morsetti C e NO dell'SM1; il morsetto C dell'SP3 tramite il contatto di K1 sul morsetto NO dell'SM1.

- R relè **K1** (“Relay”)
- EOL la resistenza di fine linea **R1** (“End of line resistor”)

3.4 Collegamento della sirena

Collega la sirena all'uscita **BELL+ / BELL−** (la portata dell'uscita BELL è 1 A, vedi i dati tecnici nel paragrafo 1.3).

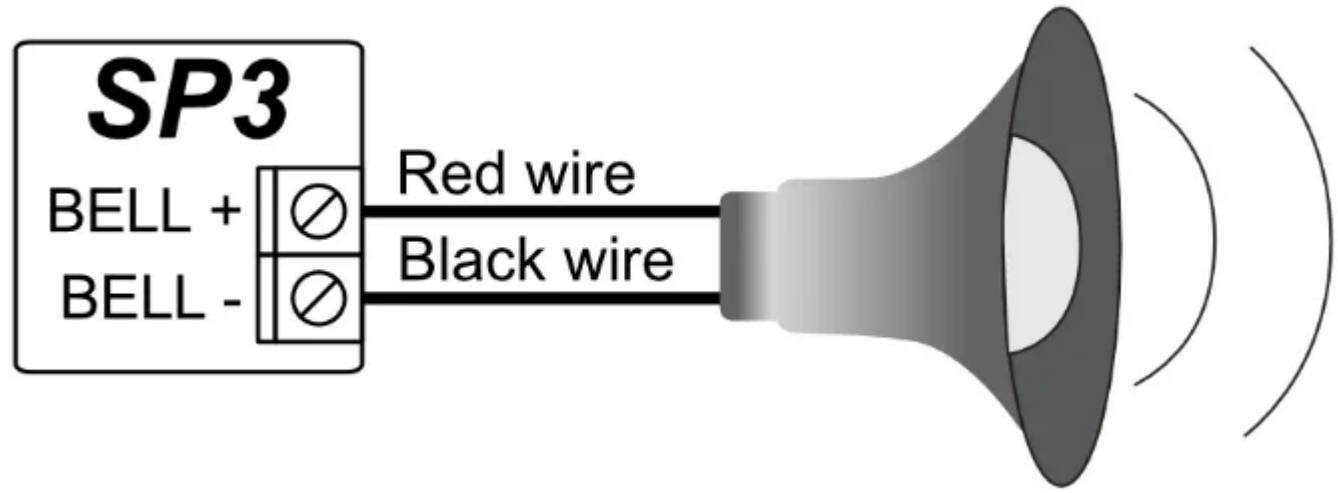


Figura 20. Sirena sull'uscita BELL: BELL+ → filo rosso, BELL− → filo nero.

Con la sirena da esterno MR100 anche il circuito antimanomissione (SAB) è supervisionato dalla centrale: di fabbrica con EOL da 2,2 kΩ, sull'ingresso **IO9**. Di fabbrica IO9 è una zona 24 ore, ma si può modificare liberamente. Se nella centrale supervisioni il circuito antimanomissione della sirena con un'altra modalità EOL, chiudi i contatti JPS1 e inserisci in serie nel circuito antimanomissione una resistenza di valore adeguato.

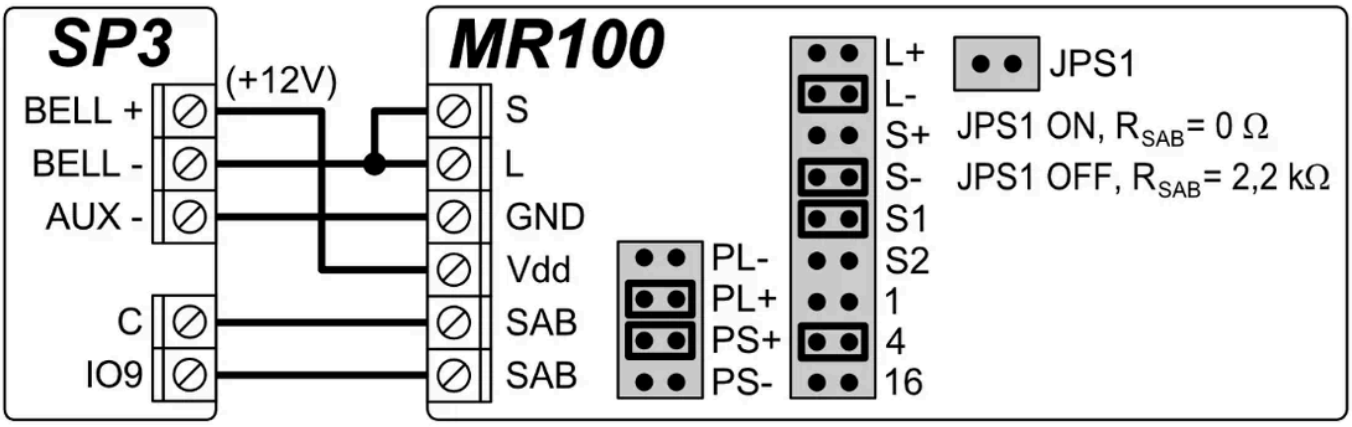


Figura 21. Sirena da esterno MR100 (“Outdoor siren”): BELL+ (+12 V) → Vdd, BELL− → S e L, AUX− → GND, C e IO9 → i due morsetti SAB (antimanomissione). Punti cortocircuitati nel disegno: PL+, PS+, L−, S−, S1 e 4. JPS1 chiuso (“ON”): R_SAB = 0 Ω, JPS1 aperto (“OFF”): R_SAB = 2,2 kΩ.

3.5 Collegamento di tastiere e lettori RFID

Rientrano qui le tastiere sul bus tastiere e i lettori RFID con protocollo Wiegand 26/34. Sul bus tastiere (**GRN**, **YEL**) si possono collegare al massimo **8 tastiere dello stesso tipo**. Il tipo di tastiera si imposta nella pagina **Modules** (6.5); i dispositivi collegati vengono riconosciuti e assegnati automaticamente dalla centrale. La tastiera ha anche un proprio ingresso di zona (ZONE): l'altro capo del rivelatore collegato qui va sul morsetto AUX−. La gestione del sistema dalle tastiere (codici utente, esclusione zone, iButton e RFID, chiamata, SMS, uscite PGM) è descritta nel manuale utente SP3 separato, realizzato per le tastiere Protegus e Paradox.

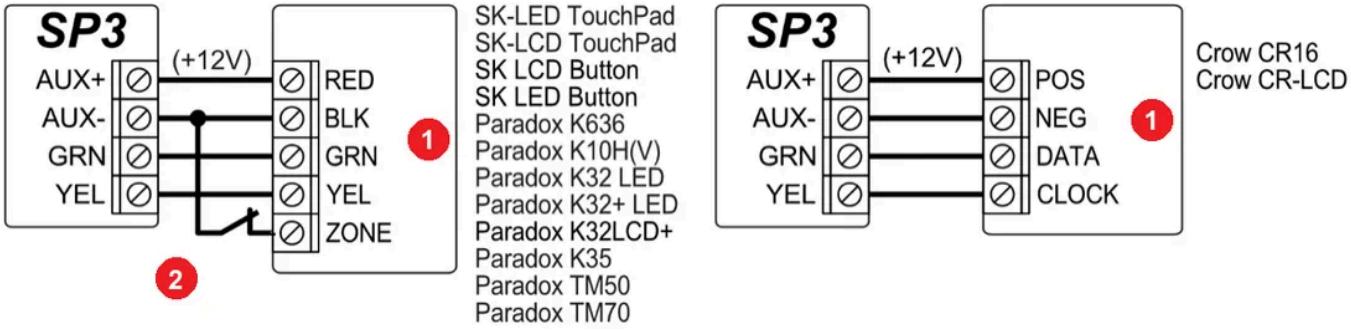


Figura 22. Collegamento delle tastiere. SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, nonché Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50, TM70: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; il morsetto ZONE della tastiera tramite il contatto del rivelatore sul morsetto AUX−. Crow CR16 e CR-LCD: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK.

- 1 tastiera (“Keypad”)
- 2 la zona della tastiera (“Keypad zone”)

Lettore RFID (Wiegand 26/34). Alla centrale si possono collegare al massimo **2 lettori**. I fili dati del lettore (D0, D1) vanno o sul bus tastiere (GRN, YEL) o sui morsetti **IO1** e **IO2**, secondo le figure. Se ci sono due lettori (lato ingresso e lato uscita), alla centrale non si può più collegare una tastiera.

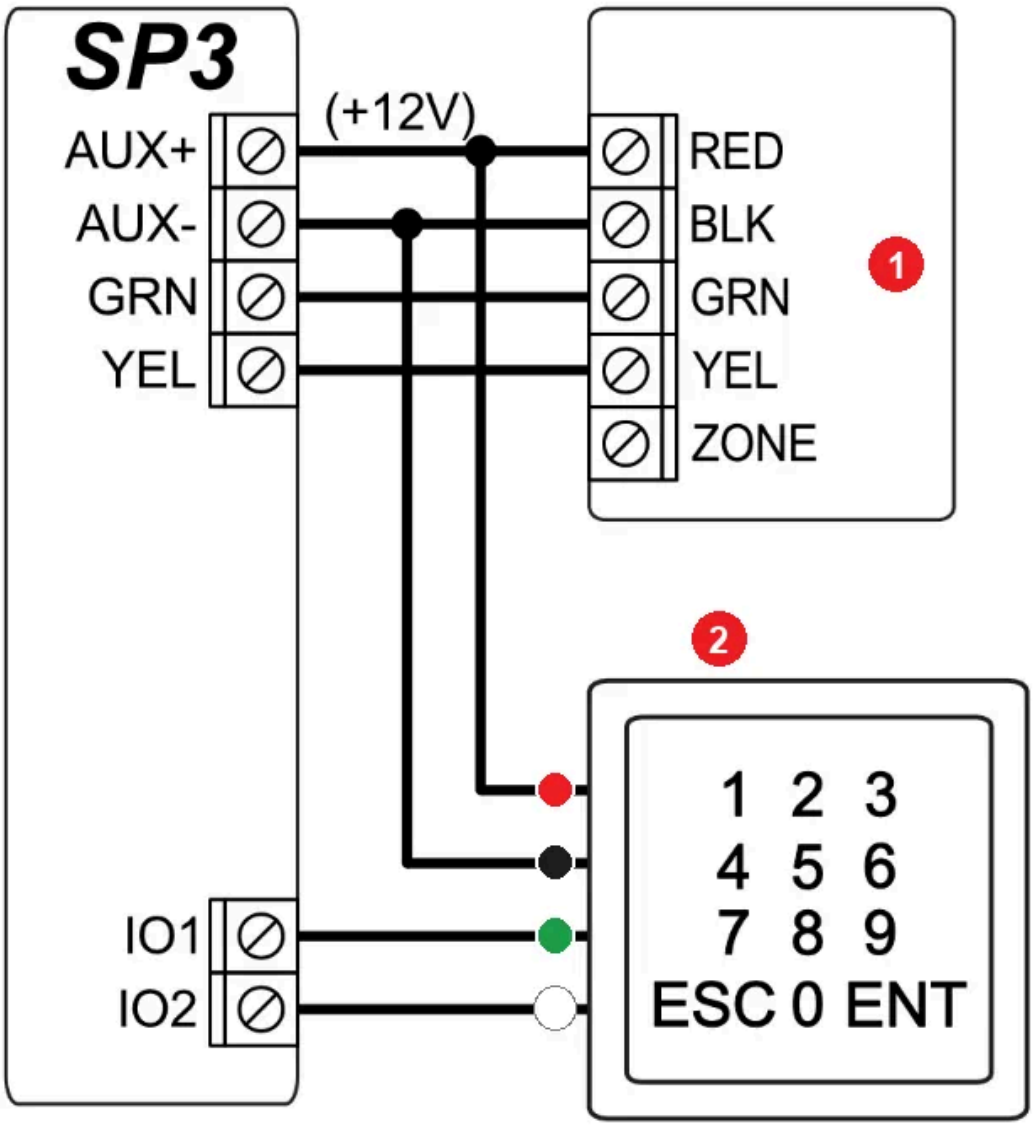


Figura 23. Tastiera e lettore d'ingresso insieme. La tastiera (SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50 o TM70) sul bus come nella figura precedente: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; filo rosso del lettore (+U) → AUX+, nero (GND) → AUX−, verde (D0) → IO1, bianco (D1) → IO2.

- 1 tastiera (“Keypad”)
- 2 lettore d'ingresso: lettore RFID con tastiera, Wiegand 26/34 (“Entry reader”, “RFID reader with keypad (Wiegand 26/34)”)
- filo rosso, +U (“R - red wire (+U)”)
- filo nero, GND (“B - black wire (GND)”)
- filo verde, D0 (“G - green wire (D0)”)
- filo bianco, D1 (“W - white wire (D1)”)

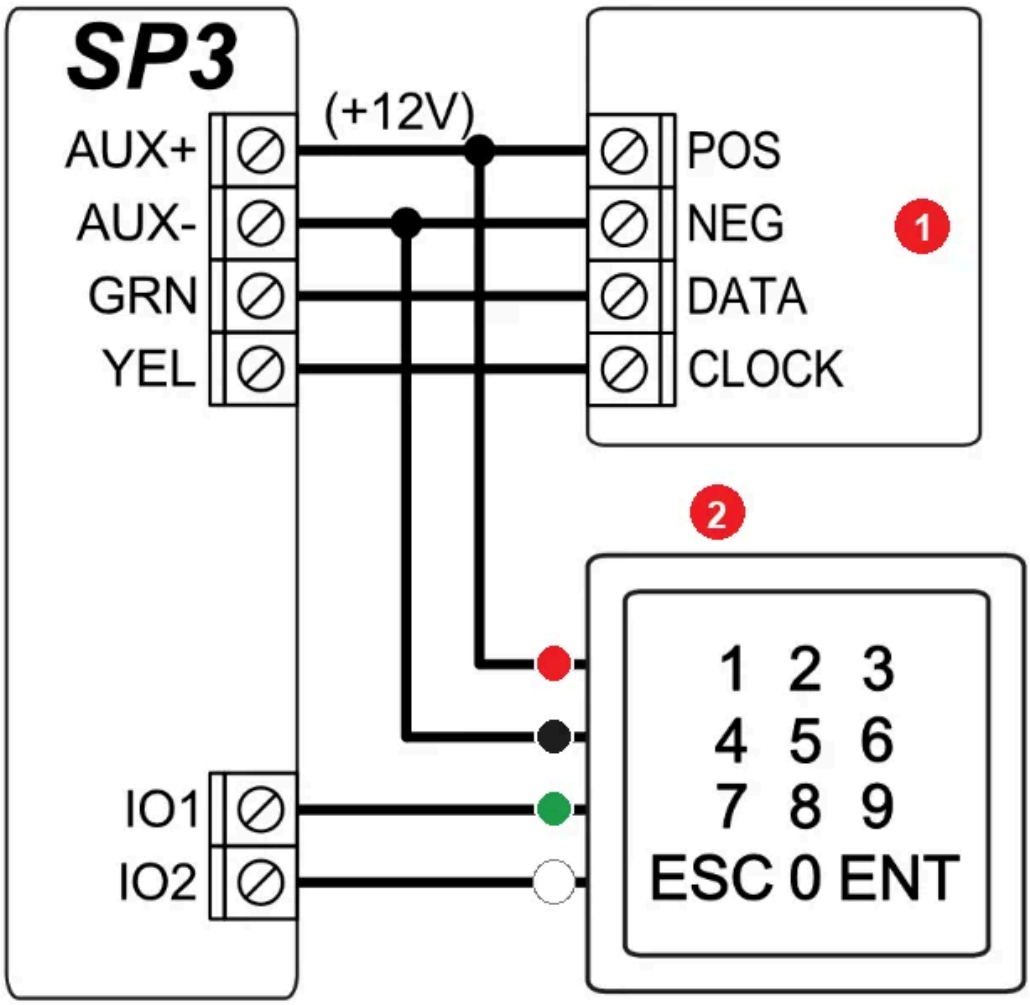


Figura 24. Tastiera Crow CR16 o Crow CR-LCD e lettore d'ingresso insieme. La tastiera sul bus: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK; filo rosso del lettore (+U) → AUX+, nero (GND) → AUX−, verde (D0) → IO1, bianco (D1) → IO2.

- 1 tastiera (“Keypad”)
- 2 lettore d'ingresso: lettore RFID con tastiera, Wiegand 26/34 (“Entry reader”, “RFID reader with keypad (Wiegand 26/34)”)
- filo rosso, +U (“R - red wire (+U)”)
- filo nero, GND (“B - black wire (GND)”)
- filo verde, D0 (“G - green wire (D0)”)
- filo bianco, D1 (“W - white wire (D1)”)

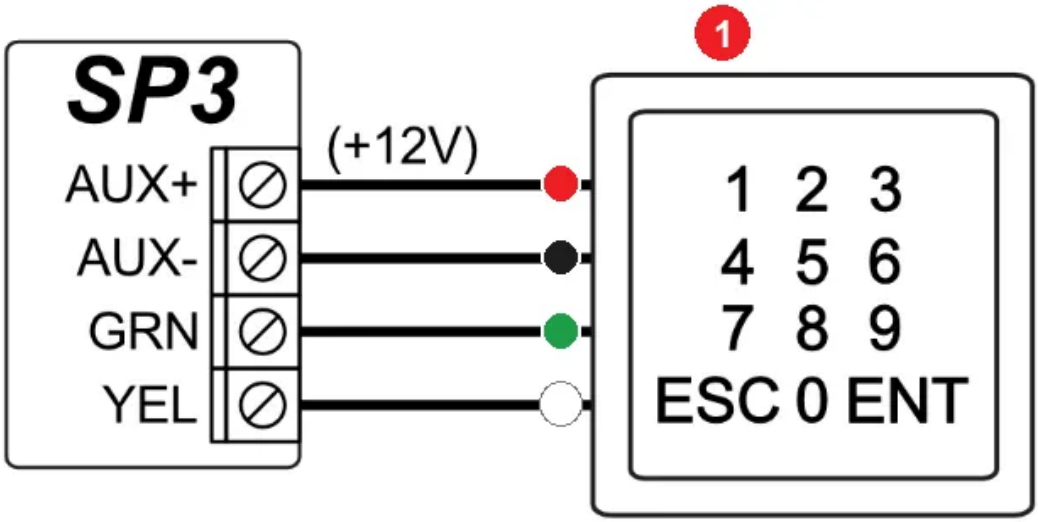


Figura 25. Un solo lettore sul bus tastiere, senza tastiera: filo rosso del lettore (+U) → AUX+, nero (GND) → AUX−, verde (D0) → GRN, bianco (D1) → YEL.

- 1 lettore d'ingresso: lettore RFID con tastiera, Wiegand 26/34 (“Entry reader”, “RFID reader with keypad (Wiegand 26/34)”)
- filo rosso, +U (“R - red wire (+U)”)
- filo nero, GND (“B - black wire (GND)”)
- filo verde, D0 (“G - green wire (D0)”)
- filo bianco, D1 (“W - white wire (D1)”)

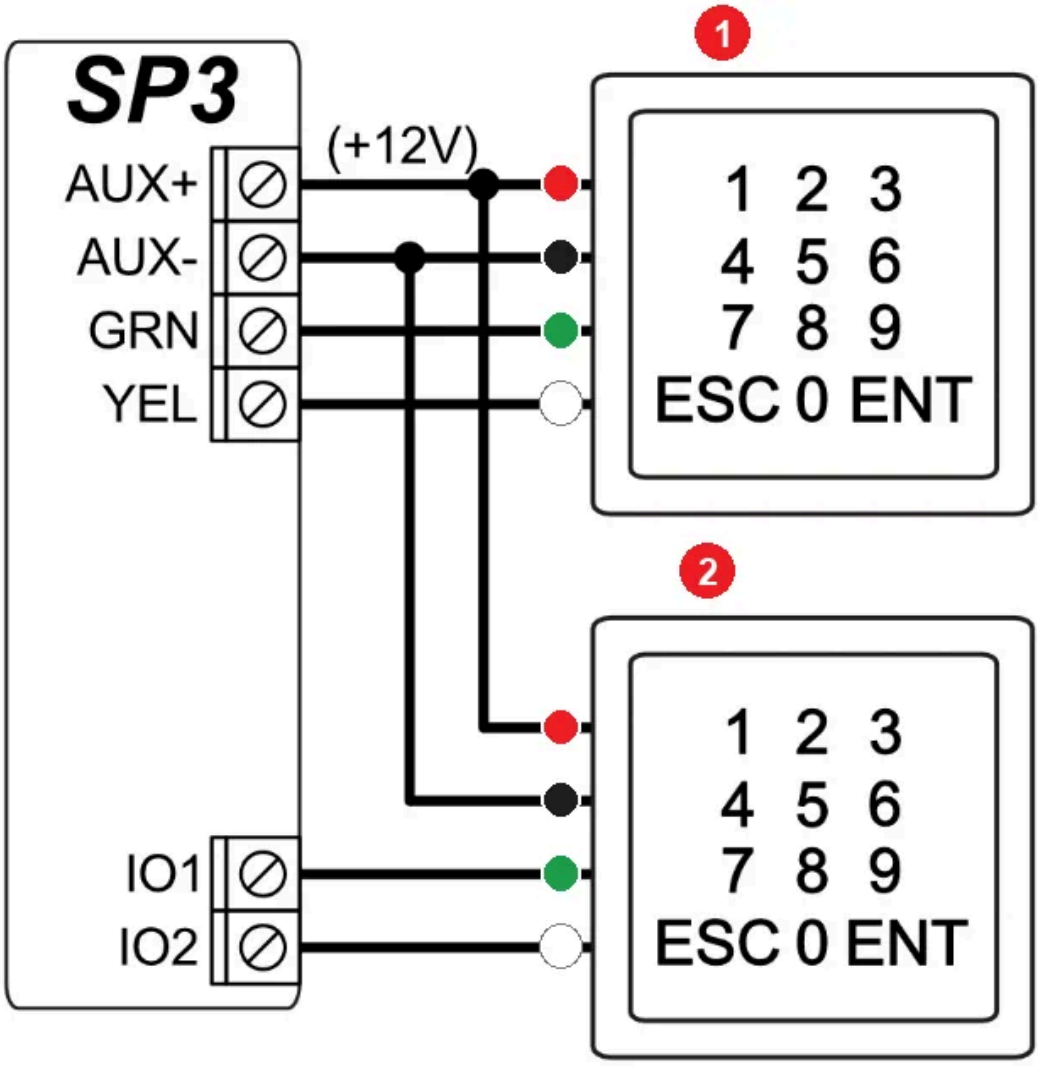


Figura 26. Due lettori, entrambi lettori RFID con tastiera, Wiegand 26/34 (“RFID reader with keypad (Wiegand 26/34)”). Lettore d'ingresso: filo rosso (+U) → AUX+, nero (GND) → AUX−, verde (D0) → GRN, bianco (D1) → YEL. Lettore d'uscita: rosso (+U) → AUX+, nero (GND) → AUX−, verde (D0) → IO1, bianco (D1) → IO2.

- 1 lettore d'ingresso (“Entry reader”)
- 2 lettore d'uscita (“Exit reader”)
- filo rosso, +U (“R - red wire (+U)”)
- filo nero, GND (“B - black wire (GND)”)
- filo verde, D0 (“G - green wire (D0)”)
- filo bianco, D1 (“W - white wire (D1)”)

3.6 Collegamento dei lettori di chiavi TM17 e CZ-Dallas

Accessorio fuori produzione

Il lettore di chiavi iButton **TM17** è un accessorio fuori produzione, non più disponibile. La descrizione è rimasta per i sistemi esistenti.

Il lettore di chiavi iButton **CZ-Dallas** si collega al bus **1 WIRE**, con un cavo lungo al massimo 30 m. Il lettore **TM17** si collega al bus **RS485**, con un cavo lungo al massimo 100 m.

I valori “al massimo 30 m” e “al massimo 100 m” sono massimi teorici, in condizioni ideali – vedi la nota del paragrafo 1.3.

Per la segnalazione luminosa del CZ-Dallas imposta il tipo dell'uscita **LED** su **System state** (stato del sistema) (6.8): con sistema inserito l'anello del lettore è rosso, con sistema disinserito giallo.

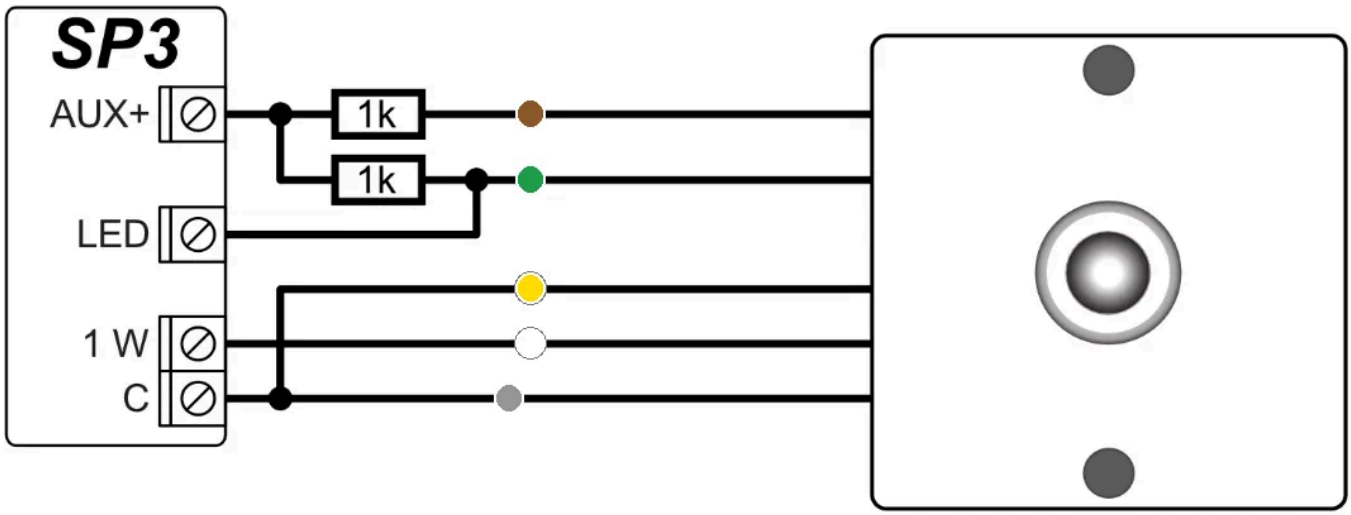


Figura 27. Lettore CZ-Dallas (“CZ-Dallas reader”): AUX+ → ciascuno tramite una resistenza da 1 kΩ sul filo marrone (RED LED+) e sul filo verde (GREEN LED+); l'uscita LED sul filo verde, dopo la resistenza; 1 W → filo bianco; C → filo giallo (LED−) e grigio. L'uscita LED va impostata sul tipo **System state** (stato del sistema) (“The output LED must be set to the »System state« type.”) – con allarme inserito la luce del lettore iButton è rossa (“Security alarm system is arm - the iButton reader light is red.”), con allarme disinserito gialla (“Security alarm system is disarm - the iButton reader light is yellow.”).

- filo marrone, RED LED+ (“Brown wire”, “RED LED+”) – la luce rossa
- filo verde, GREEN LED+ (“Green wire”, “GREEN LED+”) – la luce verde
- filo giallo, LED− (“Yellow wire”, “LED-”)
- filo bianco (“White wire”)
- filo grigio (“Gray wire”)

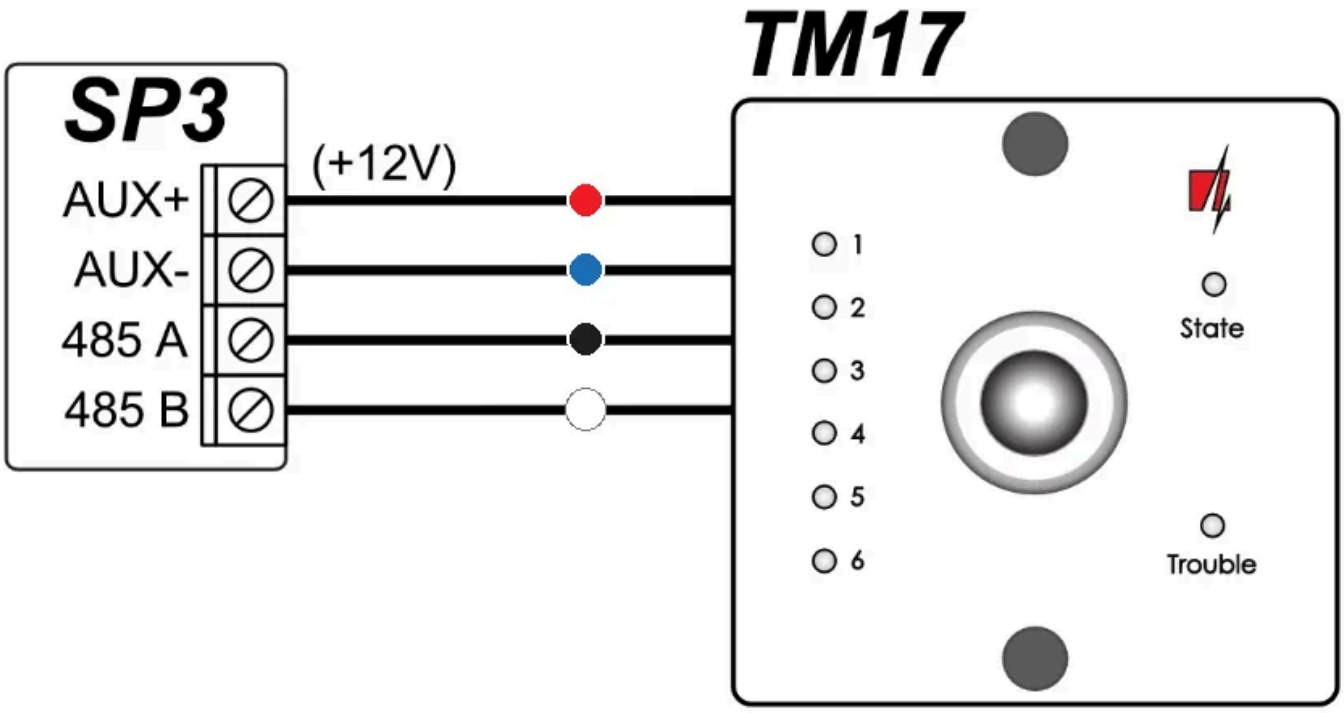


Figura 28. Lettore TM17: AUX+ (+12 V) → filo rosso, AUX− → blu, 485 A → nero, 485 B → bianco.

- filo rosso (“Red wire”)
- filo blu (“Blue wire”)
- filo nero (“Black wire”)
- filo bianco (“White wire”)

3.7 Collegamento dei sensori di temperatura

Sul bus 1 WIRE si possono collegare al massimo **8 sensori di temperatura Maxim / Dallas DS18S20 o DS18B20**, oppure **1 sensore di temperatura e umidità AM2301**; la centrale li riconosce e li assegna automaticamente, i valori si vedono nella pagina **Sensors** (6.9). Per cavi più lunghi di mezzo metro usa un cavo a coppie intrecciate (UTP 4×2×0,5 o STP 4×2×0,5). Il morsetto **+5V** della scheda alimenta i dispositivi collegati al bus 1 WIRE: 5 V DC, massimo 0,2 A, protetto contro il sovraccarico – se si supera la corrente consentita, l'uscita si spegne automaticamente.

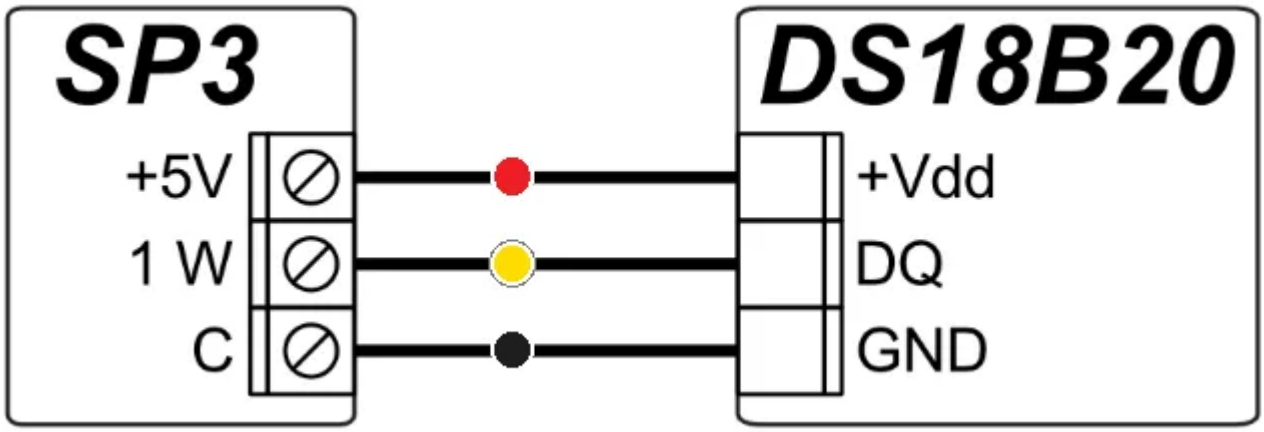


Figura 29. Sensore di temperatura DS18B20 (“Temperature sensor”): +5V → +Vdd (rosso), 1 W → DQ (giallo), C → GND (nero).

- filo rosso (“Red wire”)
- filo giallo (“Yellow wire”)
- filo nero (“Black wire”)

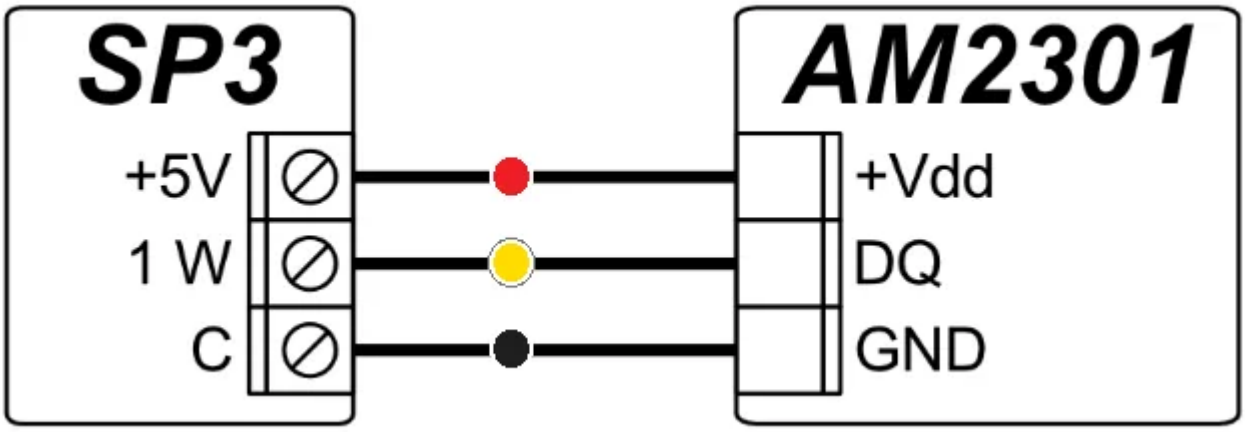


Figura 30. Sensore di temperatura e umidità AM2301 (“Temperature and humidity sensor”): +5V → +Vdd (rosso), 1 W → DQ (giallo), C → GND (nero).

- filo rosso (“Red wire”)
- filo giallo (“Yellow wire”)
- filo nero (“Black wire”)

3.8 Collegamento di relè e spia LED

Con i contatti del relè si possono comandare a distanza diverse apparecchiature elettriche. Il morsetto IO scelto va impostato come uscita (OUT), con la funzione **Remote control** (comando a distanza) (6.8). L'uscita IO è open collector, con portata massima di 100 mA, quindi i carichi maggiori vanno sempre comandati tramite relè.

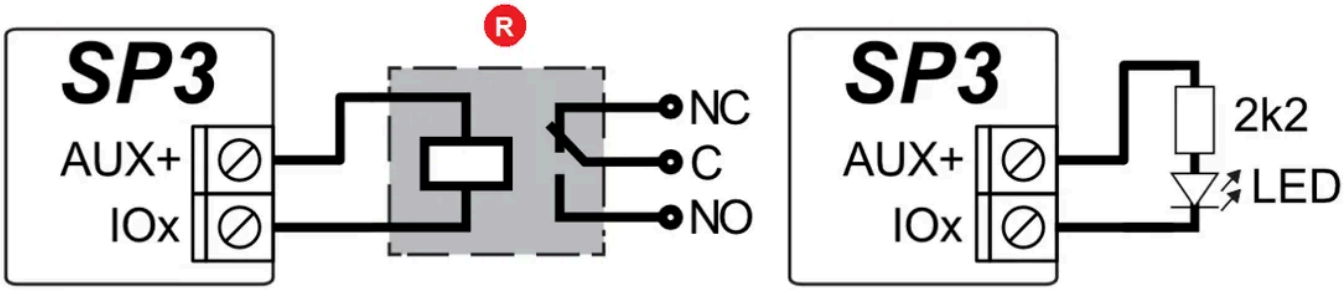


Figura 31. A sinistra relè: la bobina tra AUX+ e IOx, i contatti del relè NC, C, NO. A destra spia LED: AUX+ → resistenza da 2,2 kΩ → LED → IOx.

- R relè (“Relay”)

3.9 Accensione della centrale

Accendi l'alimentazione di rete. I LED della scheda mostrano quanto segue (la tabella completa è nel paragrafo 1.6):

- il LED **PWR** lampeggia in verde – la tensione di alimentazione è corretta;
- nella versione con modem il LED **NET** è acceso verde e ogni tanto lampeggia in giallo almeno tre volte – il verde indica che la scheda SIM si è registrata sulla rete mobile, il numero di lampeggi gialli (0–5) l'intensità del segnale;
- nella versione Wi-Fi il LED **MOD** lampeggia in verde mentre la centrale si connette alla rete Wi-Fi, e resta acceso verde fisso quando la connessione è stabilita.

L'intensità del segnale mobile adeguata è **3** (tre lampeggi gialli del LED NET). Se lampeggia meno, l'intensità del segnale di rete mobile non è sufficiente: scegli un'altra posizione per la centrale o per l'antenna, oppure usa un'antenna più sensibile. Se i LED mostrano altro, la causa si ricava dalla tabella del paragrafo 1.6. Se nessun LED della centrale è acceso, controlla l'alimentazione e i collegamenti.

4. Collegamento di espansioni e moduli radio

La maggior parte delle espansioni e dei moduli di comunicazione si collega al bus dati **RS485**. L'alimentazione del modulo è fornita dai morsetti **AUX+** (+12 V) e **AUX–**, i fili dati vanno sui morsetti **485 A** e **485 B**, sempre A → A, B → B. Sul bus si possono collegare al massimo **8 dispositivi**, la lunghezza del cavo del bus è al massimo **100 m**. Fa eccezione il ricevitore Paradox RTX3, che si collega al bus tastiere (GRN, YEL) (4.3). I moduli si impostano nella pagina **Modules** (6.5), i dispositivi radio si aggiungono nella pagina **Wireless** (6.6).

Il valore “al massimo 100 m” è un massimo teorico, in condizioni ideali – vedi la nota del paragrafo 1.3.

Tra i ricevitori radio, ogni versione firmware supporta solo il proprio; la tabella completa delle versioni e dei moduli supportati è nel paragrafo 1.7.

Modulo	Sistema radio	Firmware necessario (1.7)
RF-SH	Crow	SP3_xxx0, versione 1.01 o successiva (SP3_xxx0_0101)
RTX3	Paradox	SP3_xxx1, versione 1.12 o successiva (SP3_xxx1_0112)
RF-HW	Honeywell	SP3_xxx2, versione 1.14 o successiva (SP3_xxx2_0114)
RF-S8	S8	SP3_xxx4, versione 1.22 o successiva (SP3_xxx4_0122)
RF-LORA	dispositivi LoRa “Maximum”	per i dispositivi senza fili MAXIMUM SP3_xxx4, versione 1.21 o successiva (SP3_xxx4_0121); per le espansioni LORA qualsiasi versione
E485, T16, SF485, iO, iO-8, iO-WL, iO-MOD, espansioni LORA	–	qualsiasi versione

4.1 Modulo Ethernet E485

Con il modulo E485 la centrale invia e riceve le segnalazioni degli eventi e i comandi tramite Internet cablato. Se alla centrale è collegato un E485, le segnalazioni alla centrale di vigilanza e a Protegus 2 passano tramite Internet cablato e i dati mobili non vengono usati; se la connessione cablata si interrompe, la centrale passa ai dati mobili e, quando la connessione cablata viene ripristinata, torna automaticamente su di essa. La priorità dei canali (SIM, Wi-Fi, LAN – E485) si imposta nella pagina **Reporting to CMS** (6.3), le impostazioni dell'E485 nella pagina **Modules** (6.5). Con l'E485 la centrale non ha bisogno di una scheda SIM.

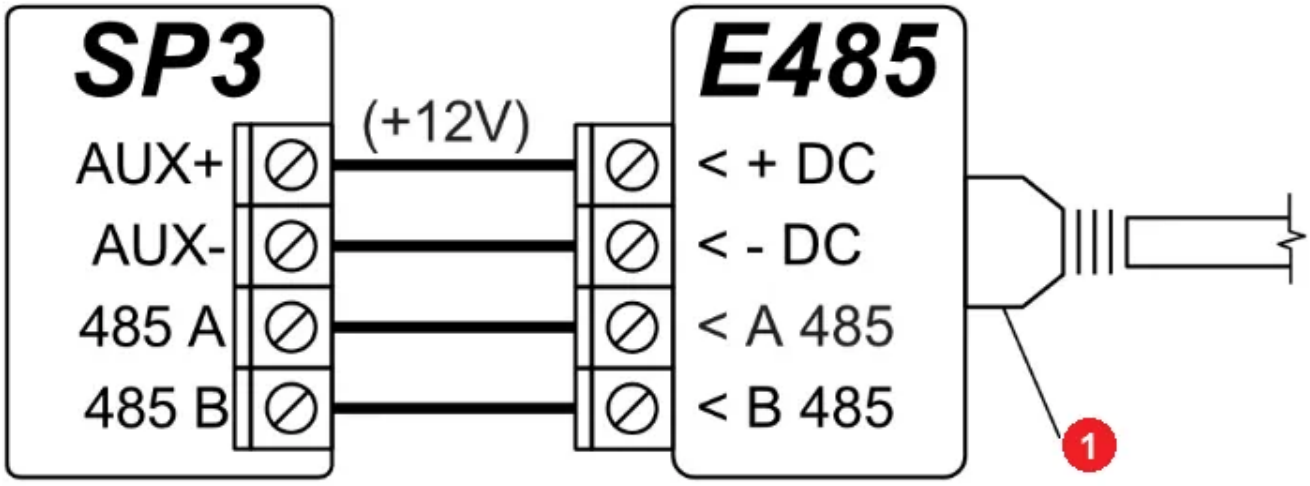


Figura 32. Modulo Ethernet E485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; nel connettore RJ45 dell'E485 il cavo LAN. Collegamento RS485 (“RS485 connection”), al massimo 100 m (“up to 100 m”).

- 1 cavo LAN (“LAN cable”)

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.

4.2 Ricevitore radio RF-SH (Crow)

Con il ricevitore RF-SH la centrale gestisce i dispositivi senza fili Crow: al massimo 32 rivelatori, 16 sirene, 42 telecomandi e 8 tastiere radio. Firmware necessario: SP3_xxx0_0101 o successivo (1.7).

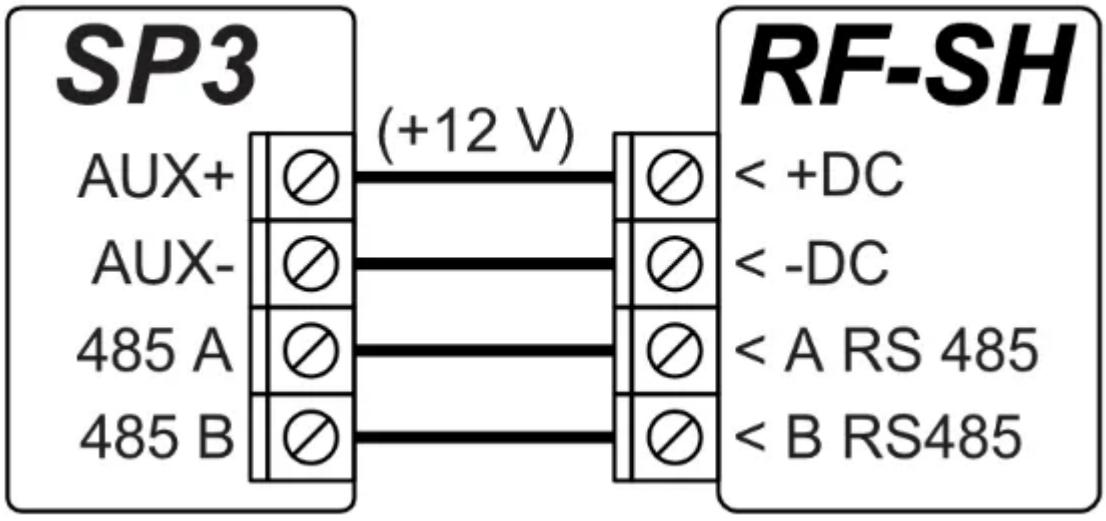


Figura 33. RF-SH: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

4.3 Ricevitore radio RTX3 (Paradox)

Il ricevitore RTX3 non si collega al bus RS485, ma al **bus tastiere**. Con esso la centrale gestisce i dispositivi senza fili Paradox: contatti magnetici, rivelatori di movimento, rivelatore di rottura vetri G550, rivelatore di fumo SD360, telecomandi REM2 e REM25, sirene SR230 e SR250, tastiera K37, espansione PGM e zone

2WPGM, ripetitore RPT1. Firmware necessario: SP3_xxx1_0112 o successivo (1.7). Il firmware dell'RTX3, il suo collegamento e l'aggiunta e la cancellazione dei dispositivi Paradox sono trattati in un articolo a parte: FLEXi SP3 e modulo di espansione senza fili Paradox RTX3.

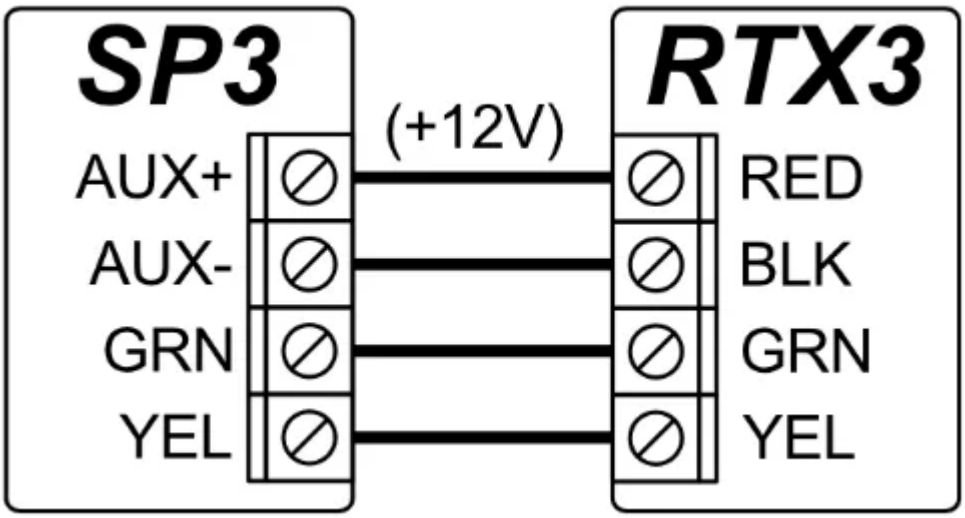


Figura 34. RTX3 sul bus tastiere: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL.

4.4 Ricevitore radio RF-HW (Honeywell)

Con il ricevitore RF-HW la centrale gestisce rivelatori, sirene, tastiere e telecomandi senza fili Honeywell. Firmware necessario: SP3_xxx2_0114 o successivo (1.7).

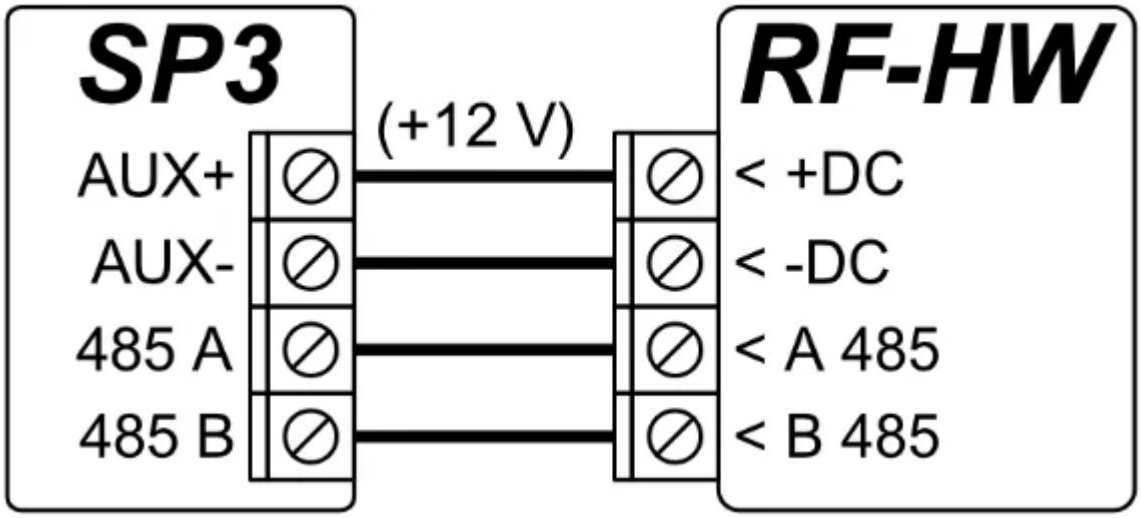


Figura 35. RF-HW: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.5 Ricevitore radio RF-S8

Con il ricevitore RF-S8 la centrale gestisce rivelatori, sirene e telecomandi senza fili S8. Firmware necessario: SP3_xxx4_0122 o successivo (1.7). La registrazione dell'RF-S8, la sostituzione del firmware e l'accoppiamento dei dispositivi S8 sono descritti in un manuale a parte: Manuale del ricetrasmettitore RF-S8 e dei rivelatori S8.

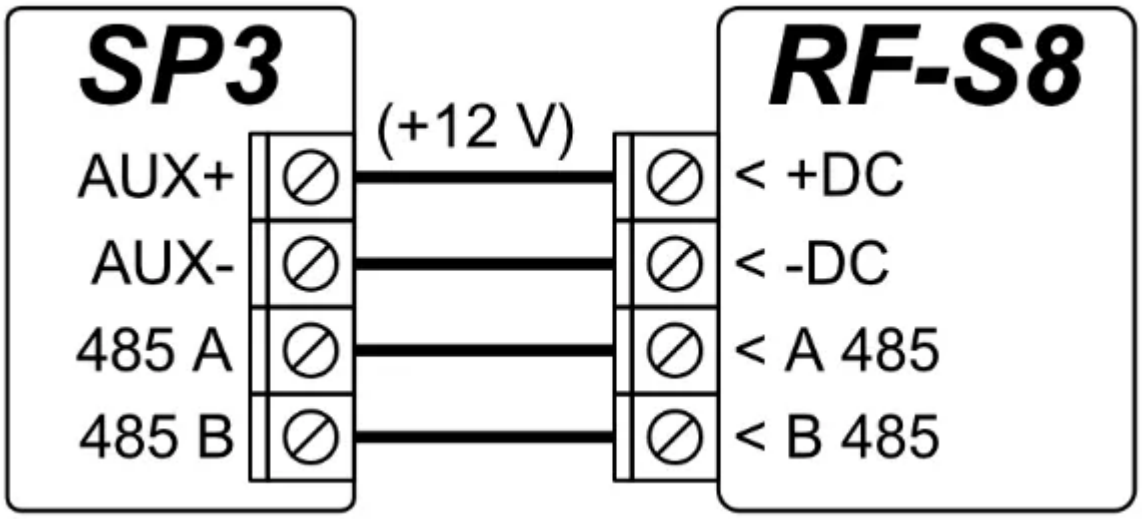


Figura 36. RF-S8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.6 Ricevitore radio RF-LORA

Con il ricevitore RF-LORA la centrale gestisce i dispositivi radio LoRa “Maximum”: al massimo 32 rivelatori, 16 sirene e 32 telecomandi, oltre alle espansioni LORA (4.7). Per i rivelatori, le sirene e i telecomandi MAXIMUM serve il firmware SP3_xxx4, versione 1.21 o successiva; le espansioni LORA funzionano con qualsiasi versione firmware (1.7). Il ricevitore si imposta nella pagina **Modules** (6.5), i dispositivi si aggiungono nella pagina **Wireless** (6.6).

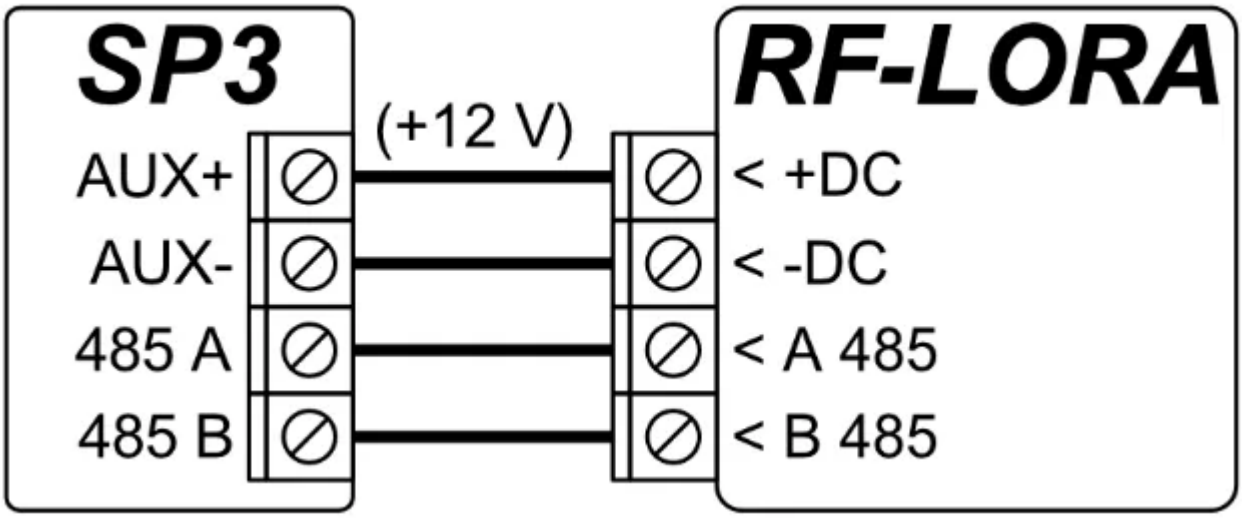


Figura 37. RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.7 Espansioni LORA

Le espansioni LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) si collegano alla centrale via radio tramite il ricevitore RF-LORA, da una distanza massima di 5000 m. **iO-LORA**: espansione di ingressi e uscite con collegamento per lettore iButton CZ-Dallas, alimentata a 12 V DC; il lettore Wiegand collegato a essa non funziona con l'SP3. **iO8-LORA**: espansione a otto ingressi/uscite, alimentata a 12–26 V, con tutti i tipi di circuito della centrale (3.2). **PB-LORA**: pulsante antipanico. **REL-LORA**: modulo relè, alimentato a 100–230 V AC.

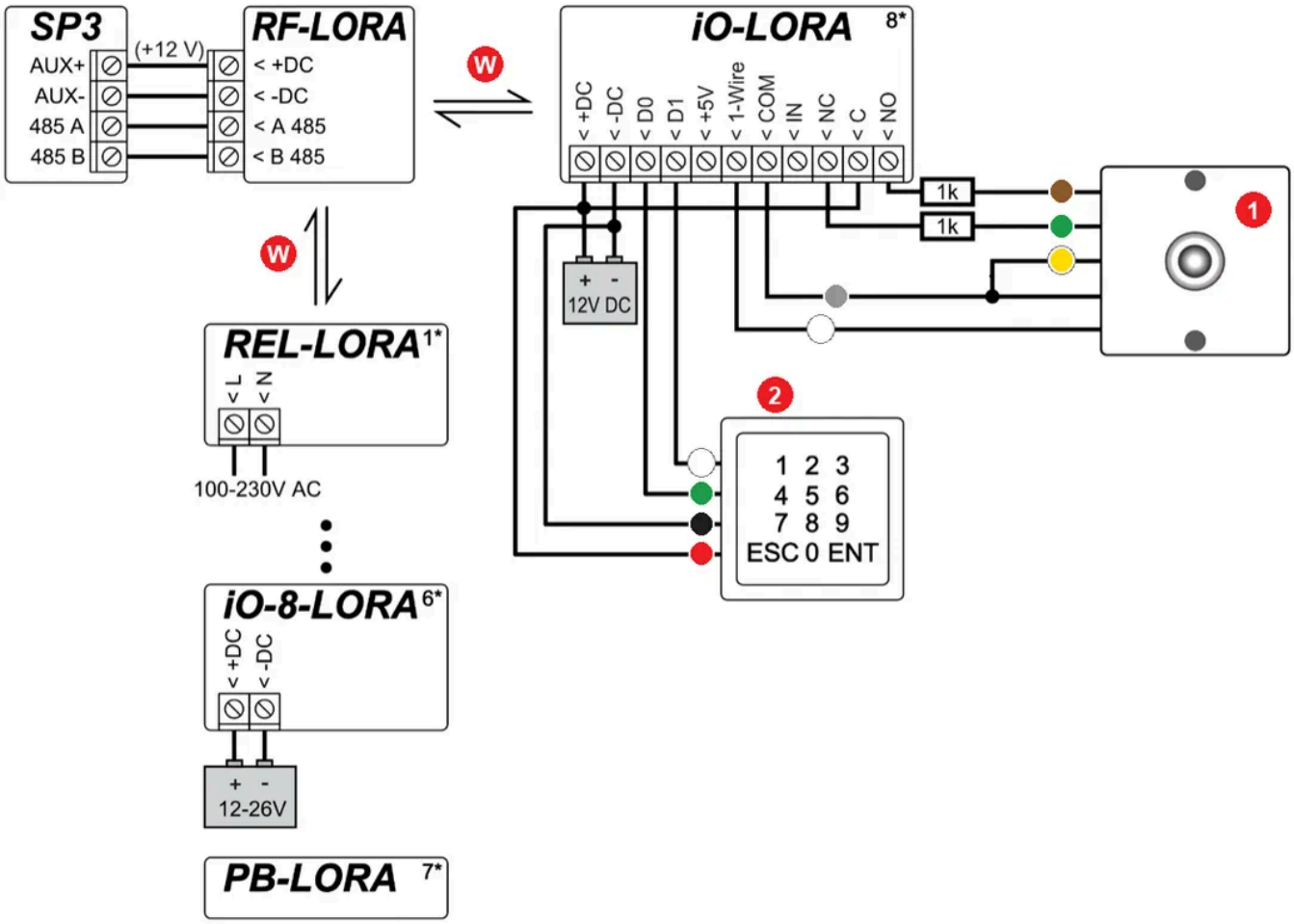


Figura 38. Espansioni LORA tramite il ricevitore RF-LORA. SP3 → RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; l'RF-LORA raggiunge via radio, da al massimo 5000 m, le unità iO-LORA, iO8-LORA, PB-LORA e REL-LORA. REL-LORA: L, N → 100–230 V AC. iO8-LORA: +DC, −DC → 12–26 V. iO-LORA: +DC, −DC → 12 V DC; filo rosso del lettore d'ingresso (+U) → +DC, nero (GND) → −DC, verde (D0) → D0, bianco (D1) → D1; il collegamento 1-Wire del lettore CZ-Dallas al massimo 30 m ("1-Wire connection up to 30 m"): 1-Wire → bianco, COM → grigio e giallo (LED−), C → +DC, NO → 1 kΩ → marrone (RED LED+), NC → 1 kΩ → verde (Green LED+). L'uscita xOUT va impostata sul tipo **System State** (stato del sistema) ("The output xOUT must be set to the »System State« type.") – con allarme inserito la luce del lettore iButton è rossa ("Security alarm is on - the iButton reader light is red."), con allarme disinserito verde ("The security alarm is off - the iButton reader light is green.").

- 1 lettore iButton CZ-Dallas ("CZ-Dallas reader")
- 2 lettore d'ingresso: lettore RFID con tastiera, Wiegand 26/34 ("Entry reader", "RFID reader with keypad (Wiegand 26/34)") – con la FLEXi SP3 così non funziona
- W collegamento senza fili ("Wireless connection"), al massimo 5000 m ("up to 5000 m")
- filo marrone, RED LED+ ("Brown wire", "RED LED+") – la luce rossa
- filo verde: sul lettore CZ-Dallas Green LED+, la luce verde ("Green wire", "Green LED+"); sul lettore d'ingresso D0 ("G - green wire (D0)")
- filo giallo, LED− ("Yellow wire", "LED-")
- filo grigio ("Gray wire")
- filo bianco ("White wire"); sul lettore d'ingresso D1 ("W - white wire (D1)")
- filo rosso, +U ("R - red wire (+U)")
- filo nero, GND ("B - black wire (GND)")

Il lettore d'ingresso (2) collegato all'iO-LORA nel disegno non funziona con la FLEXi SP3. Collega il lettore RFID direttamente alla centrale (3.5).

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.

4.8 Espansioni della serie iO

Se alla centrale servono più ingressi (IN) o uscite (OUT), collega un'espansione Trikdis della serie iO cablata o senza fili (iO, iO-8, iO-WL, iO-MOD). **iO**: espansione di ingressi/uscite con collegamento 1-Wire. **iO-8**: espansione a otto ingressi/uscite, con tutti i tipi di circuito della centrale (3.2). **iO-WL**: espansione senza fili che si collega alla centrale tramite il ricetrasmettitore **iO-MOD**, da una distanza massima di 300 m; si può collegare anche via cavo al bus RS485. Nel sistema possono esserci al massimo 8 moduli di espansione e al massimo 4 iO-MOD. Le espansioni si impostano nella pagina **Modules** (6.5).

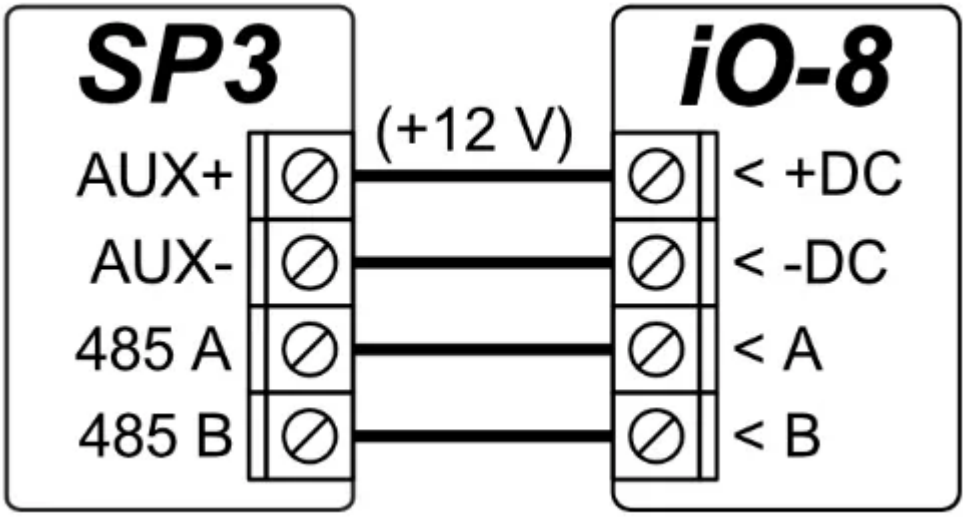


Figura 39. iO-8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A, 485 B → B.

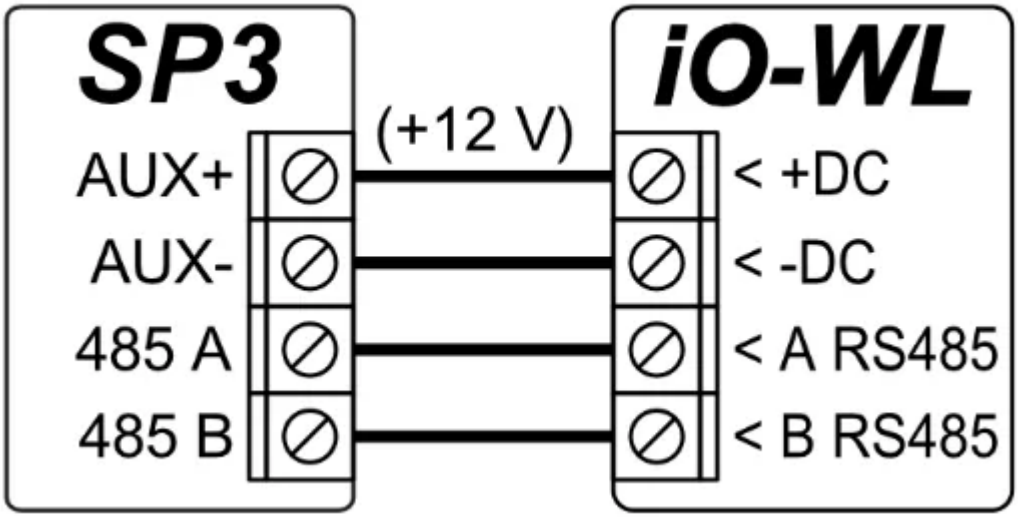


Figura 40. iO-WL via cavo: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

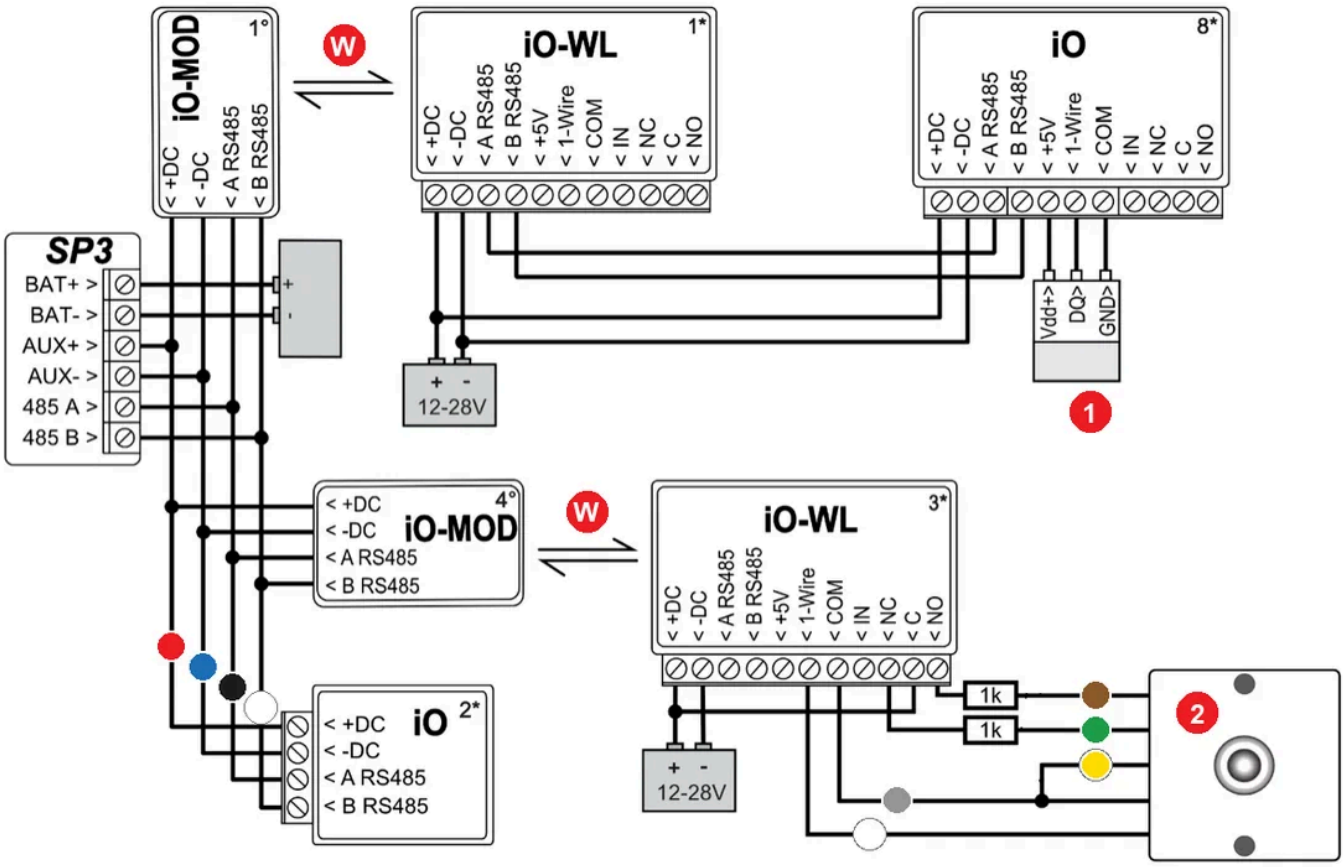


Figura 41. Panoramica del sistema iO. SP3: BAT+ / BAT− → batteria da 12 V (“Battery 12V”); AUX+ (rosso) e AUX− (blu) → +DC e −DC sulle unità iO-MOD e iO; 485 A (nero) e 485 B (bianco) → A RS485 e B RS485. I due iO-MOD raggiungono via radio, da al massimo 300 m, un'unità iO-WL ciascuno. L'iO-WL e l'iO in alto sono alimentati da un'alimentazione comune a 12–28 V, tra loro un collegamento RS485 (“RS485 connection”), al massimo 300 m (“up to 300 m”); i morsetti +5V, 1-Wire e COM dell'iO → Vdd+, DQ e GND di un sensore di temperatura DS18B20 / DS18S20. L'iO-WL in basso (12–28 V) gestisce un lettore CZ-Dallas, il collegamento 1-Wire al massimo 30 m (“1-Wire connection up to 30 m”): 1-Wire → bianco, COM → grigio e giallo (LED−), C → +DC, NO → 1 kΩ → marrone (RED LED+), NC → 1 kΩ → verde (Green LED+). L'uscita xOUT va impostata sul tipo **System State** (stato del sistema) (“The output xOUT must be set to the »System State« type.”) – con allarme inserito la luce del lettore iButton è rossa (“Security alarm is on - the iButton reader light is red.”), con allarme disinserito verde (“The security alarm is off - the iButton reader light is green.”). Delle unità contrassegnate con l'asterisco possono esserci al massimo 8 moduli di espansione del sistema (“* up to 8 system expansion modules”), di quelle contrassegnate con ° al massimo 4 moduli iO-MOD (“° up to 4 iO-MOD modules”).

- 1 sensore di temperatura, DS18B20 o DS18S20 (“Temperature sensor: DS18B20 or DS18S20”)
- 2 lettore iButton CZ-Dallas (“CZ-Dallas reader”)
- W collegamento senza fili (“Wireless connection”), al massimo 300 m (“up to 300 m”)
- filo rosso (“Red wire”)
- filo blu (“Blue wire”)
- filo nero (“Black wire”)
- filo bianco (“White wire”)
- filo marrone, RED LED+ (“Brown wire”, “RED LED+”) – la luce rossa
- filo verde, Green LED+ (“Green wire”, “Green LED+”) – la luce verde
- filo giallo, LED− (“Yellow wire”, “LED-”)
- filo grigio (“Gray wire”)

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.

4.9 Trasmettitore radio T16

Il trasmettitore radio VHF/UHF T16 inoltra gli eventi della centrale alla centrale di vigilanza tramite la rete radio Trikdis: invia sia i propri eventi sia quelli ricevuti dalla centrale, e la centrale di vigilanza può inoltrarli all'utente.

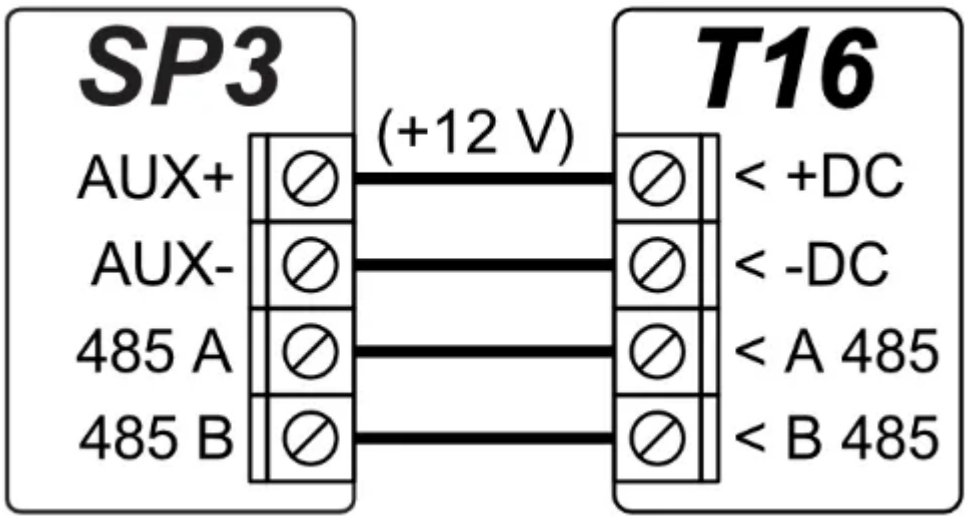


Figura 42. T16: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.10 Modulo Sigfox SF485

L'SF485 è un canale di riserva: se il canale primario viene a mancare, invia gli eventi della centrale tramite la rete Sigfox alla centrale di vigilanza o all'app Protegus 2, in formato Contact ID.

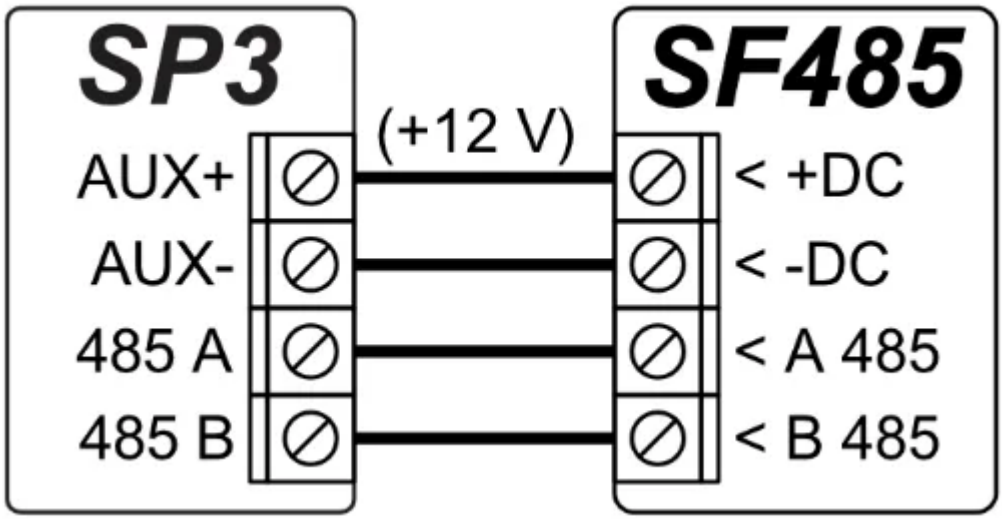


Figura 43. SF485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.11 Misura della tensione continua

La centrale può misurare una tensione continua di 0–30 V; **sopra 30 V la scheda si danneggia**. Il polo positivo della tensione misurata va su IO1 (nel disegno di fabbrica IN1), il negativo sul morsetto C.

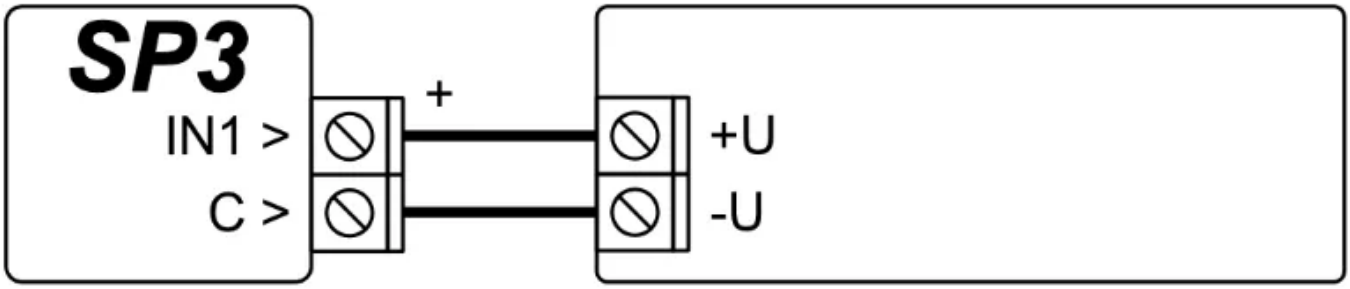


Figura 44. Misura della tensione: l'apparecchiatura misurata (“Equipment whose voltage is measured”) +U → IO1 (nel disegno IN1), −U → C.

Collega la centrale al computer con il cavo USB e avvia TrikdisConfig (capitolo 6); il programma riconosce automaticamente la centrale collegata e apre la sua finestra di configurazione. Nella pagina **Sensors** imposta il sensore **In1 Voltage** e i valori limite:

- **Max** – sopra questa tensione viene generato un evento, se la casella **High** è spuntata;
- **Min** – sotto questa tensione viene generato un evento, se la casella **Low** è spuntata.

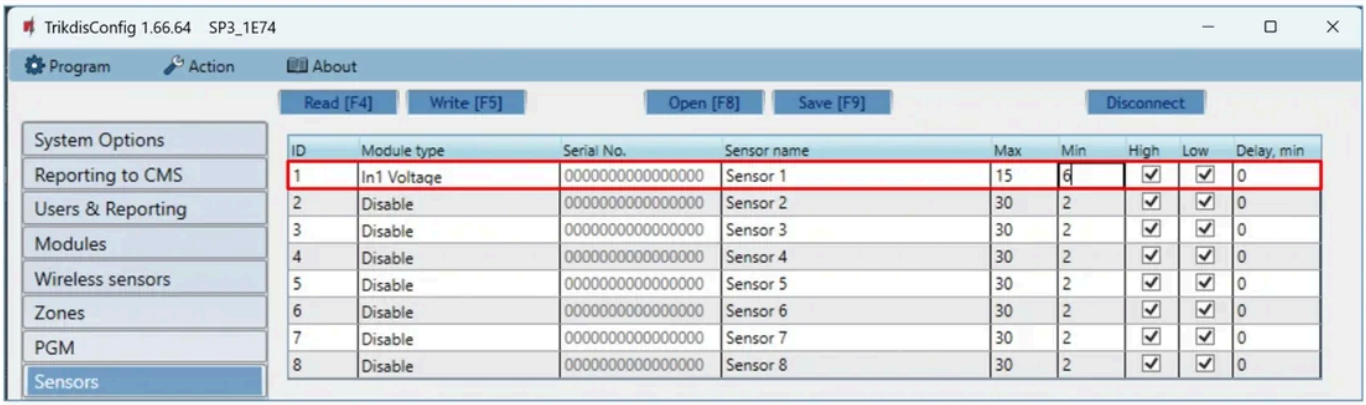


Figura 45. La pagina Sensors: il sensore In1 Voltage con identificativo 1, Max 15, Min 6, High e Low spuntati, Delay 0 minuti.

La tensione misurata può anche comandare un'uscita PGM. Nella scheda **Outputs** della pagina **PGM** imposta l'uscita in modalità **Remote Control**, poi nella scheda **Set Action** definisci la condizione:

- **Enable** – abilitazione della PGM;
- **PGM No.** – l'uscita PGM comandata;
- **Action** – il funzionamento dell'uscita: **PGM OFF** (spegne), **PGM ON** (accende), **Pulse OFF** (al comando si spegne per la durata dell'impulso, poi si riaccende), **Pulse ON** (si accende per la durata dell'impulso, poi si spegne);
- **Pulse time, s** – la durata dell'impulso, 0–9999 s;
- **Factor** – l'origine della condizione: **Sensor**;
- **Factor No.** – l'ingresso di misura della tensione (S1);
- **Start when** – la condizione: **Higher than set** (sopra il valore impostato) o **Lower than set** (sotto);
- **Set value** – la tensione controllata (V).

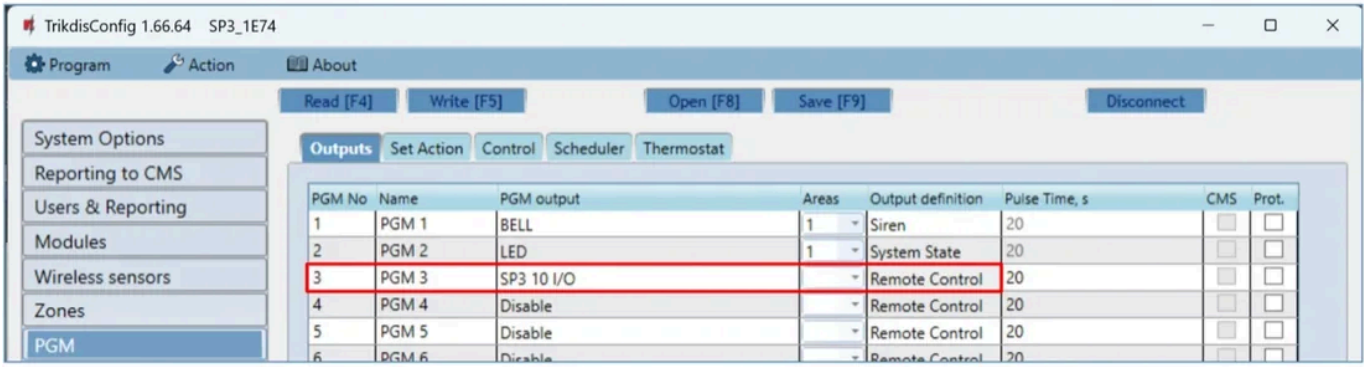


Figura 46. La scheda Outputs della pagina PGM: la PGM 3 sul morsetto I/O 10 dell'SP3, di tipo Remote Control, con durata dell'impulso di 20 s.

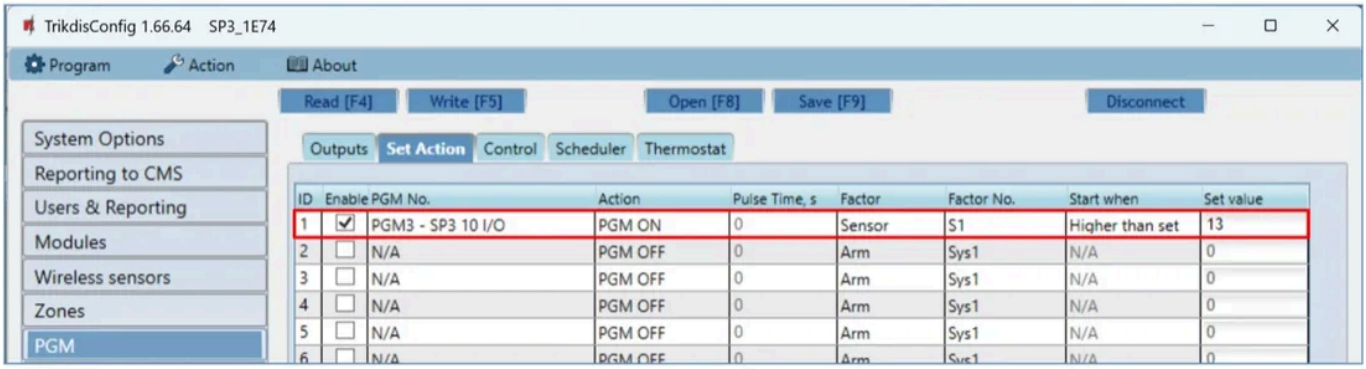


Figura 47. La scheda Set Action: Enable spuntato, PGM No. PGM3, Action PGM ON, Pulse Time 0, Factor Sensor, Factor No. S1, Start when Higher than set, Set value 13 V.

5. Protegus 2 e controllo a distanza

Puoi controllare a distanza la "FLEXi" SP3 in tre modi: dall'app Protegus 2, via SMS e con una chiamata telefonica. L'app funziona su tutte le versioni che raggiungono Internet (WiFi, Ethernet o rete mobile). I comandi SMS e il controllo tramite chiamata sono disponibili solo nelle versioni con modem di rete mobile (ad esempio SP3_24E, SP3_44E, SP3_12E) e solo con una scheda SIM funzionante. Nella versione SP3_3E (WiFi + Ethernet) non c'è il modem.

5.1 Collegamento all'account Protegus 2

In Protegus 2 l'utente inserisce e disinserisce il sistema, vede lo stato delle zone e delle aree e riceve notifiche sugli eventi. Prima di aggiungere la centrale all'account, verifica quanto segue:

- **Tensione di alimentazione** – il LED **POWER** è acceso verde fisso.
- **Rete** – il LED **NET** è verde fisso (rete mobile) e/o il LED **MOD** è verde fisso (modulo WiFi o Ethernet). Il significato dei LED è descritto nel paragrafo 1.6.
- **Scheda SIM** – nella versione con modem la SIM è attiva e hai inserito il codice PIN in TrikdisConfig (**System Options** → **SIM** → **PIN**), oppure hai disattivato la richiesta del PIN sulla scheda.
- **Servizio cloud** – nella scheda **Users & Reporting** → **Protegus** di TrikdisConfig è spuntato **Enable cloud service** (6.4). Il valore di fabbrica del **Cloud access code** è 123456; se lo modifichi, l'app chiederà il nuovo codice quando aggiungi il sistema.
- **Identificativo univoco** – il numero **IMEI/Unique ID** della centrale si trova sull'etichetta della confezione e della scheda, e si vede anche nell'angolo in basso a sinistra di TrikdisConfig, dopo aver letto la centrale.

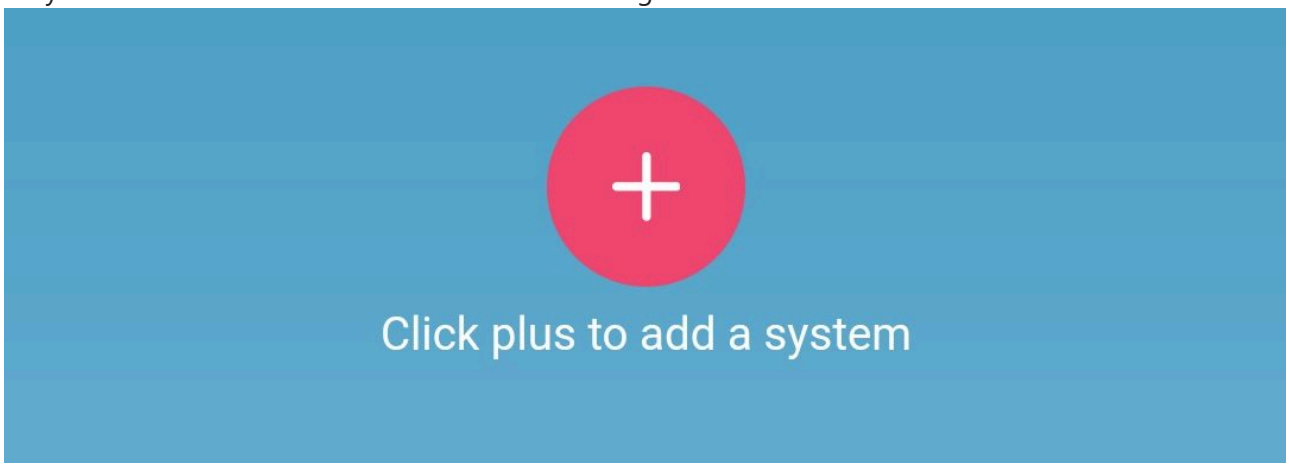
Se non hai ancora un account Protegus, crealo sul sito www.protegus.app con il link **Sign up** e attivalo facendo clic sul link ricevuto via e-mail; poi installa l'app Protegus 2 sul telefono e accedi con il tuo nome utente e la tua password.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



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

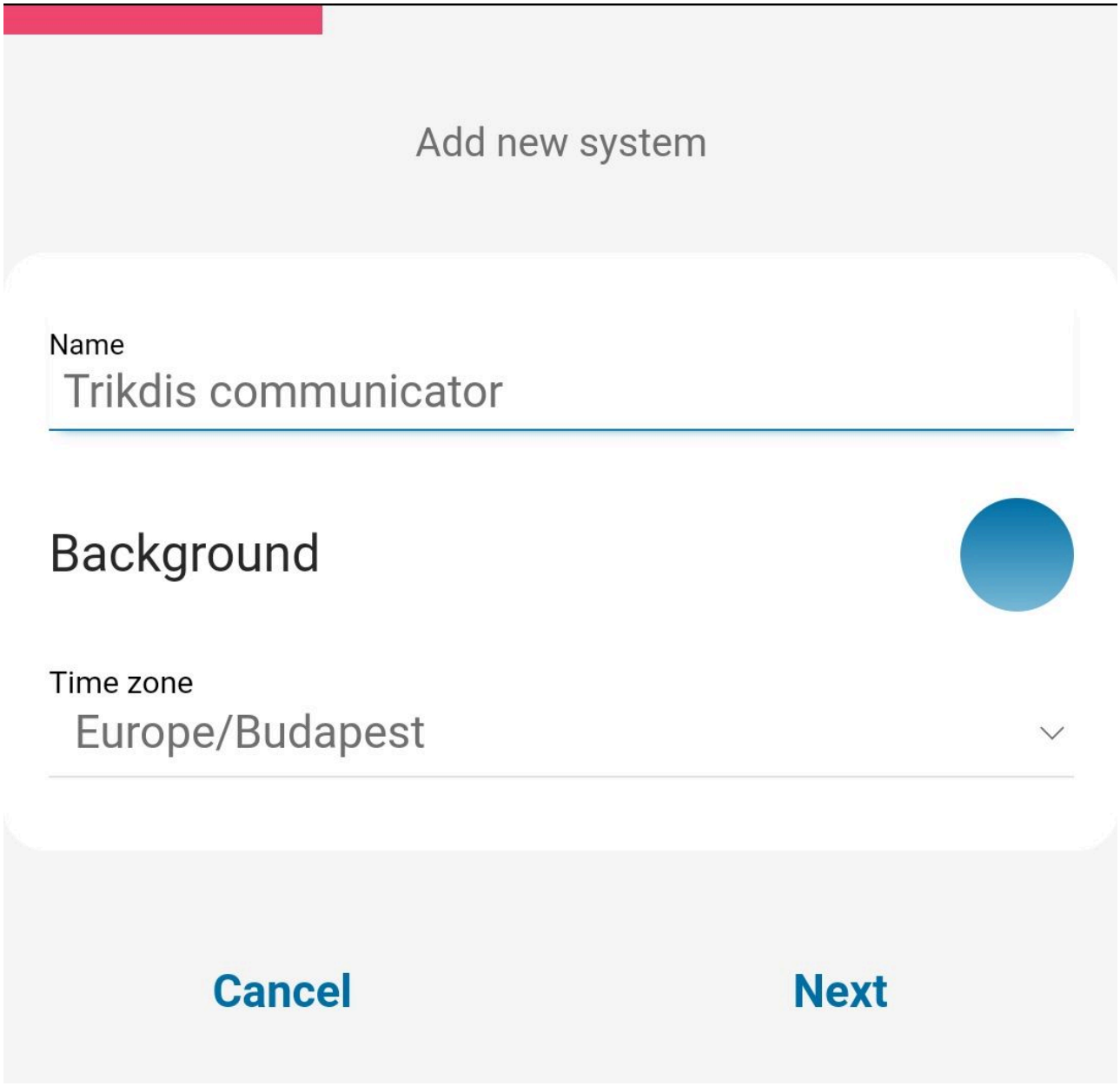


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

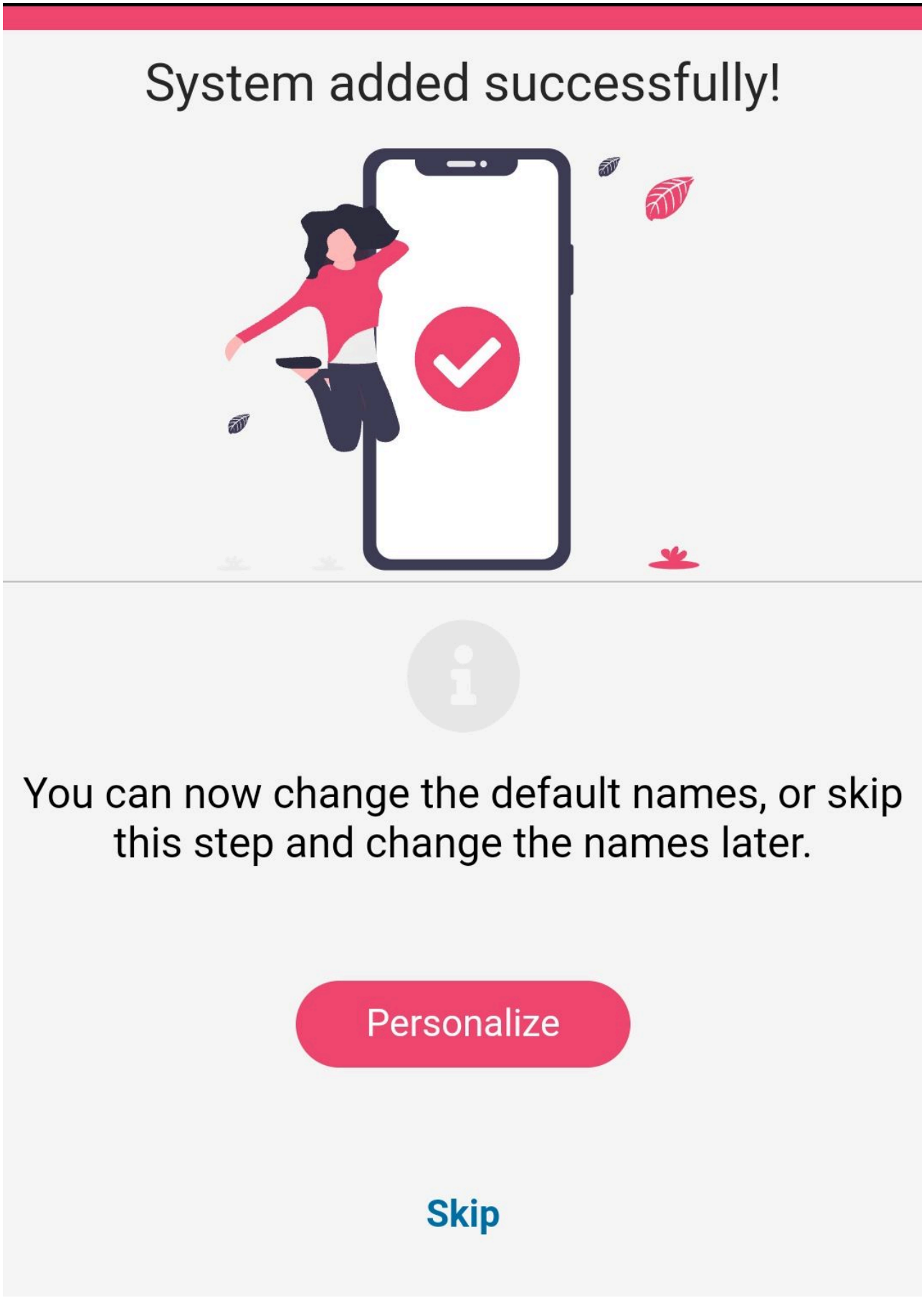
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



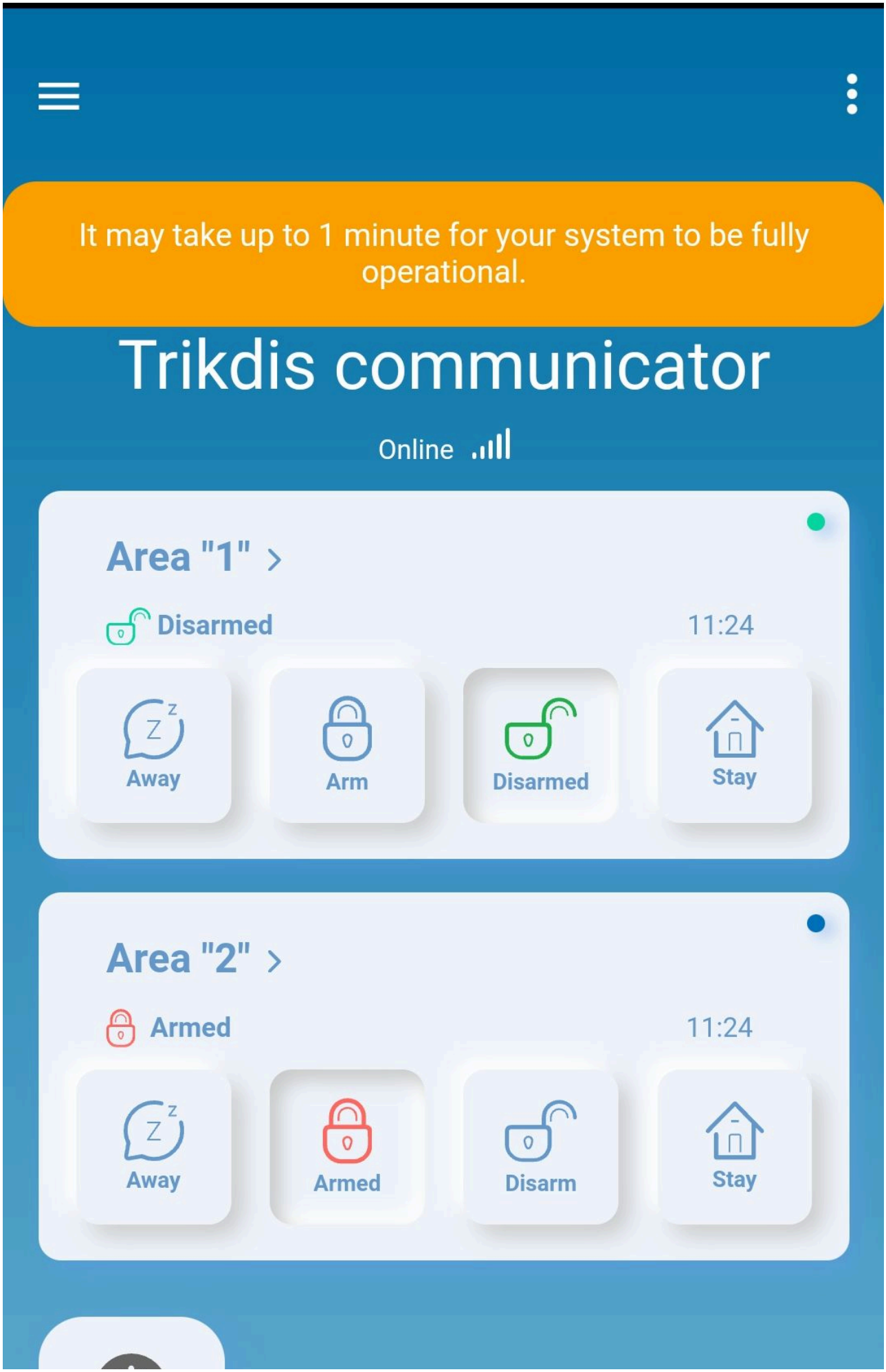
6. Add meg a rendszer nevét és válassz idozónát



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



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


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

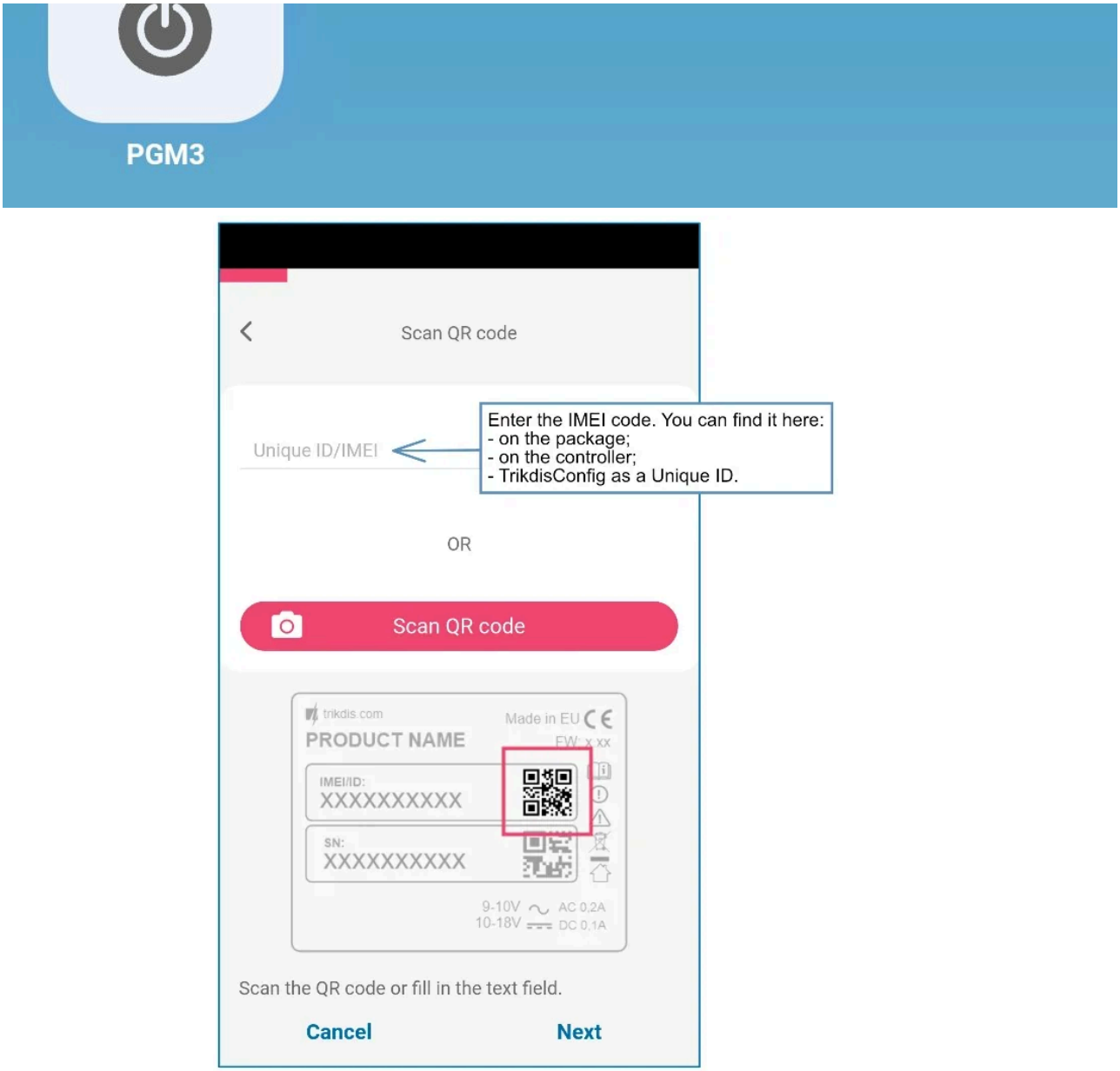


Figura 48. Aggiunta del sistema in Protegus 2: inserisci il numero **IMEI/Unique ID** oppure leggi con la fotocamera il codice QR dell'etichetta.

Altri utenti

Il proprietario può invitare altri utenti in Protegus 2. Il sistema invia un invito anche agli indirizzi scritti nella colonna **Email** della scheda **Users & Reporting** → **Users** di TrikdisConfig, così l'utente vede il sistema dal proprio account (6.4).

5.2 Inserimento e disinserimento nell'app

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

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

Con l'SP3, dopo aver toccato il lucchetto devi inserire il **codice utente** della centrale. È il codice indicato nella colonna **Code** della scheda **Users & Reporting** → **Users** di TrikdisConfig, non la password dell'account Protegus 2. Ogni area compare su una scheda separata, e vedi solo le aree per cui l'utente è abilitato nella colonna **Areas**. Oltre all'inserimento totale, dall'app avvii anche le modalità parziali: **Stay** (resti in casa, le zone interne non si inseriscono) e **Sleep** (modalità notte). In quale modalità una zona sorveglia lo stabilisce il campo **Definition** della zona (6.7).

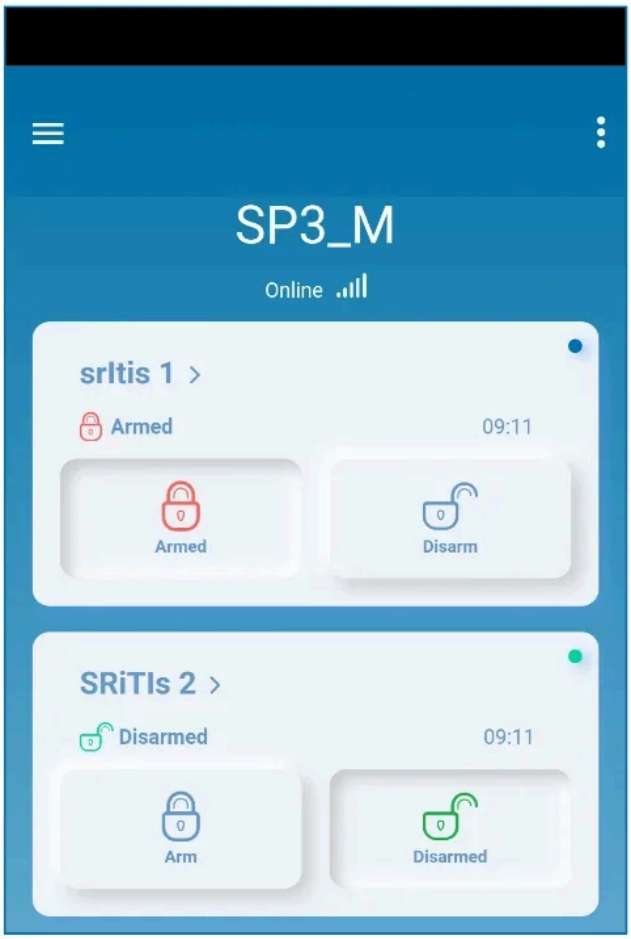


Figura 49. Due aree in Protegus 2: la 1ª inserita (lucchetto rosso, chiuso), la 2ª disinserita (lucchetto verde, aperto).

Se l'app non segue la centrale

Se ai comandi non succede nulla, o l'app mostra tutt'altro rispetto allo stato reale della centrale, apri in Protegus 2 il menu **Settings** → **System configuration** e alla riga **System out of sync?** premi il pulsante **Sync**. L'app rilegge le impostazioni della centrale.

5.3 Configurazione e controllo via SMS

Solo nelle versioni con modem. L'SMS si invia al numero della scheda SIM della centrale. Ogni messaggio ha la stessa struttura:

Comando spazio **Password** spazio **Dati**

La password è la **SMS password** a sei cifre (**System Options** → **Access**, 6.2). Il valore di fabbrica è **123456**. Per motivi di sicurezza, alla messa in servizio cambiala con una password nota solo a te, in TrikdisConfig o con il comando `PSW` – e non dimenticarla –, e non diffondere inutilmente il numero della scheda SIM della centrale. Il campo dati dipende dal comando; per diversi comandi è vuoto.

Chi può inviare comandi?

L'amministratore può controllare la centrale via SMS e con una chiamata. Se vuoi abilitare anche altri utenti, aggiungi il loro numero di telefono nella scheda **Users & Reporting** → **Users** di TrikdisConfig (6.4) o con il comando `SETN`. La centrale invia le risposte con i testi impostati nella scheda **SMS answer texts**.

Comando	Dati	Che cosa fa	Esempio
INFO	–	Richiesta dello stato: nome dell'impianto, stato delle aree, IMEI, intensità del segnale, versione firmware, numero di serie.	`INFO 123456`
RESET	–	Riavvio della centrale.	`RESET 123456`
OUTPUTx	ON	Attivazione dell'uscita x.	`OUTPUT1 123456 ON`
	OFF	Disattivazione dell'uscita x.	`OUTPUT1 123456 OFF`
	PULSE=ttt	Attivazione dell'uscita x per ttt secondi (tre cifre).	`OUTPUT1 123456 PULSE=002`
PSW	nuova password	Cambio della password SMS.	`PSW 123456 654123`
TIME	AAAA/MM/GG,hh:mm:ss	Impostazione di data e ora.	`TIME 123456 2026/10/30,10:02:00`
TXTA	nome dell'impianto	Impostazione del nome dell'impianto (compare nei rapporti).	`TXTA 123456 Casa`
RDR	numero di telefono#testo	La centrale inoltra via SMS al numero indicato il testo che segue il #. Il numero inizia con il segno + e il prefisso internazionale.	`RDR 123456 +393401234567#testo inoltrato`
ASKI	–	Stato degli ingressi (IN) via SMS.	`ASKI 123456`
ASKO	–	Stato delle uscite (OUT) via SMS.	`ASKO 123456`
ASKA	–	Stato delle aree via SMS.	`ASKA 123456`
ASKT	–	Valori di tutti i sensori di temperatura via SMS.	`ASKT 123456`
ARM	SYS:x	Inserimento dell'area x (1–8).	`ARM 123456 SYS:1`

Comando	Dati	Che cosa fa	Esempio
DISARM	SYS:x	Disinserimento dell'area x (1–8).	`DISARM 123456 SYS:1`
STAY	SYS:x	Inserimento dell'area x in modalità Stay (1–8).	`STAY 123456 SYS:1`
SLEEP	SYS:x	Inserimento dell'area x in modalità Sleep (1–8).	`SLEEP 123456 SYS:1`
FRS	–	Ripristino dell'alimentazione dei rivelatori d'incendio, se un'uscita è definita come **Fire Sensor Reset**.	`FRS 123456`
SETN	PhoneX=numero#nome#e-mail	Aggiunta di un utente alla riga x con numero di telefono, nome e indirizzo e-mail; il numero di telefono e il nome sono separati dal segno #. Il numero inizia con il segno + e il prefisso internazionale.	`SETN 123456 PHONE5=+393401234567#MARIO#mario@esempio.it`
	PhoneX=DEL	Cancellazione del numero di telefono e del nome della riga x.	`SETN 123456 PHONE5=DEL`
UUSD	*codice#	Invio di un codice USSD all'operatore mobile (ad esempio verifica del credito). Il nome del comando nella centrale è proprio così, UUSD.	`UUSD 123456 *245#`
CONNECT	Protegus=ON	Connessione al cloud Protegus.	`CONNECT 123456 PROTEGUS=ON`
	Protegus=OFF	Interruzione della connessione a Protegus.	`CONNECT 123456 PROTEGUS=OFF`
	Code=123456	Il codice di accesso al cloud Protegus (**Cloud access code**).	`CONNECT 123456 CODE=123456`
	IP=indirizzo:porta	Indirizzo IP e porta del canale principale verso la centrale di vigilanza.	`CONNECT 123456 IP=0.0.0.0:8000`
	IP=0	Disattivazione del canale principale.	`CONNECT 123456 IP=0`

Comando	Dati	Che cosa fa	Esempio
	ENC=123456	Chiave di crittografia TRK.	`CONNECT 123456 ENC=123456`
	APN=nome	Il nome APN della scheda SIM.	`CONNECT 123456 APN=INTERNET`
	USER=nome	Nome utente APN.	`CONNECT 123456 USER=User`
	PSW=password	Password APN.	`CONNECT 123456 PSW=Password`

Prima verifica

Il comando `INFO` è il modo più rapido per vedere sul posto che la SIM è attiva, che la centrale accetta comandi e qual è l'intensità del segnale. La risposta arriva entro pochi secondi.

5.4 Controllo con chiamata telefonica

Non su tutte le versioni

Il controllo tramite chiamata non funziona sulle centrali **SP3_xx7x**. Il tipo **SP3_12xx** con firmware 1.14 o successivo non riproduce messaggi vocali, ma i comandi da tastiera funzionano comunque.

Condizioni:

1. Il numero di telefono del chiamante è presente nella scheda **Users & Reporting** → **Users** e per l'utente è spuntata la colonna **PGM** (comando delle uscite dal telefono), oppure il sistema è diviso in almeno un'area e l'utente è abilitato per essa.
2. Il campo **Output definition** dell'uscita da comandare è **Remote control** (6.8). Per il comando a impulso è compilato anche il **Pulse time**.

Chiama il numero della scheda SIM della centrale. La centrale risponde alla chiamata, dopodiché digita il comando sulla tastiera del telefono:

Tasti	Funzione	Esempio
[1][area][#]	Inserimento dell'area indicata.	`12#` – inserimento dell'area 2
[2][area][#]	Disinserimento dell'area indicata.	`22#` – disinserimento dell'area 2
[3][uscita][#][stato]	Controllo dell'uscita indicata. Stato: 0 – disattiva, 1 – attiva, 2 – disattiva per la durata dell'impulso, 3 – attiva per la durata dell'impulso.	`31#1` – attivazione dell'uscita 1; `32#3` – attivazione dell'uscita 2 per la durata dell'impulso

Solo sulle vecchie centrali SP3_12xx (firmware fino alla 1.13), per i messaggi vocali:

Tasti	Funzione	Esempio
[4][#][numero della registrazione][#]	Avvio della registrazione di un messaggio vocale (1–5).	`4#1#`
[5]	Riascolto del messaggio appena registrato.	`5`
[6]	Salvataggio della registrazione.	`6`

Registrazione dei messaggi vocali

L'inizio e la fine della registrazione sono segnalati da un segnale acustico. Un messaggio dura al massimo 15 secondi. Anche la fine del riascolto è segnalata da un segnale acustico, e l'operazione successiva va avviata solo dopo il segnale acustico. La centrale riproduce il messaggio registrato all'utente chiamato in caso di allarme: quale messaggio appartiene a quale zona lo stabilisce il campo **Sound** della zona (6.7). La chiamata vocale c'è solo nella versione SP3_12xx, con firmware fino alla 1.13.

6. TrikdisConfig – le impostazioni in dettaglio

TrikdisConfig è il programma di configurazione gratuito di Trikdis, che funziona su Windows. Con esso leggi e scrivi tutte le impostazioni della centrale: sul posto via USB, oppure a distanza tramite il cloud Protegus. Il programma si scarica dal sito trikdis.com (nel campo di ricerca scrivi: TrikdisConfig).

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

Connessione via USB

1. Installa e avvia TrikdisConfig.
2. Collega la centrale al computer con un cavo USB Mini-B. Il programma riconosce la centrale e apre la finestra di configurazione dell'SP3.
3. Premi il pulsante **Read [F4]**. Se il programma chiede un codice, inserisci il codice amministratore o installatore (6.2.6). Con il codice amministratore di fabbrica non lo chiede.
4. Imposta ciò che serve, poi premi il pulsante **Write [F5]**. Solo così l'impostazione viene scritta nella centrale.

Modalità di programmazione

Se colleghi il cavo USB a una centrale alimentata e in funzione, la centrale passa in modalità di programmazione e, finché il cavo non viene scollegato, non svolge funzioni d'allarme. Su un impianto in servizio avvisa l'utente e alla fine scollega il cavo.

I pulsanti della riga superiore: **Read [F4]** – lettura dalla centrale; **Write [F5]** – scrittura nella centrale; **Open [F8]** – apertura di un'impostazione salvata in precedenza su file; **Save [F9]** – salvataggio su file dell'impostazione attuale; **Disconnect** – chiusura della connessione. Le finestre del menu a sinistra: **System Options**, **Reporting to CMS**, **Users & Reporting**, **Modules**, **Wireless sensors**, **Zones**, **PGM**, **Sensors**, **System events**, **Events Log** e **Firmware** (aggiornamento del firmware, capitolo 9). Nell'angolo in basso a sinistra si vedono le caselle **Remember password** e **Show passwords**, il pulsante **Default settings** → **Restore** (6.12) e il numero **IMEI/Unique ID** della centrale.

Salva su file

Il file salvato con il pulsante **Save [F9]** è la documentazione del sistema. Dopo la sostituzione della scheda o un ripristino di fabbrica, con **Open [F8]** e poi **Write [F5]** ricarichi tutto in pochi minuti.

Puoi configurare la centrale anche a distanza: nella schermata iniziale di TrikdisConfig scrivi nel campo **Remote access** il numero **IMEI/Unique ID** della centrale e premi il pulsante **Configure** (figura nel paragrafo 6.6.2, procedura completa nel capitolo 7). Ciò richiede il servizio cloud attivato (6.4.3) e una connessione di rete funzionante.

6.1 La barra di stato

Con la centrale collegata, la riga inferiore del programma e il campo in basso a sinistra mostrano i dati del dispositivo.

Campo	Significato
IMEI/Unique ID	L'identificativo univoco della centrale. Nella versione con modem è l'IMEI, nella versione WiFi/Ethernet un identificativo hardware. Lo chiedono Protegus 2 e anche il **Remote access**.
Status	Lo stato dell'operazione (ad esempio "reading done").
Device	Il tipo di centrale, nella forma SP3_xxxx.
SN	Il numero di serie della centrale.
BL	La versione del bootloader.
FW	La versione del firmware.
HW	La versione dell'hardware.
State	Il tipo di connessione: **USB** o remota.
Role	Il livello di accesso dopo l'inserimento del codice: **Administrator** o **Installer**.



Figura 50. La barra di stato di TrikdisConfig. I valori di **IMEI/Unique ID** e **SN** sono nascosti nella figura.

Il pulsante **Read [F4]** legge e visualizza le impostazioni memorizzate nella centrale. Di seguito esaminiamo i campi finestra per finestra.

6.2 System Options

È composta da sei schede: **System general**, **Partitions**, **Scheduler**, **Holidays**, **System troubles** e **Access**.

6.2.1 Scheda System general

Gruppo **General**:

- **Object ID** – identificativo dell'impianto, numero esadecimale a quattro cifre (0–9, A–F). Lo assegna la centrale di vigilanza (CMS); serve solo se la centrale trasmette a una centrale di vigilanza. FFFE e FFFF non si possono usare.
- **Object name** – il nome dell'impianto, al massimo 20 lettere e cifre. Compare nelle segnalazioni SMS.
- **Test period** – se lo spunti, la centrale invia una segnalazione di test a questo intervallo, a meno che sia spuntato anche **Start test at** e tu abbia indicato un orario.
- **Start test at** – l'orario giornaliero della segnalazione di test.
- **Areas in test SMS** – l'SMS di test contiene anche lo stato delle aree indicate.
- **Clear Events after reset** – al riavvio gli eventi non ancora inviati vengono cancellati dal buffer.
- **Text language** – gli SMS usano i caratteri propri della lingua scelta.

- **Suspend event reporting when ... same events per ... s** – sospensione della trasmissione se lo stesso evento si ripete più volte del numero indicato nel tempo indicato (ad esempio un rivelatore guasto). **Restore event reporting after** – dopo questi minuti (0–999) la centrale segnala di nuovo l'evento.
- **Call** – in caso di evento la centrale chiama l'utente questo numero di volte. Se la chiamata viene accettata o rifiutata, non chiama più. Una chiamata dura 20 secondi.
- **EOL Type** – il valore delle resistenze di fine linea collegate alle zone: RT è la resistenza antimanomissione, R1 quella del 1°, R2 quella del 2° rivelatore. Il collegamento è mostrato nel capitolo 3.
- **Communication path test** – a questo intervallo la centrale invia un messaggio di prova alla centrale di vigilanza anche sui canali di riserva, poi torna al canale principale.
- **LED out as 2Wire fire** – spunta se colleghi all'uscita LED un rivelatore d'incendio a due fili.

Gruppo **SIM**:

- **PIN** – il codice PIN della scheda SIM. Se sulla scheda non c'è la richiesta del PIN, lascia il valore di fabbrica.
- **APN** – il nome del punto di accesso Internet dell'operatore mobile. Obbligatorio se la centrale trasmette al cloud Protegus o alla centrale di vigilanza tramite Internet mobile.
- **Login**, **Password** – nome utente e password dell'APN, solo se l'operatore li richiede.
- **Locked ICCID** – il numero ICCID della scheda SIM. Se lo compili, la centrale funziona solo con questa scheda.
- **Preferred operator** – codice operatore (MCC + MNC). Se lo compili, la centrale si registra solo sulla rete di questo operatore.

Codici operatore – esempio: Italia

TIM 22201, Vodafone 22210, WINDTRE 22288, Iliad 22250. Il codice di un operatore di un altro paese è composto allo stesso modo dall'MCC del paese e dall'MNC dell'operatore. Se lasci il campo vuoto, la centrale sceglie la rete automaticamente; inserisci il codice solo se deve restare su una rete specifica.

Gruppo **Time settings**:

- **Set PC time** – scrive nella centrale l'ora del computer. Se nel campo **Time synchronization** c'è **Disabled**, resta quest'ora; se c'è **modem** o **server**, dopo l'accensione la centrale si sincronizza da lì.
- **Time zone (Hours)** – il fuso orario; ad esempio +1 in Italia (Europa centrale).
- **Time set** – il server dell'ora con cui la centrale si sincronizza all'accensione.
- **Daylight saving time** – passaggio automatico tra ora legale e ora solare.
- **AC failure delay** – la centrale segnala la mancanza della tensione di rete con questo ritardo, e anche il ritorno con ritardo.

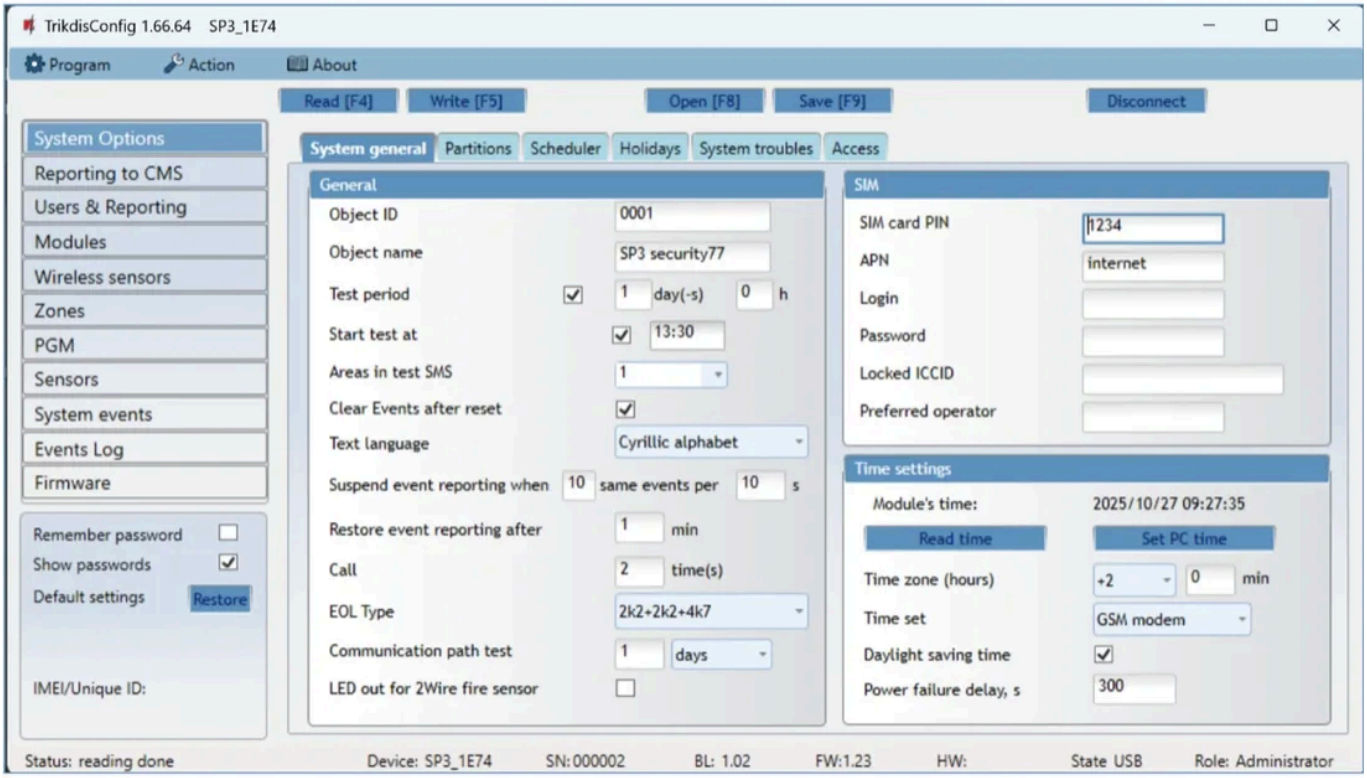


Figura 51. System Options → System general: i gruppi General, SIM e Time settings.

6.2.2 Scheda Partitions

- **Partitions enabled** – in quante parti indipendenti (aree) dividi il sistema.
- **Partition name** – il nome dell'area.
- **Entry** – ritardo d'ingresso, 0–999 s. È il tempo che hai per raggiungere la tastiera attraverso la zona Delay e disinserire il sistema.
- **Exit** – ritardo d'uscita, 0–999 s. Dopo l'inserimento – contando dal codice di inserimento digitato sulla tastiera – è il tempo che hai per lasciare il locale attraverso la zona Delay. Con l'inserimento a distanza (ad esempio da Protegus 2) il sistema si inserisce subito, senza tempo d'uscita.
- **Bell** – il tempo di funzionamento della sirena in caso di allarme, 0–999 s.
- **Squawk** – la sirena emette un bip all'inserimento e due al disinserimento.
- **Re-ARM** – reinserimento automatico se il sistema è stato disinserito a distanza ma durante il tempo d'ingresso nessuno ha violato la zona Delay.
- **Force-ARM** – inserimento forzato. Il sistema si può inserire anche con zone Stay aperte, purché la zona d'ingresso sia chiusa.
- **Keyswitch** – la zona a chiave inserisce e disinserisce con impulso (**Pulse**) o con livello (**Level**).
- **Tamper** – gestione dell'evento di manomissione quando la centrale rileva la manomissione di un rivelatore: **Silent** (va solo la segnalazione ai destinatari, la sirena non suona), **Audible when armed** (va la segnalazione, la sirena suona solo se la manomissione avviene a sistema inserito), **Always Audible** (va la segnalazione e la sirena suona anche a sistema disinserito).

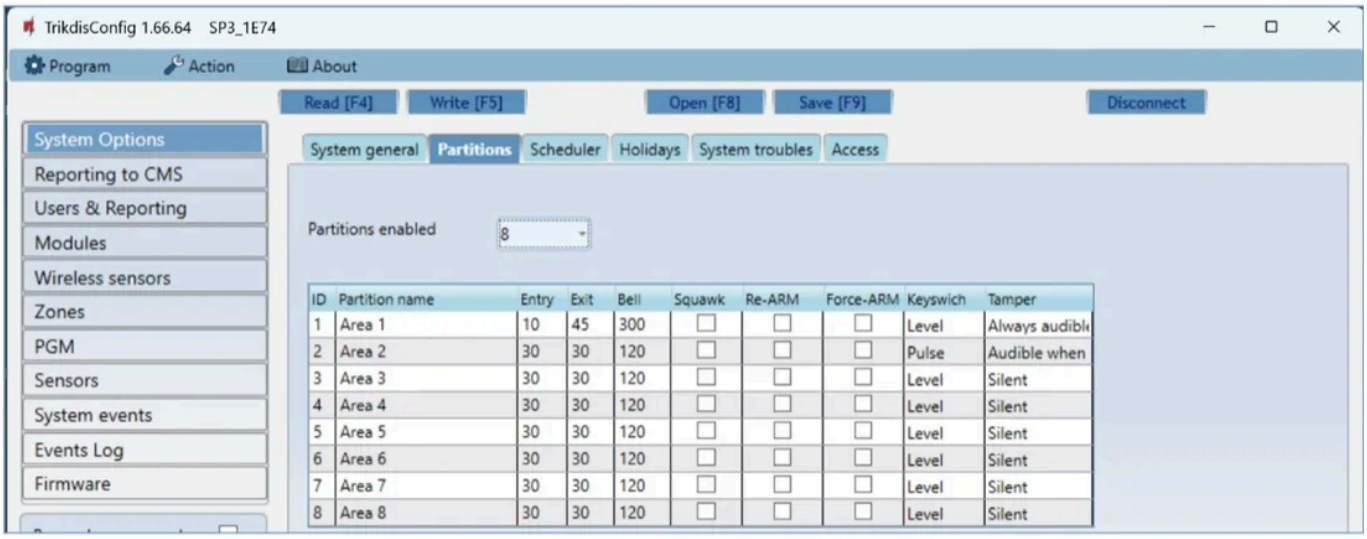


Figura 52. System Options → Partitions: per ogni area il tempo d'ingresso, d'uscita e della sirena, oltre al comportamento.

6.2.3 Scheda Scheduler

Inserimento e disinserimento automatici in base ai giorni della settimana, con i giorni festivi.

- **Enable** – abilitazione della programmazione.
- **Partition** – l'area a cui si riferisce.
- **Time** – l'orario dell'operazione.
- **Not Armed** – l'operazione viene eseguita solo se la centrale non è inserita in modalità totale (Away).
- **Action** – la modalità da impostare: **Disarm**, **Arm**, **Sleep** o **Stay**.
- **Monday … Sunday** – in quali giorni vale.
- **Holiday** – comportamento nei giorni festivi: **Disabled** (nessuna festività), **Ignore on holidays** (non viene eseguita nei festivi), **Additional when holidays** (viene eseguita anche nei festivi), **Only holidays** (viene eseguita solo nei festivi).
- **Holiday group** – quale gruppo di festività (**Any**, 1–4) considerare come festivo. Con **Any** conta qualsiasi festività attiva.

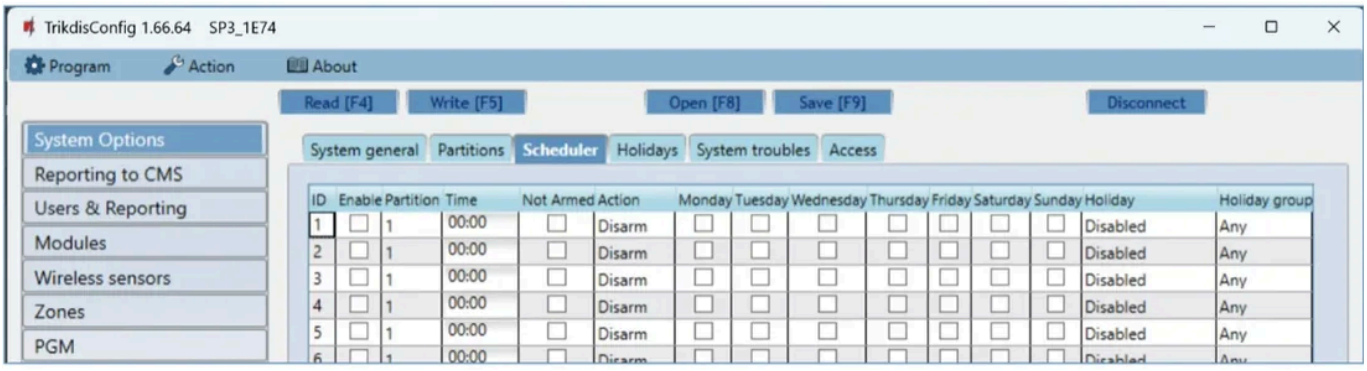


Figura 53. System Options → Scheduler: programma settimanale di inserimento e disinserimento.

6.2.4 Scheda Holidays

- **Enable** – abilitazione della festività.
- **Start date**, **Stop date** – il primo e l'ultimo giorno della festività. Per una festività di un giorno le due date coincidono.
- **Group 1 … Group 4** – raggruppi le festività in gruppi, a cui fa riferimento la programmazione.

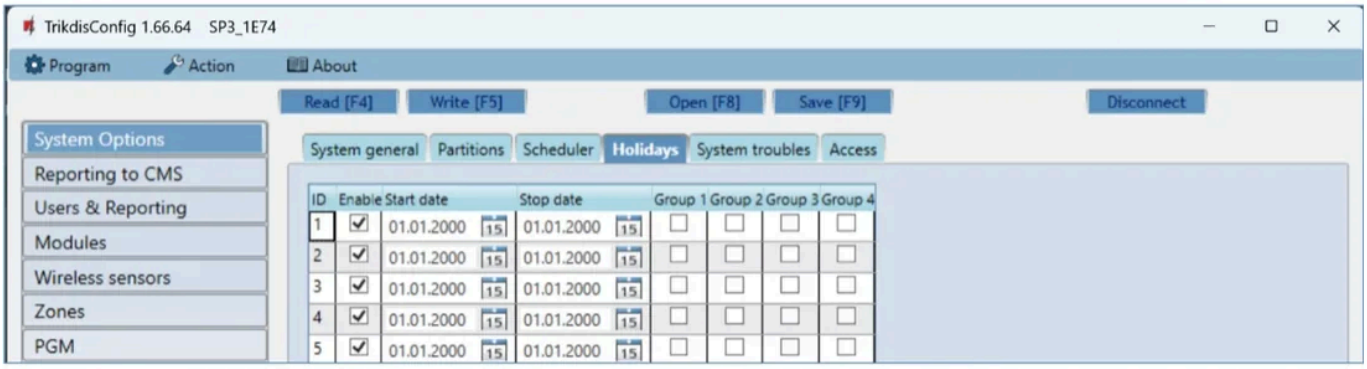


Figura 54. System Options → Holidays: giorni festivi in quattro gruppi.

6.2.5 Scheda System troubles

Se qui spunti un guasto interno, il sistema non si può inserire finché il guasto persiste. In questo modo puoi impedire che si inserisca ad esempio con la batteria scarica o senza alimentazione di rete.

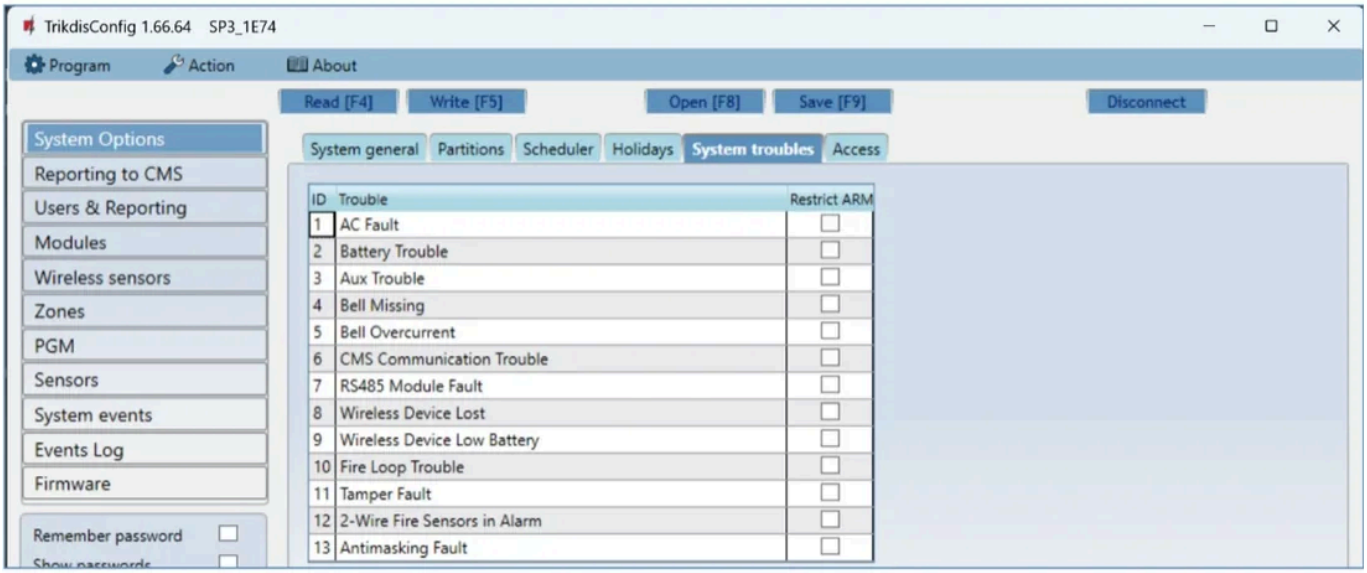


Figura 55. System Options → System troubles: quali guasti impediscono l'inserimento.

6.2.6 Scheda Access

Gruppo **Access codes**:

- **Administrator Code** – valore di fabbrica 123456. Accesso completo alle impostazioni. Sei caratteri, lettere latine e/o cifre.
- **SMS password** – valore di fabbrica 123456. La password dei comandi SMS (5.3), con cui il sistema si controlla in sicurezza via SMS; per motivi di sicurezza sostituiscila con una password a sei cifre nota solo a te.
- **Installer Code** – valore di fabbrica 654321. L'accesso dell'installatore alle impostazioni; per motivi di sicurezza sostituiscilo con un codice a sei cifre noto solo a te.

Gruppo **Installer permissions** – qui stabilisci cosa può impostare chi accede con il codice installatore.

Codice amministratore di fabbrica

Finché il codice amministratore è quello di fabbrica 123456, dopo **Read [F4]** il programma mostra le impostazioni senza chiedere il codice.

Prima della consegna

Prima della consegna cambia tutti e tre i codici. Il codice amministratore appartiene al proprietario; il codice installatore e i suoi permessi possono essere modificati in seguito dal proprietario.

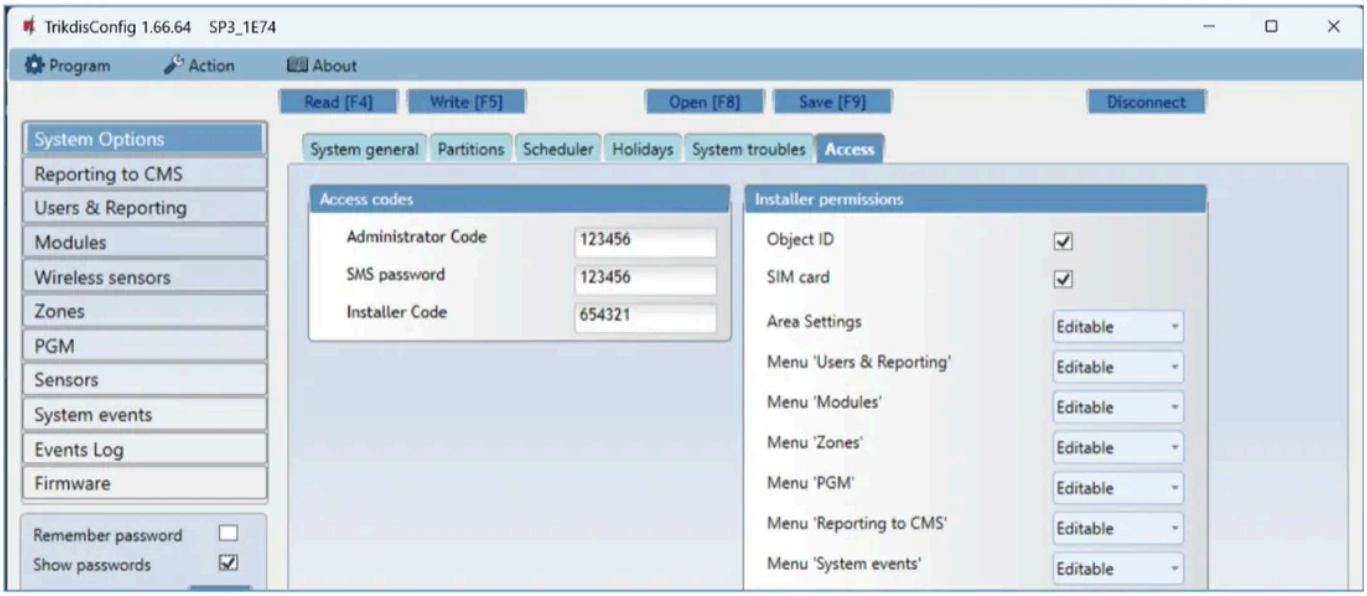


Figura 56. System Options → Access: i tre codici e i permessi dell'installatore.

6.3 Reporting to CMS

La centrale invia gli eventi alla centrale di vigilanza (CMS) tramite Internet mobile (IP) o via SMS. Puoi indicare più canali: il canale principale (**Primary**) e quello parallelo (**Parallel**) funzionano contemporaneamente, quindi due ricevitori possono ricevere gli eventi; a entrambi si può assegnare un canale di riserva (**Backup**), che entra in funzione se la connessione del canale principale o di quello parallelo si interrompe. La connessione è crittografata e protetta da password; per la ricezione serve un ricevitore Trikdis: su IP il ricevitore software IPcom, il ricevitore hardware RL14 o RM14; per gli SMS l'RL14, l'RM14 o il GM14. L'SMS va bene come canale di riserva, perché funziona anche senza Internet mobile; come canale principale non è consigliato.

6.3.1 Scheda Reporting

Gruppi **Primary channel**, **Backup channel**, **Parallel channel** e **Parallel backup channel**:

- **Communication type** – il protocollo usato con il ricevitore: **TCP/IP**, **UDP/IP**, **SMS** o **Disabled**.
- **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- **Port** – la porta del ricevitore.
- **Protocol** – **TRK** per un ricevitore Trikdis, **SIA DC-09** per un ricevitore IP che accetta il formato SIA DC-09.
- **Phone number** – solo per gli SMS: il numero di telefono del ricevitore SMS Trikdis, con il prefisso internazionale (ad esempio 39… per l'Italia).
- **Encryption key** – chiave di crittografia a sei cifre, deve coincidere con la chiave del ricevitore.

Se compili anche il canale parallelo, gli eventi vanno contemporaneamente su entrambi i canali, quindi due ricevitori (ad esempio una centrale di vigilanza locale e una centrale) li ricevono contemporaneamente. I due canali non possono puntare allo stesso ricevitore.

Backup channel 2 e **Parallel backup channel 2** – riserva SMS: nel campo **Phone number** va il numero del ricevitore SMS della centrale di vigilanza (con il prefisso internazionale). La centrale invia qui se l'invio non riesce né sul canale principale, né su quello parallelo, né su quello di riserva; è particolarmente utile perché funziona anche quando nella rete dell'operatore mobile non c'è connessione IP. Funziona solo se il primo canale e la sua riserva sono IP. L'SMS viene inviato alla prima accensione e quando la connessione IP si interrompe sul primo canale e sulla sua riserva.

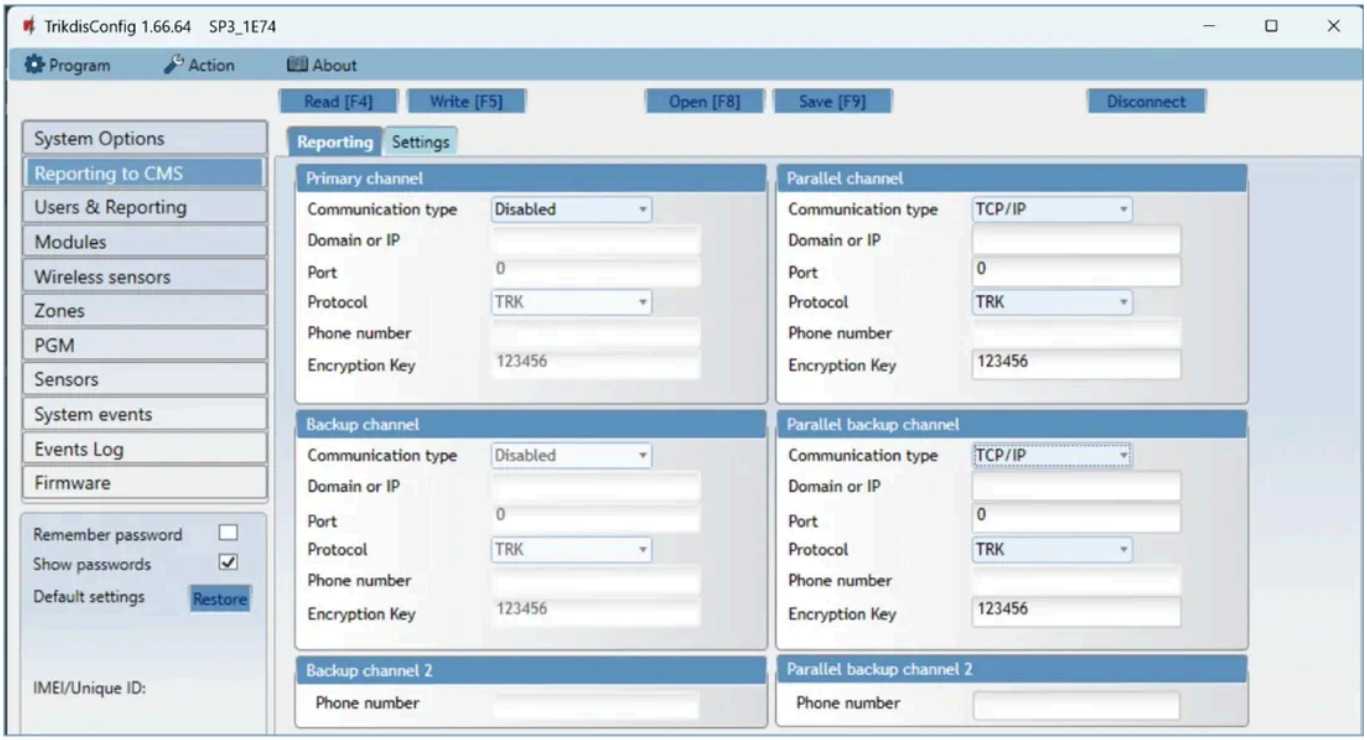


Figura 57. Reporting to CMS → Reporting: canali principale, di riserva e parallelo.

6.3.2 Scheda Settings

Gruppo **Settings**:

- **Return to primary after** – dopo questi minuti la centrale prova a tornare al canale principale.
- **IP Ping period** – l'intervallo in secondi dei segnali di controllo della connessione IP; la spunta lo attiva.
- **SMS Ping period** – l'intervallo in minuti dei segnali di controllo del canale SMS; la spunta lo attiva.
- **Backup reporting after** – dopo questo numero di invii falliti la centrale passa al canale di riserva.
- **DNS1**, **DNS2** – indirizzo dei server DNS. Con qualsiasi impostazione IP indica un indirizzo DNS supportato dall'operatore.
- **Object ID in SIA DC-09**, **SIA DC-09 receiver No.**, **Line No.** – numero impianto, numero ricevitore e numero linea per il protocollo SIA DC-09.
- **Local time in SIA** – nei messaggi inviati alla centrale di vigilanza compare l'ora propria della centrale.

Gruppo **Reporting mode** – su quale via la centrale comunica con la centrale di vigilanza e con Protegus 2. L'ordine dei tipi conta: se la connessione **Main type** non si stabilisce, la centrale passa alla via **Backup type** e poi **Backup type 2**.

- **Main type**, **Backup type**, **Backup type 2** – **SIM**, **WiFi** o **LAN(E485)**, separatamente nella colonna CMS e in quella Protegus.
- **Radio T16 (SF485)** – spunta se trasmette anche un trasmettitore radio T16. Il T16 funziona come canale di riserva se almeno una tra SIM, WiFi e LAN è in uso; se non c'è altra connessione, il T16 è il canale principale. Il T16 invia segnalazioni solo alla centrale di vigilanza.

- **Return to main (both channel)** – dopo questi minuti la centrale prova a tornare alla via principale, se stava trasmettendo sulla riserva.

Gruppo **Communicator network settings** (versione WiFi):

- **DHCP mode** – se spuntato, la centrale riceve automaticamente indirizzo IP, maschera di sottorete e gateway.
- **Static IP**, **Subnet mask**, **Default gateway** – per l'impostazione manuale.
- **WiFi SSID name**, **WiFi SSID password** – il nome e la password della rete WiFi.

Gruppo **SIM parameters**:

- **Disable indication of the absence of a SIM card** – la centrale non segnala l'assenza della scheda SIM.
- **Use dial and SMS when working over internet module** – se spuntato, chiamata e SMS funzionano anche quando la centrale trasmette su WiFi o LAN. Senza spunta, se c'è il WiFi la centrale non usa SMS e chiamate; se senza spunta il WiFi non c'è, la centrale resta controllabile con chiamata e SMS e invia SMS all'utente.
- **Disable the use of SIM card mobile data** – la centrale non usa i dati mobili della SIM, trasmette solo su WiFi. Se il WiFi viene a mancare temporaneamente, memorizza gli eventi e li invia più tardi.

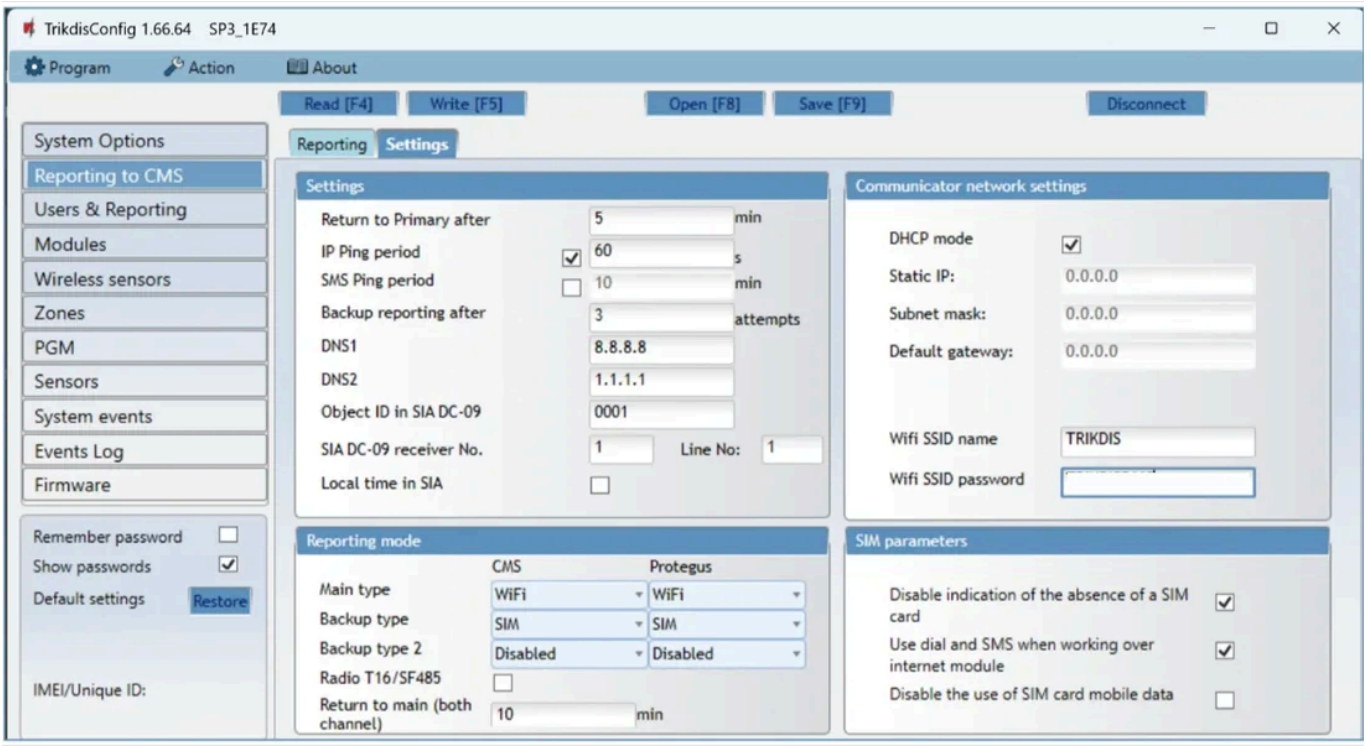


Figura 58. Reporting to CMS → Settings: segnali di controllo, ordine delle connessioni, WiFi e parametri SIM.

6.4 Users & Reporting

Nelle righe della scheda **Users** (gruppo **Users & Reporting to User**) aggiungi gli utenti:

- **Name** – il nome dell'utente, compare negli SMS degli eventi.
- **Tel number** – numero di telefono con il prefisso internazionale. Da questo numero l'utente può controllare il sistema, e su di esso riceve gli SMS. I primi otto numeri ricevono segnalazioni via SMS e con chiamata.
- **Email** – indirizzo e-mail; l'utente riceve un invito a Protegus 2.

- **Code** – il codice di inserimento e disinserimento dell'utente.
- **Tag code** – il numero identificativo della tessera RFID, del portachiavi RFID o della chiave iButton.
- **Areas** – quali aree può gestire.
- **A**, **D** – può inserire, rispettivamente disinserire.
- **PGM** – può comandare le uscite con una chiamata telefonica, con toni DTMF (5.4).
- **ACK** – la centrale conferma via SMS l'esecuzione dei comandi ricevuti.
- **FWD** – la centrale inoltra a questo utente gli SMS che arrivano da non utenti (comunicazione del credito, pubblicità).

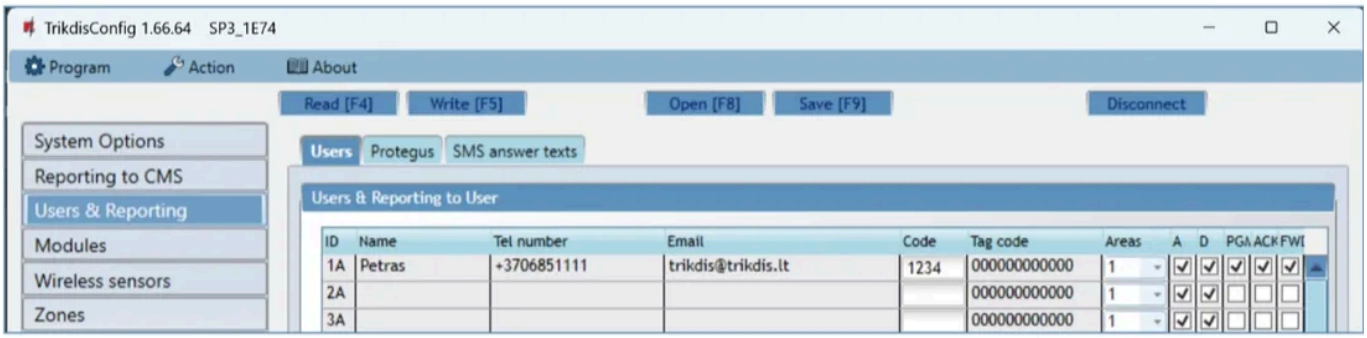


Figura 59. Users & Reporting → Users: utenti, codici, identificativi e permessi.

6.4.1 Tessere e portachiavi RFID

La tessera e il portachiavi RFID non si memorizzano avvicinandoli al lettore: scrivi a mano il numero identificativo della tessera come numero decimale nel campo **Tag code**, poi **Write [F5]**. Il numero è stampato sulla maggior parte delle tessere.



Figura 60. I numeri stampati su una tessera RFID: il primo gruppo di cifre incorniciato è il **Tag code**.

Un lettore Wiegand senza tastiera, per l'apertura della porta

1. Colleghi i fili dati del lettore ai morsetti **GRN** e **YEL** della scheda.
2. Nella scheda **Modules** → **Keypads**, nel gruppo **Keypad parameters**, il **Keypad type** deve essere **Wiegand reader**, anche se non c'è una tastiera.
3. Nella finestra **PGM** il campo **Output definition** dell'uscita comandata è **Remote control**, il **Pulse time, s** ad esempio 5.
4. Nella scheda **PGM** → **Control**, alla riga del lettore spunta il campo **En**, nel campo **PGM** scrivi il numero dell'uscita, il **PGM mode** deve essere **Pulse**.

6.4.2 Chiavi iButton

Memorizzazione con il lettore **TM17**:

1. Se l'elenco **Tag code** è vuoto, la prima chiave memorizzata va nella prima riga dell'elenco e diventa chiave master (Master).
2. Per attivare la modalità di apprendimento tieni la chiave master sull'"occhio" del lettore per almeno 10 secondi. In modalità di apprendimento il LED **State** del TM17 lampeggia in verde.
3. Avvicina le chiavi utente al lettore una per una. Tre bip segnalano che la chiave è stata aggiunta al sistema.
4. Alla fine avvicina di nuovo la chiave master al lettore; il LED **State** smette di lampeggiare.
5. Per cancellare tutte le chiavi (compresa la chiave master) tieni la chiave master sul lettore per almeno 20 secondi.

Con il lettore **CZ-Dallas** allo stesso modo, ma senza segnalazione LED: chiave master per 10 secondi, chiavi utente una per una, alla fine di nuovo la chiave master; cancellazione con 20 secondi.

Il ruolo della chiave master

La chiave master serve a memorizzare le altre chiavi. Se la usi anche per inserire e disinserire, il comando viene eseguito con un ritardo.

6.4.3 Scheda Protegus

Gruppo **Cloud application**:

- **Enable cloud service** – abilitazione del cloud Protegus. Tramite esso la centrale comunica con Protegus 2, e tramite esso si può configurare a distanza con TrikdisConfig.
- **Parallel reporting** – gli eventi vanno contemporaneamente sul canale principale alla centrale di vigilanza e a Protegus 2.
- **Cloud access code** – codice a sei cifre per la connessione a Protegus 2, valore di fabbrica 123456.

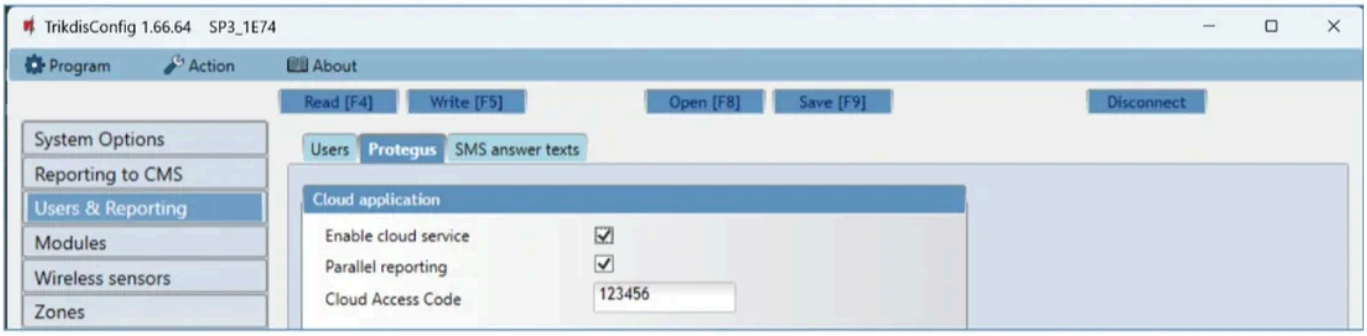


Figura 61. Users & Reporting → Protegus: l'interruttore del servizio cloud e il codice di accesso.

6.4.4 Scheda SMS answer texts

Il testo delle risposte ai comandi SMS si può riscrivere nella colonna **SMS text**, ad esempio in italiano.

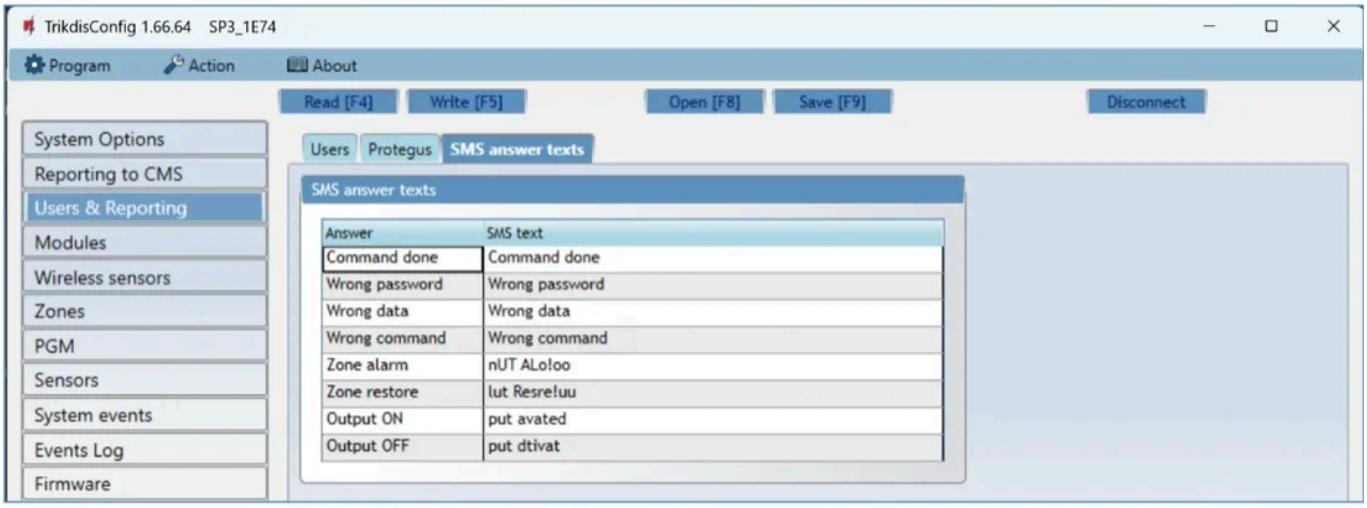


Figura 62. Users & Reporting → SMS answer texts: il testo degli SMS di risposta.

6.5 Modules

Scheda **Keypads**:

- **Serial** – il numero di serie della tastiera, riconosciuto automaticamente dalla centrale. Per cancellarlo scrivi degli zeri o premi il pulsante **Remove**.
- **Keypad type** – il tipo di tastiera, riconosciuto automaticamente.
- **Areas** – quali aree può gestire la tastiera (solo per le tastiere FLEXi SK LCD, FLEXi SK LED, SK LCD Button e SK LED Button).
- **Remove** – cancellazione della tastiera dall'elenco.

Gruppo **Keypad parameters**:

- **Keypad type** – il tipo di tastiera collegata ai morsetti **GRN** e **YEL**: **Crow CR16**, **Paradox LED** o **Wiegand reader**.
- **Additional Wiegand on 1IO/2IO** – spunta se colleghi un secondo lettore RFID ai morsetti **IO1** e **IO2**. In tal caso questi non si possono usare come ingressi o uscite.
- **6 digits user code** – codice utente a sei cifre sulla tastiera. A un codice esistente a quattro cifre il programma aggiunge le prime due cifre (1234 diventa 123412); tutti i codici utente a quattro cifre vengono trasformati così.
- **Duress code type** – il tipo di codice sotto coercizione. Sotto costrizione inserisci o disinserisci con questo: il sistema esegue e invia un allarme silenzioso alla centrale di vigilanza.
- **Quick ARM** – i pulsanti **ARM**, **STAY** e **SLEEP** della tastiera inseriscono senza codice.
- **Incorrect codes until lockout** – dopo questo numero di codici errati la tastiera si blocca.
- **Lockout timer** – la durata del blocco in minuti.
- **Panic alarm type**, **Medical alarm type**, **Fire alarm type** – l'effetto dei tasti funzione panico, soccorso medico e incendio della tastiera, quando vengono premuti: **Audible** (suona la sirena, la tastiera dà un allarme sonoro e la segnalazione va a Protegus 2 e alla centrale di vigilanza), **Silent** (va solo la segnalazione a Protegus 2 e alla centrale di vigilanza, la centrale disattiva l'allarme sonoro), **Disabled** (non va nessuna segnalazione né a Protegus 2 né alla centrale di vigilanza).
- **Low voltage reader (1IO/2IO)** – se il lettore RFID collegato non funziona, con questo cambi il protocollo tra la centrale e il lettore.
- **Use fingerprint** – per un lettore di impronte digitali con protocollo Wiegand 26/34.
- **Do not change charset** – sulla tastiera SK-LCD TouchPad la codifica dei caratteri dei nomi di zone e aree resta invariata.

- **Custom entry beep** – il suono del ritardo d'ingresso sulla tastiera è intermittente.

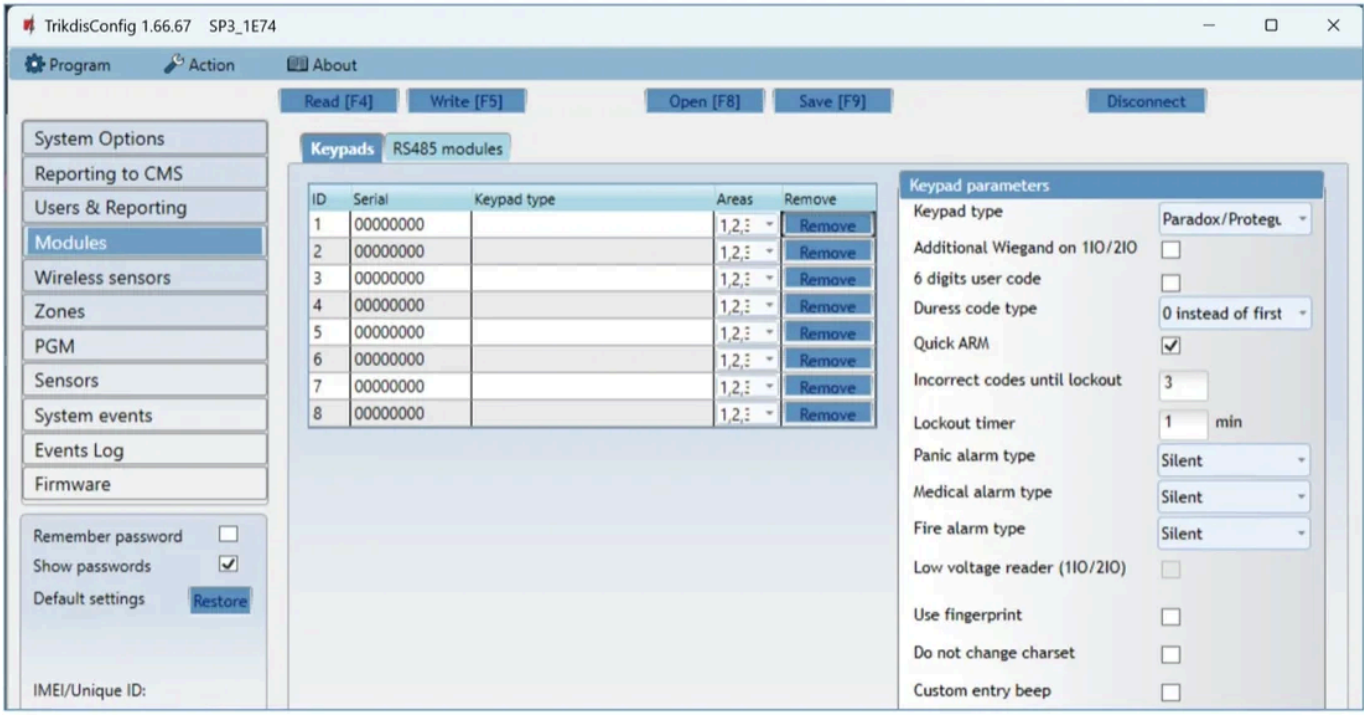


Figura 63. Modules → Keypads: le tastiere riconosciute e i parametri delle tastiere.

Scheda **RS485 modules**:

- **ID** – il numero d'ordine del modulo.
- **Module** – il tipo di espansione dall'elenco: iO, iO-WL, TM17, iO-8, RF-SH, E485, T16, SF485, iO-MO, iO-LORA, iO8-LORA, PB-LORA, REL-LORA, RF-LORA, RF-HW, RF-S8.
- **Serial No.** – obbligatorio, numero a sei cifre dall'etichetta sull'involucro e sulla confezione del modulo.
- **Area** – l'area del modulo. Il TM17 mostra lo stato e le zone di quest'area.
- **Name** – il nome del modulo.
- **Firmware version** – non appena la centrale trova il modulo, qui compare la sua versione firmware. È il segno che il modulo è attivo.

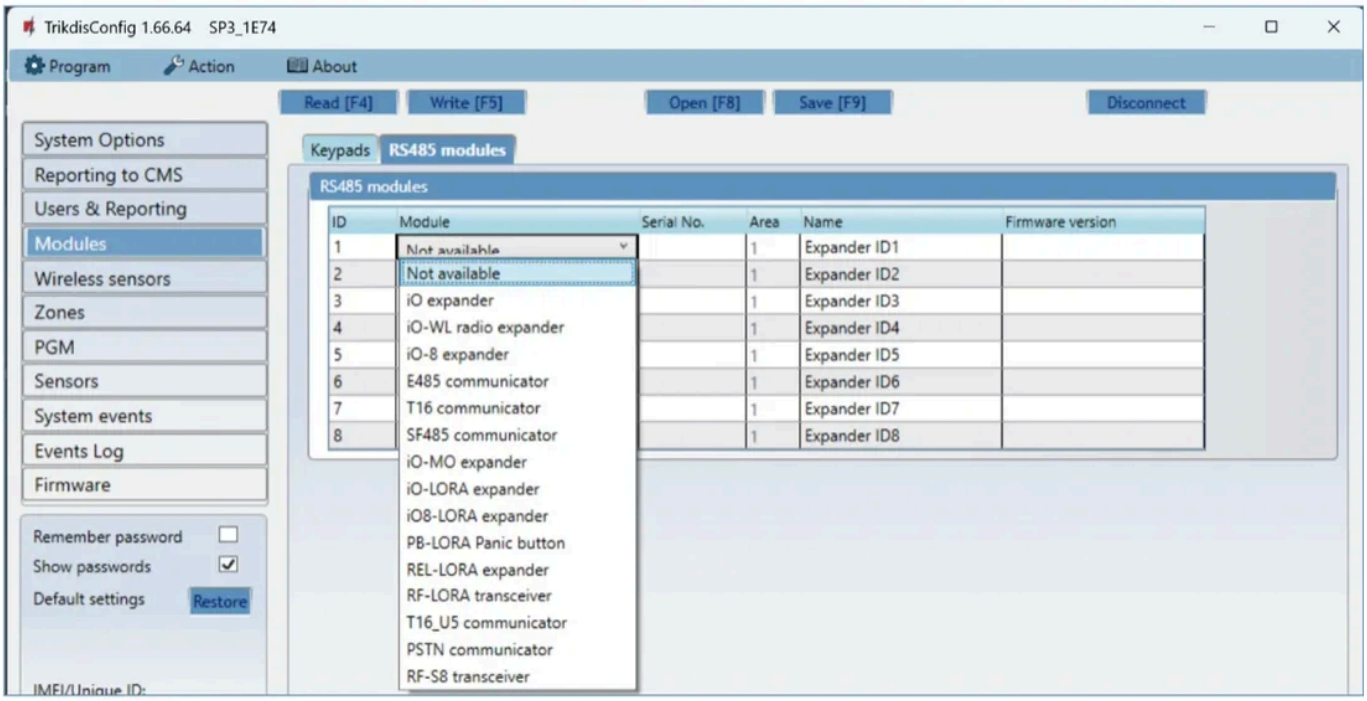


Figura 64. Modules → RS485 modules: l'elenco delle espansioni con il menu a tendina **Module**.

Scheda **E485 settings** – le impostazioni di rete del comunicatore LAN E485: **DHCP mode** (indirizzo automatico: se spuntato, la centrale legge automaticamente le impostazioni di rete – maschera di sottorete, gateway – e riceve automaticamente l'indirizzo IP), oppure per l'impostazione manuale **Static IP**, **Subnet mask**, **Default gateway**.



Figura 65. Modules → E485 settings: l'indirizzamento del modulo LAN E485.

6.6 Wireless sensors

Con il modulo RF-LORA la "FLEXi" SP3 usa i rivelatori, le sirene e i telecomandi senza fili del produttore Maximum. Per questo sulla centrale serve il firmware con codice ricevitore 4, almeno nella versione 1.21 (SP3_xxx4_0121 o successiva; la 4ª cifra del nome del firmware è il tipo di ricevitore, vedi 1.7). Il ricetrasmettitore RF-LORA si collega al bus RS485 della centrale (4.6). Prima registri il modulo RF-LORA nella centrale (6.6.1), poi memorizzi i rivelatori: a distanza da TrikdisConfig (6.6.2) o con il pulsante LEARN del modulo (6.6.3). L'accoppiamento dei rivelatori S8 che funzionano con il ricevitore RF-S8 è descritto nel capitolo 4 del Manuale del ricetrasmettitore RF-S8 e dei rivelatori S8.



Figura 66. La finestra **Wireless sensors**: l'elenco dei dispositivi memorizzati, sopra i pulsanti **Learn sensors** e **Update**.

6.6.1 Registrazione dell'RF-LORA

1. Accendi l'alimentazione della centrale e attendi 1 minuto.
2. Avvia TrikdisConfig e collega la centrale al computer con un cavo USB Mini-B.
3. Premi il pulsante **Read [F4]** e apri la scheda **Modules** → **RS485 modules**. Se nell'elenco c'è l'**RF-LORA transceiver** con il suo numero di serie e la versione firmware, hai finito, gli altri passaggi si saltano.
4. Se non c'è, in una riga vuota seleziona nel campo **Module** la voce **RF-LORA transceiver**.
5. Nel campo **Serial No.** scrivi il numero di serie del modulo dall'etichetta sull'involucro o sulla confezione.
6. **Write [F5]**, poi scollega il cavo USB.
7. Attendi 1 minuto, finché la centrale e l'RF-LORA si collegano.
8. Ricollega il cavo USB e premi il pulsante **Read [F4]**. Nella finestra **Modules** compare la versione firmware dell'RF-LORA: il modulo è registrato.
9. Scollega il cavo USB, premi il pulsante **Disconnect** e attendi 1 minuto.

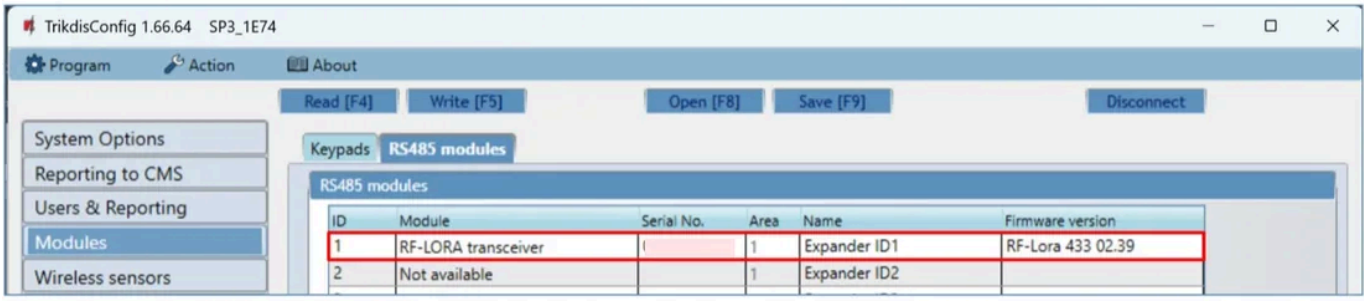


Figura 67. Nella scheda **RS485 modules** la riga dell'RF-LORA registrato: tipo, **Area**, nome e **Firmware version**. Il numero di serie è nascosto nella figura.

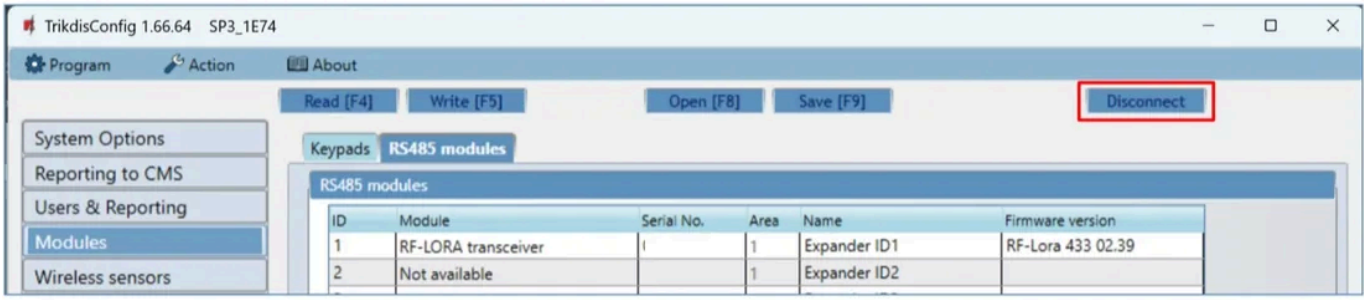


Figura 68. Dopo la lettura compare la versione firmware dell'RF-LORA, poi **Disconnect**.

6.6.2 Accoppiamento dei rivelatori a distanza

Condizioni per la configurazione a distanza: scheda SIM attivata con PIN inserito o disattivato e Internet mobile (oppure connessione WiFi), servizio cloud attivato (6.4.3), tensione di alimentazione e connessione di rete (il LED **NET** è verde fisso).

1. Nella schermata iniziale di TrikdisConfig scrivi nel campo **Unique ID** del gruppo **Remote access** il numero **IMEI/Unique ID** della centrale (sull'etichetta della scheda e della confezione) e premi il pulsante **Configure**.
2. Nella finestra che si apre **Read [F4]**; se serve, inserisci il codice amministratore o installatore.
3. Apri la finestra **Wireless sensors** e premi il pulsante **Learn sensors**. L'RF-LORA passa in modalità di apprendimento, il suo LED **DATA/TROUBLE** inizia a lampeggiare verde-rosso, TrikdisConfig apre la finestra di apprendimento.
4. Inserisci le batterie nei rivelatori (rivelatori di movimento, contatti magnetici, rivelatori d'acqua, di fumo, sirena). Puoi memorizzare più rivelatori contemporaneamente. L'RF-LORA deve essere ad almeno 1 m dai rivelatori.
5. Premi il pulsante **TAMPER** (antimanomissione) del rivelatore. Il LED **DATA/TROUBLE** dell'RF-LORA lampeggia brevemente in verde (il rivelatore è stato aggiunto), poi dopo qualche secondo di nuovo verde-rosso.
6. TrikdisConfig apre una nuova finestra: inserisci i valori **Zone number** e **Zone definition** del rivelatore, poi **Save**. Il rivelatore viene aggiunto all'elenco.
7. Per il rivelatore successivo di nuovo il pulsante **TAMPER**, e così via. Alla fine premi il pulsante **Stop learning**.
8. Alla domanda **Yes**: i rivelatori vengono scritti nella centrale (**No**, se vuoi prima modificarli ancora). Attendi qualche minuto, poi **Read [F4]**: nella finestra **Wireless sensors** si vedono i rivelatori memorizzati e, nella colonna **Serial No.**, il loro numero di serie.
9. Verifica nella finestra **Zones** che i rivelatori siano assegnati alla zona e all'area corrette. Se il campo **Type** della zona è **EOL_T**, è attiva anche la supervisione antimanomissione del rivelatore. Dopo una modifica **Write [F5]**.

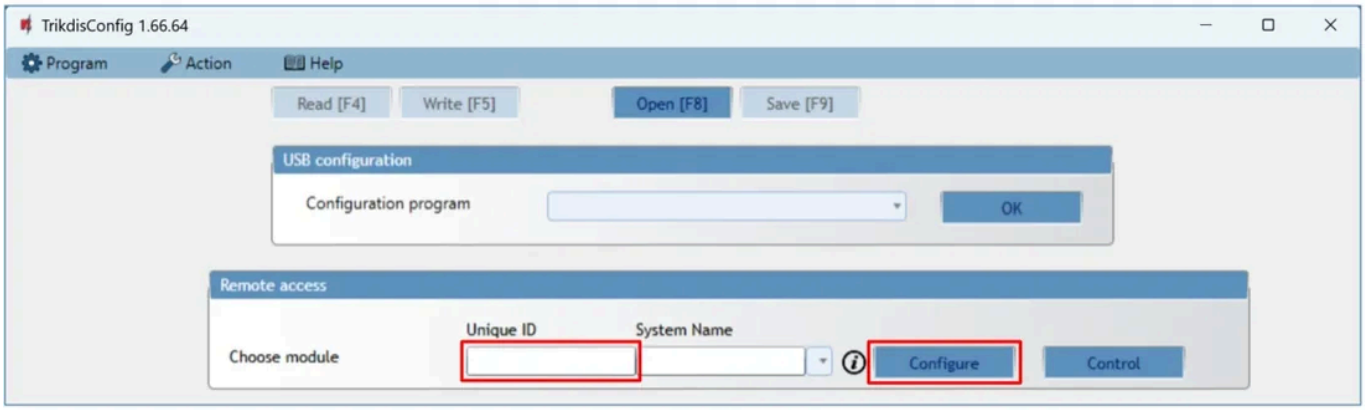


Figura 69. Il gruppo **Remote access** della schermata iniziale: **Unique ID**, **System Name**, **Configure**.

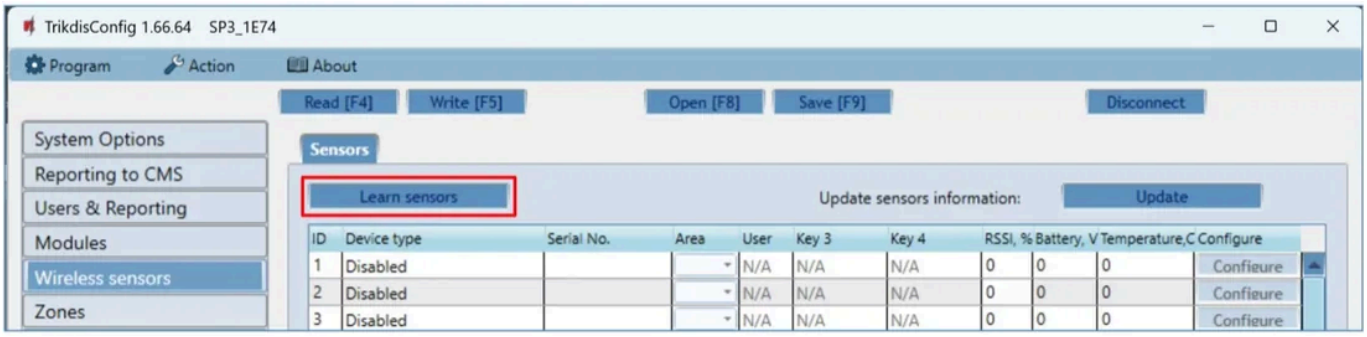


Figura 70. Il pulsante **Learn sensors** della finestra **Wireless sensors** avvia la modalità di apprendimento.

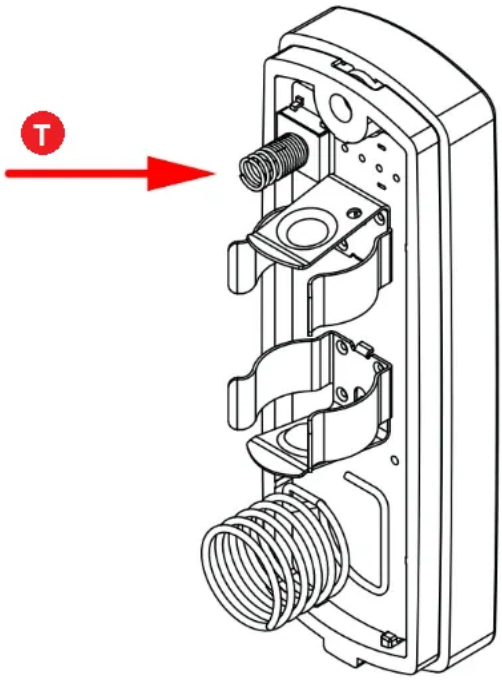


Figura 71. La pressione del pulsante **TAMPER** sotto il coperchio posteriore del rivelatore registra il rivelatore.

- T pulsante antimanomissione (“Tamper”)

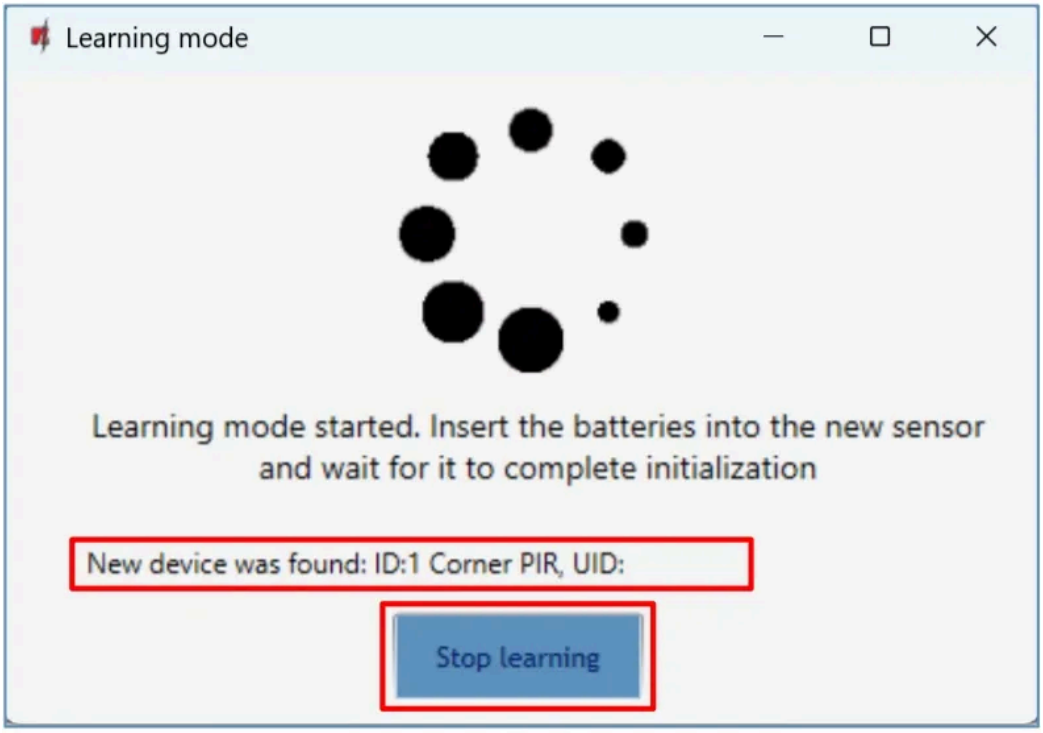


Figura 72. La finestra di apprendimento: tipo e identificativo del rivelatore trovato, sotto il pulsante **Stop learning**. L'identificativo è nascosto nella figura.

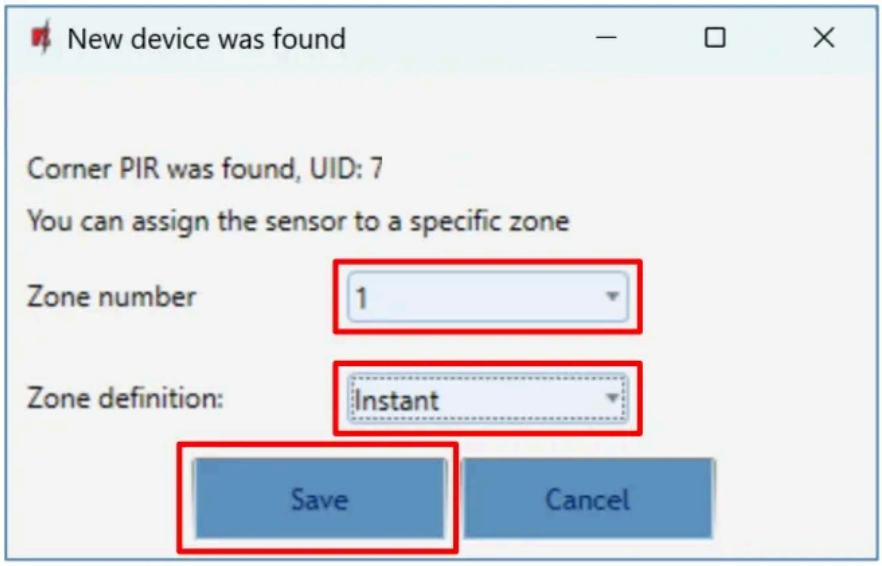


Figura 73. La finestra del nuovo dispositivo: **Zone number**, **Zone definition**, **Save**.

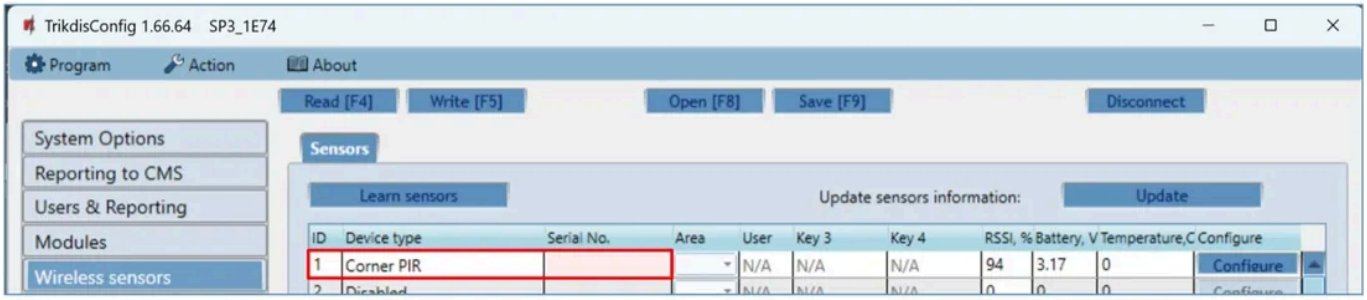


Figura 74. Il rivelatore memorizzato nell'elenco, con intensità del segnale (**RSSI**), tensione della batteria e temperatura. Il numero di serie è nascosto nella figura.

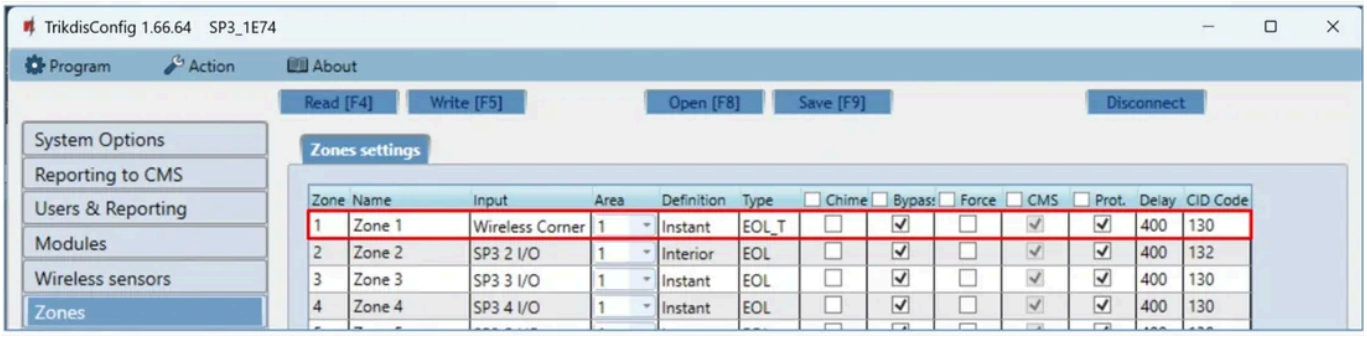


Figura 75. Nella finestra **Zones** la zona del rivelatore senza fili con tipo **EOL_T**: è supervisionata anche la segnalazione di manomissione.

Cancellazione di un rivelatore senza fili

Collegati alla centrale via USB o a distanza, **Read [F4]**, poi nella colonna **Device type** della finestra **Wireless sensors** seleziona per il rivelatore da cancellare la voce **Disabled**, e **Write [F5]**.

6.6.3 Accoppiamento con il pulsante LEARN

1. L'RF-LORA deve essere registrato nella centrale (6.6.1), la centrale deve essere accesa.
2. Togli il coperchio dell'RF-LORA. Tieni premuto il pulsante **LEARN** finché il LED **DATA/TROUBLE** non inizia a lampeggiare verde-rosso, poi rilascialo. Il lampeggio indica la modalità di apprendimento.
3. Inserisci le batterie nei rivelatori e premi il pulsante **TAMPER** del rivelatore. Un breve lampeggio verde del LED **DATA/TROUBLE** indica il successo; dopo qualche secondo lampeggia di nuovo verde-rosso. Per il rivelatore successivo di nuovo il pulsante **TAMPER**.
4. Alla fine tieni premuto il pulsante **LEARN** finché il lampeggio verde-rosso non si interrompe, poi rilascialo. L'RF-LORA è uscito dalla modalità di apprendimento.
5. Collega la centrale al computer via USB, avvia TrikdisConfig, **Read [F4]**. Nella finestra **Wireless sensors** i dispositivi memorizzati si vedono con il loro numero di serie a sette cifre.
6. Nella finestra **Zones** controlla le zone e le aree, dopo una modifica **Write [F5]**.

6.6.4 RF-SH e dispositivi Crow

I sistemi più vecchi con modulo RF-SH usano i dispositivi senza fili delle serie Crow FW2 e Shepherd (SH). L'RF-SH non è più in vendita; la descrizione resta qui in breve per la manutenzione dei sistemi esistenti; il collegamento del modulo è mostrato nel paragrafo 4.2.

- **Registrazione dell'RF-SH** – come per l'RF-LORA (6.6.1): nella scheda **Modules** → **RS485 modules** **RF-SH**, **Serial No.**, **Write [F5]**, USB scollegato, 1 minuto di attesa, USB ricollegato, **Read [F4]**; la comparsa della versione firmware è il segno del successo.
- **Rivelatori FW2** – premi il pulsante **LEARN** del modulo finché il LED **LEARN** lampeggia in verde. Inserisci la batteria del rivelatore e attendi che i suoi LED si spengano. Esci con il pulsante **LEARN**, USB, **Read [F4]**: il numero di serie a sette cifre deve coincidere con quello sull'involucro. Imposta la zona e l'area, **Write [F5]**. Cancellazione: **Device type** → **Disabled**.
- **Telecomando FW2** – tieni premuti insieme i pulsanti 3 e 4 finché il LED lampeggia in giallo e poi in verde. Nell'elenco imposta la sua area e il suo utente; la funzione dei pulsanti 3 e 4 (inserimento, disinserimento, panico silenzioso o sonoro) si sceglie nella tabella. Ripristino del telecomando: pulsanti 2 e 3 insieme, finché non vedi un lampeggio verde-rosso.
- **Sirena FW2** – accendi l'alimentazione della sirena; il lampeggiante lampeggia lentamente per 30 secondi. In questo tempo tieni premuto il pulsante **LEARN** sulla scheda della sirena finché il lampeggiante lampeggia velocemente, poi rilascialo. Ripristino: tenendo premuto il pulsante **LEARN**,

collega l'alimentazione, fino a tre lampeggi.

- **Rivelatori e tastiera SH** – inserisci la batteria; l'accensione del LED verde per 3 secondi indica la memorizzazione riuscita. Se non è riuscita, togli la batteria per 10 secondi e riprova.

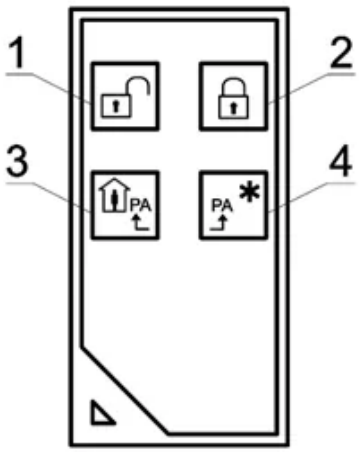


Figura 76. Telecomando Crow FW2: per la memorizzazione tieni premuti insieme i pulsanti 3 e 4.

6.7 Zones

Scheda **Zones settings**:

- **Zone No** – il numero d'ordine della zona.
- **Name** – il nome della zona.
- **Input** – quale ingresso **IN** della centrale o dell'espansione appartiene alla zona.
- **Area** – l'area della zona.
- **Definition** – il funzionamento della zona:
  - **Delay** – zona ritardata, per il contatto magnetico della porta d'ingresso. Per questo tipo di zona puoi impostare il tempo d'ingresso e d'uscita. Dopo l'inserimento, durante il tempo d'uscita la zona Delay si può violare liberamente (si può aprire la porta); se allo scadere del tempo d'uscita è ancora violata, si attivano le uscite **Siren** e **Flash** e parte la segnalazione d'allarme. A sistema inserito la violazione della zona Delay avvia il tempo d'ingresso, durante il quale va disinserito il sistema; se non lo disinserisci entro lo scadere del tempo d'ingresso, si attivano le uscite **Siren** e **Flash** e parte la segnalazione d'allarme.
  - **Interior** – zona a seguire, per il rivelatore di movimento vicino alla porta d'ingresso. A sistema inserito, alla sua violazione si attivano le uscite **Siren** e **Flash** e parte la segnalazione d'allarme. Se a sistema inserito viene violata prima la zona Delay, la zona Interior si può violare liberamente durante il tempo d'ingresso impostato; se durante il tempo d'ingresso non disinserisci il sistema, si attivano le uscite **Siren** e **Flash** e parte la segnalazione d'allarme.
  - **Interior Stay** – zona a seguire, per il rivelatore di movimento vicino alla porta d'ingresso; funziona come la Interior: a sistema inserito, alla sua violazione si attivano le uscite **Siren** e **Flash** e parte la segnalazione d'allarme, ma se prima è stata violata la zona Delay, si può violare liberamente durante il tempo d'ingresso. Con il sistema inserito in modalità STAY le zone Interior Stay non sono protette (la centrale non le sorveglia).
  - **Instant** – zona istantanea, per rivelatori di movimento. Se a sistema inserito la zona Instant viene violata, senza tempo d'ingresso si attivano subito le uscite **Siren** e **Flash** e parte la segnalazione d'allarme.

    - **Instant Stay** – zona istantanea, per rivelatori di movimento. Se a sistema inserito la zona Instant Stay viene violata, si attivano subito le uscite **Siren** e **Flash** e parte la segnalazione d'allarme. Con il sistema inserito in modalità STAY le zone Instant Stay non sono protette.
    - **Fire** – per rivelatori d'incendio. Alla violazione partono subito le uscite **Siren** e **Flash** e parte la segnalazione.
    - **Keyswitch** – per un interruttore a chiave o un altro interruttore: la zona inserisce e disinserisce. L'inserimento avviene dopo lo scadere del tempo d'uscita.
    - **24_hour** – per rivelatori di rottura vetri e antimanomissione. Sempre sorvegliata, alla violazione dà subito l'allarme: si attivano le uscite **Siren** e **Flash** e parte la segnalazione dell'evento.
    - **Silent** – a sistema inserito, alla violazione parte subito la segnalazione, ma le uscite **Siren** e **Flash** non si attivano.
    - **Silent 24h** – per il pulsante antipanico. Indipendentemente dallo stato del sistema parte subito la segnalazione dell'evento, senza sirena: le uscite **Siren** e **Flash** non si attivano.
- **Type** – il tipo di circuito collegato all'ingresso, dall'elenco: **NC** (normalmente chiuso), **NO** (normalmente aperto), **EOL** (con resistenza di fine linea), **EOL_T** (con resistenza di fine linea e supervisione antimanomissione), **ATZ** (due zone su un ingresso: due circuiti di zona normalmente chiusi con resistenze di fine linea, senza supervisione antimanomissione – per questo tipo seleziona nell'elenco **Input** anche la seconda zona ATZ), **ATZ_T** (due zone con supervisione antimanomissione: due circuiti di zona normalmente chiusi con resistenze di fine linea e supervisione antimanomissione – anche per questo seleziona la seconda zona ATZ nell'elenco **Input**), **3EOL** (con resistenza di fine linea e supervisione antimanomissione, per rivelatori di movimento con funzione antimascheramento – anti-masking). I valori delle resistenze si impostano nel campo **System Options** → **EOL Type** (6.2.1).
- **Chime** – campanello: all'apertura della zona la tastiera emette un bip.
- **Bypass** – la zona si può escludere.
- **Force** – inserimento forzato: il sistema si può inserire anche con la zona aperta; la zona aperta al momento dell'inserimento resta temporaneamente esclusa, dopo la sua chiusura (ripristino) è di nuovo sorvegliata e da quel momento la sua violazione provoca un allarme.
- **CMS** – gli eventi della zona vanno alla centrale di vigilanza.
- **Prot.** – gli eventi della zona vanno al cloud Protegus.
- **Delay** – il tempo di reazione dell'ingresso in millisecondi.
- **CID code** – il codice Contact ID dell'evento, si compila automaticamente alla scelta della definizione.
- **Sound** – il numero del messaggio vocale che la centrale riproduce in caso di allarme all'utente chiamato (solo SP3_12xx, firmware fino alla 1.13).

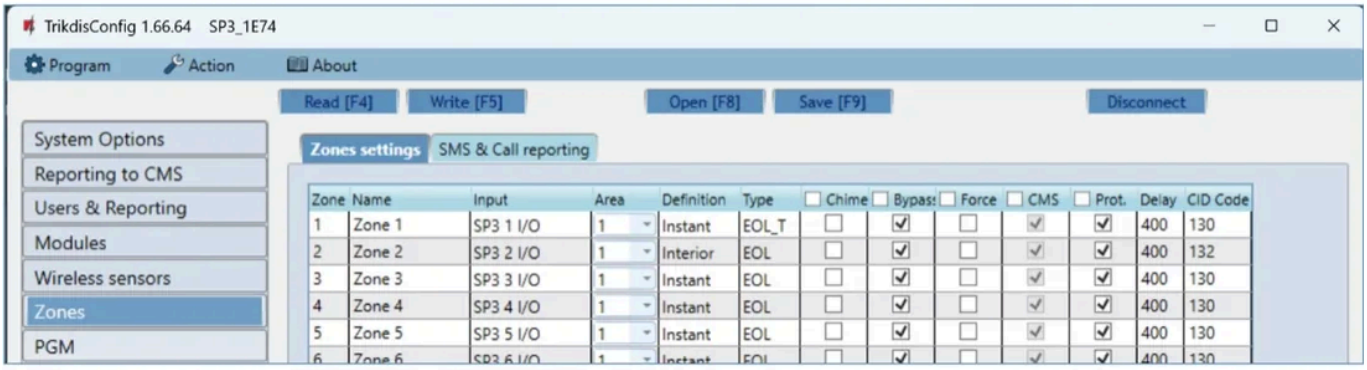


Figura 77. Zones → Zones settings: definizione, tipo di circuito e opzioni delle zone.

Scheda **SMS & Call reporting** – visibile solo se nella finestra **Users & Reporting** c'è almeno un numero di telefono.

- **Zn** – il numero della zona e il tipo di evento: **Event** (allarme) o **Restore** (ripristino).

- **User / SMS and Call** – per ogni utente spunti se deve ricevere un SMS e/o una chiamata sull'evento della zona.

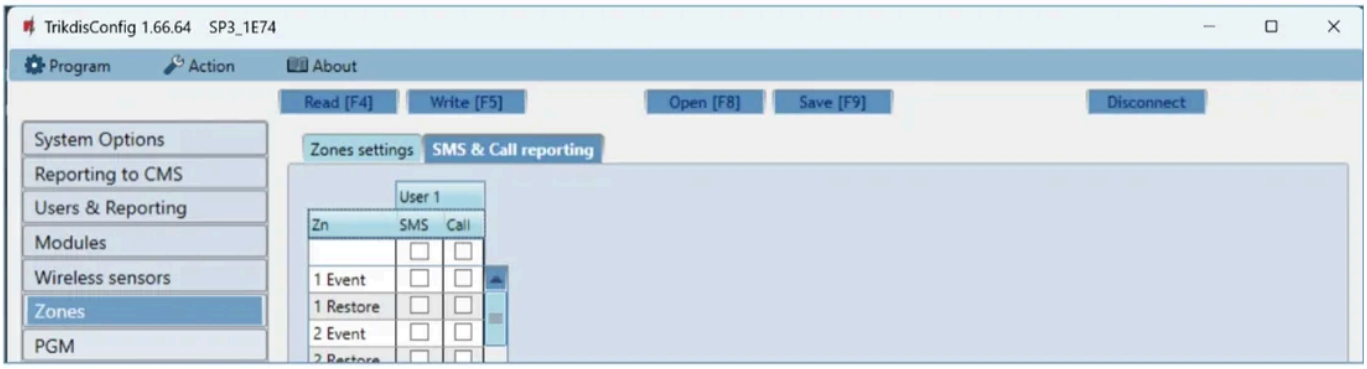


Figura 78. Zones → SMS & Call reporting: chi riceve un SMS o una chiamata sugli eventi delle singole zone.

6.8 PGM

Scheda **Outputs**:

- **PGM No** – il numero d'ordine dell'uscita PGM.
- **Name** – il nome dell'uscita.
- **PGM output** – quale uscita **OUT** della centrale o di un'espansione appartiene alla PGM.
- **Area** – l'area dell'uscita.
- **Output definition** – il funzionamento dell'uscita:
  - **Siren** – per la sirena.
  - **Remote control** – per comandare un dispositivo esterno (dall'app, via SMS, con chiamata, con lettore).
  - **Fire Sensor Reset** – per il reset dei rivelatori d'incendio dopo un allarme.
  - **System State** – per un indicatore di stato, ad esempio un LED mostra se il sistema è inserito.
  - **Flash** – per un lampeggiante: segnale continuo a sistema inserito, a impulsi in caso di allarme, cessa al disinserimento.
  - **Thermostat** – modalità termostato. Serve un sensore di temperatura sulla centrale, la temperatura da mantenere si imposta nella scheda **Thermostat**.
  - **Buzzer** – ripete le segnalazioni acustiche della tastiera.
- **Pulse time, s** – il tempo di attivazione nel funzionamento a impulsi, 0–9999 s.
- **CMS**, **Prot.** – sull'accensione e lo spegnimento dell'uscita va una segnalazione alla centrale di vigilanza, rispettivamente al cloud Protegus.

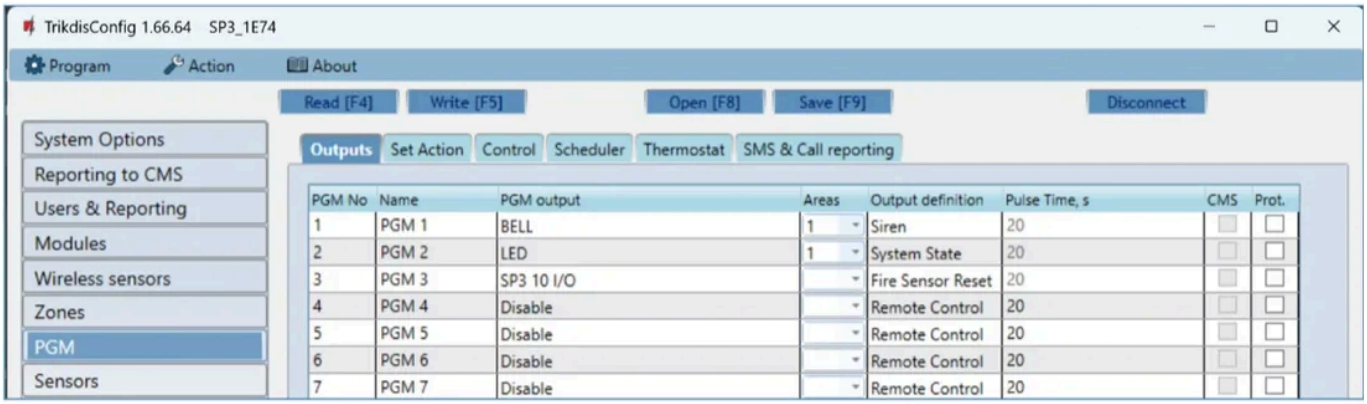


Figura 79. PGM → Outputs: definizione e durata dell'impulso delle uscite.

Scheda **Set Action** – cosa comanda l'uscita:

- **ID** – il numero della riga.
- **Enable** – abilitazione della regola.
- **PGM No.** – l'uscita comandata, attivata dall'evento descritto nelle colonne **Factor**, **Factor No.**, **Start when** e **Set value**.
- **Action** – **PGM OFF** (spegne), **PGM ON** (accende), **Pulse OFF** (normalmente accesa, spenta per il tempo **Pulse time**), **Pulse ON** (normalmente spenta, accesa per il tempo **Pulse time**).
- **Pulse time, s** – 0–9999 s.
- **Factor**, **Factor No.** – l'evento scatenante e il suo numero: **Zone**, **Sensor**, **Jamming**, **Sensor lost**, **iButton**, **Arm**, **Disarm**, **SMS received**, **Zone(follow)**, **Stay**, **Sleep**, **AC lost**, **Low battery**, **Zone tamper**. All'uscita si può assegnare anche una programmazione oraria – la programmazione indica quando l'uscita deve essere accesa; nella scheda **Scheduler** se ne possono creare al massimo dieci diverse.
- **Start when** – ulteriore condizione per l'evento scatenante.
- **Set value** – il valore che dipende dalla condizione: testo dell'SMS ricevuto, tensione o temperatura. Se la centrale riconosce questo valore, esegue l'operazione scelta nella colonna **Action**. Per gli SMS la parola chiave che comanda l'uscita si separa dal resto del messaggio ricevuto con i segni `%`: `%testo%` – il messaggio contiene il testo (ad esempio `%hoUSe%`: nel messaggio c'è "hoUSe", come nel messaggio `VacationhoUSe25864`); `testo%` – il messaggio inizia con questo (ad esempio `hoUSe%`: il messaggio inizia con "hoUSe", come `hoUSeddss`); `%testo` – il messaggio finisce con questo (ad esempio `%hoUSe`: il messaggio finisce con "hoUSe", come `1144hoUSe`). Il testo distingue tra maiuscole e minuscole.

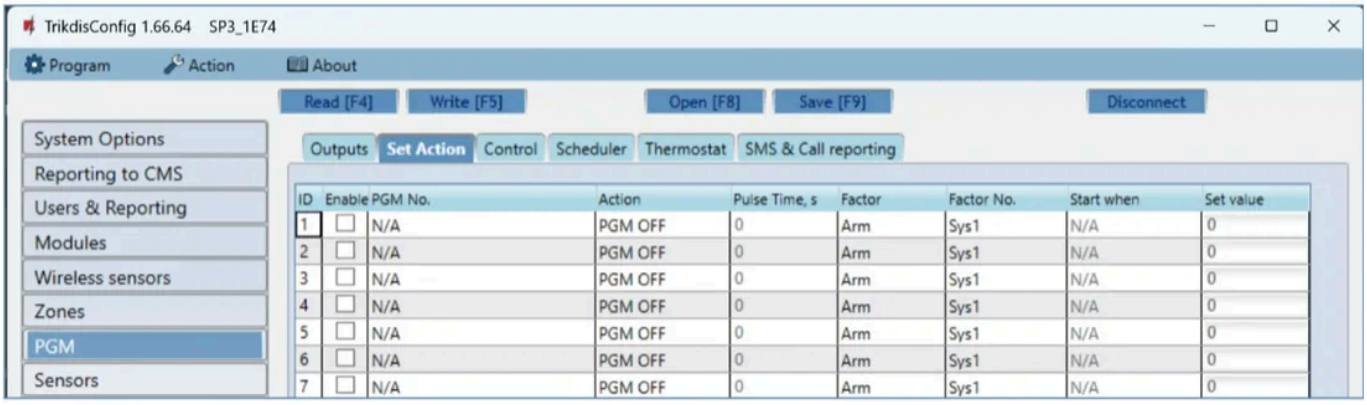


Figura 80. PGM → Set Action: uscite comandate da un evento, da un SMS o da un valore.

Scheda **Control**:

- Gruppo **Entry/Exit control**: **Reader** – i lettori collegabili (iButton, Wiegand 1 sul morsetto **G/Y**, Wiegand 2 sul morsetto **IO**); **En** – il lettore può comandare un'uscita; **Code** – l'operazione si può eseguire anche con un codice utente (comando dell'uscita PGM o controllo della centrale); **PGM** – l'uscita comandata (deve essere in modalità **Remote control**); **PGM mode** – **Pulse** o **Level**; **Area action** – cosa deve succedere allo stato di inserimento del sistema quando si avvicina una chiave o una tessera al lettore.
- Gruppo **Paradox keypad control**: **Utility key** – tenendo premuto per 3 secondi il tasto ausiliario della tastiera l'uscita commuta: per il tempo dell'impulso (**Pulse**) o cambiando stato (**Level**).

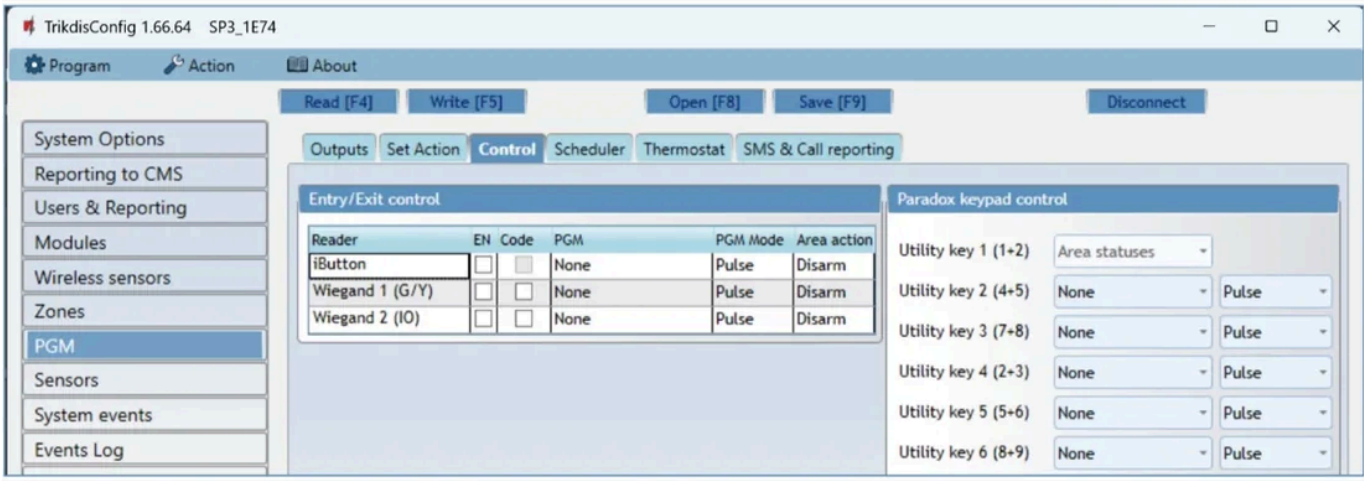


Figura 81. PGM → **Control**: comando delle uscite da lettori e tasti delle tastiere Paradox.

Scheda **Scheduler** – **ID**, **Enable**, **Start time** (accensione), **Stop time** (spegnimento), **Mon – Sun** (giorni).

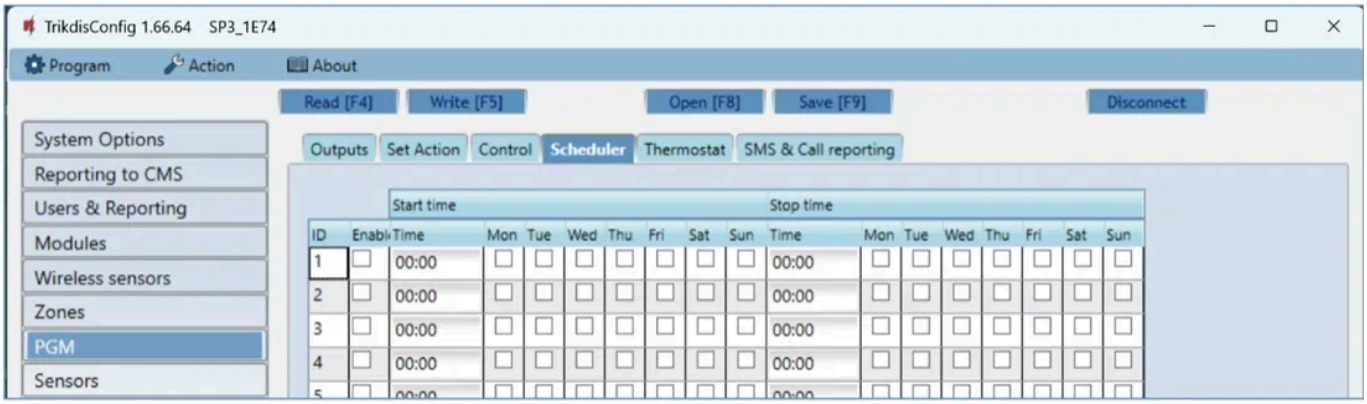


Figura 82. PGM → **Scheduler**: temporizzazione delle uscite, al massimo dieci programmazioni.

Scheda **Thermostat** – **ID**; **PGM No.** (l'uscita comandata); **Action** (riscaldamento o raffreddamento); **Active** (il termostato funziona con il sensore selezionato); **Sensor No** (il sensore di temperatura); **Temperature** (la temperatura da mantenere).

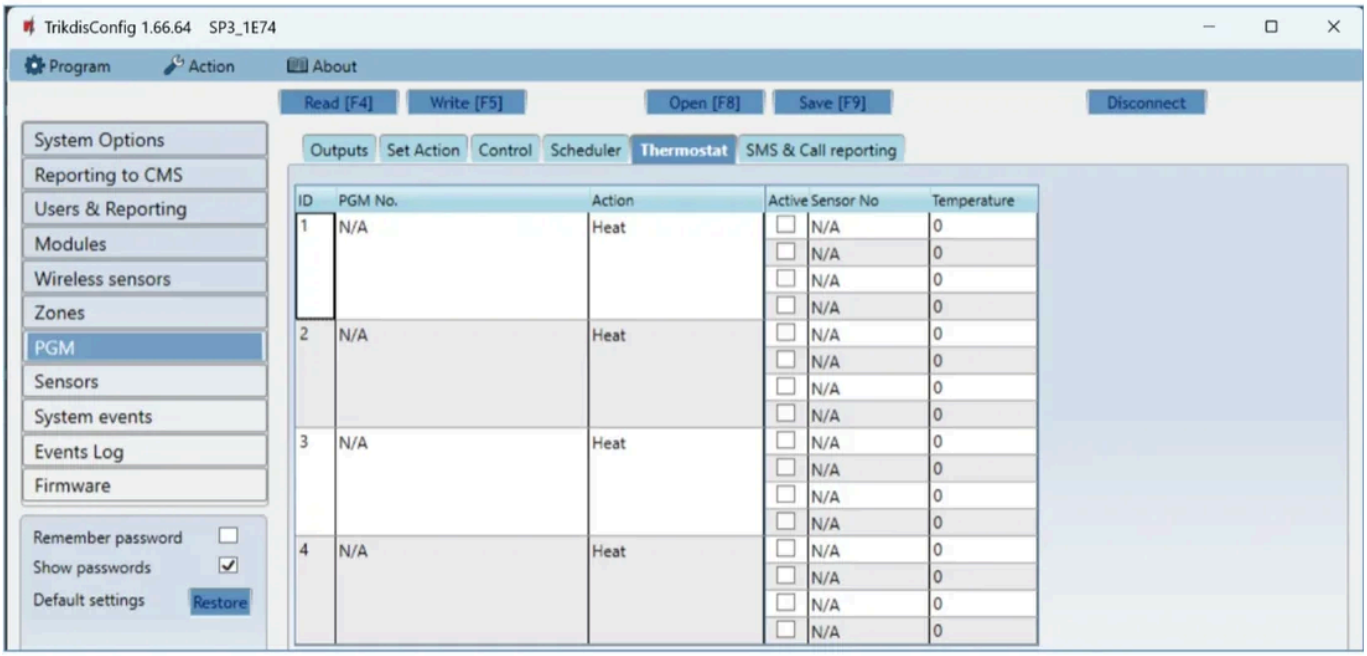


Figura 83. PGM → **Thermostat**: uscita per la regolazione della temperatura.

Scheda **SMS & Call reporting** – visibile solo se c'è un numero di telefono utente, e impostabile solo per i primi otto utenti. **PGM** – il numero dell'uscita e il tipo di evento (**Event** – accensione, **Restore** – spegnimento); **User / SMS and Call** – chi riceve un SMS e/o una chiamata.

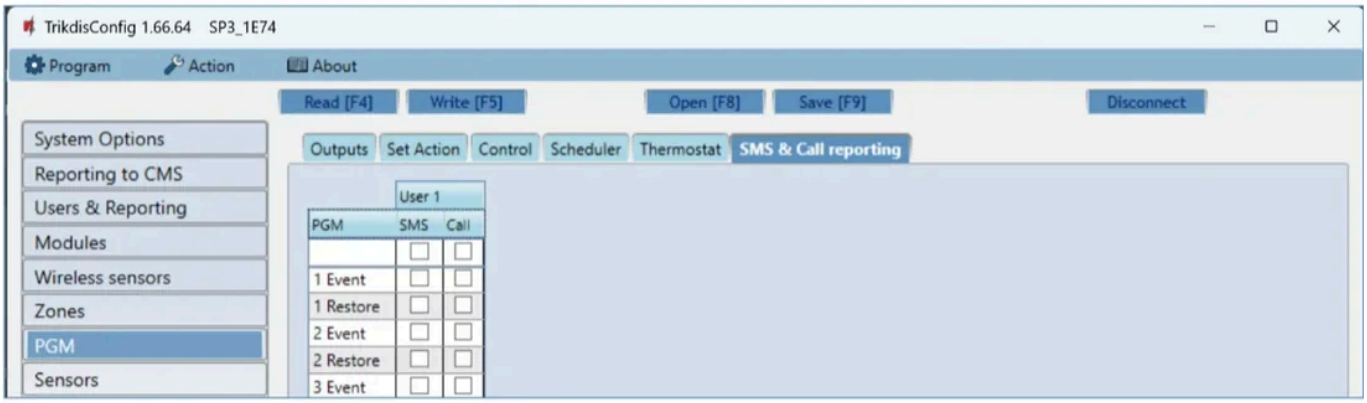


Figura 84. PGM → SMS & Call reporting: notifica sulla commutazione delle uscite.

6.9 Sensors

- **ID** – il numero d'ordine del sensore di temperatura.
- **Module type** – il sensore assegnato all'identificativo.
- **Serial No.** – il numero di serie del sensore collegato alla centrale.
- **Sensor name** – il nome del sensore.
- **Max** – a una temperatura superiore a questa viene generato un evento, se **High** è spuntato.
- **Min** – a una temperatura inferiore a questa viene generato un evento, se **Low** è spuntato.
- **Delay, min** – l'evento viene inviato solo se il superamento del valore limite persiste per questi minuti.
- **Sensor type** – **Dallas 1-Wire**: al massimo otto sensori, riconosciuti automaticamente; **Humidity & Temperature (AM23xx series)**: un sensore di umidità e temperatura AM2301, da selezionare manualmente nella colonna **Module type**.

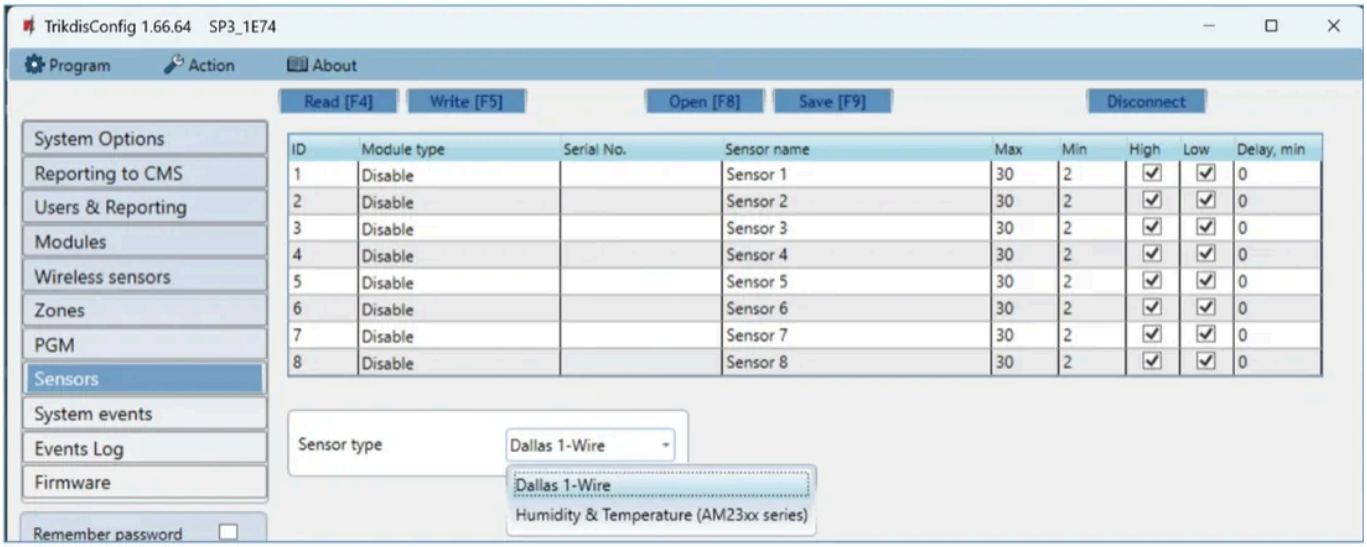


Figura 85. La finestra **Sensors**: valori limite dei sensori di temperatura. La colonna dei numeri di serie è lasciata vuota nella figura.

6.10 System events

Scheda **Events**:

- **ID** – il numero d'ordine dell'evento.

- **Event name** – il nome dell'evento.
- **Enable** – sorveglianza e segnalazione dell'evento.
- **CMS**, **Prot.** – segnalazione alla centrale di vigilanza, rispettivamente al cloud Protegus.
- **CID Code** – il codice Contact ID dell'evento.
- **SMS event text**, **SMS restore text** – il testo SMS dell'evento e del ripristino.

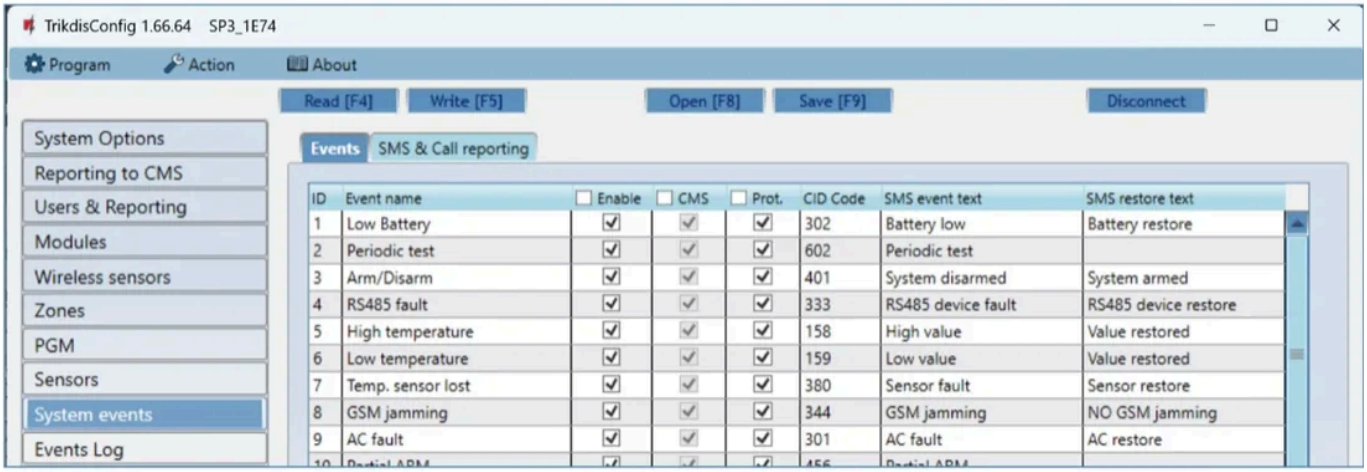


Figura 86. System events → Events: codice, destinazione e testo SMS degli eventi di sistema.

Scheda **SMS & Call reporting** – visibile solo con un numero di telefono utente. **ID** – il numero e il tipo dell'evento (**Event**, **Restore**); **Event SMS text** – il testo dell'SMS; **User / SMS and Call** – chi riceve un SMS e/o una chiamata.

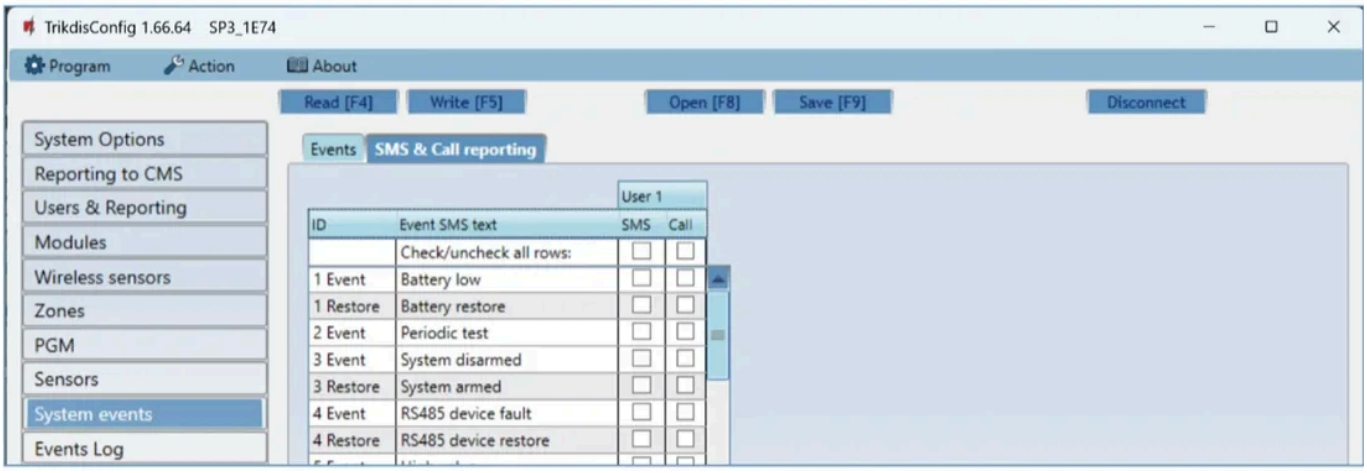


Figura 87. System events → SMS & Call reporting: notifica sugli eventi di sistema.

6.11 Events log

- **Read Log** – lettura del registro eventi dalla memoria della centrale.
- **Clear Log** – cancellazione del registro.
- Le colonne della tabella: **Event No.**, **Time**, codice **CID**, **Event definition**. Il registro mostra al massimo 1000 eventi.

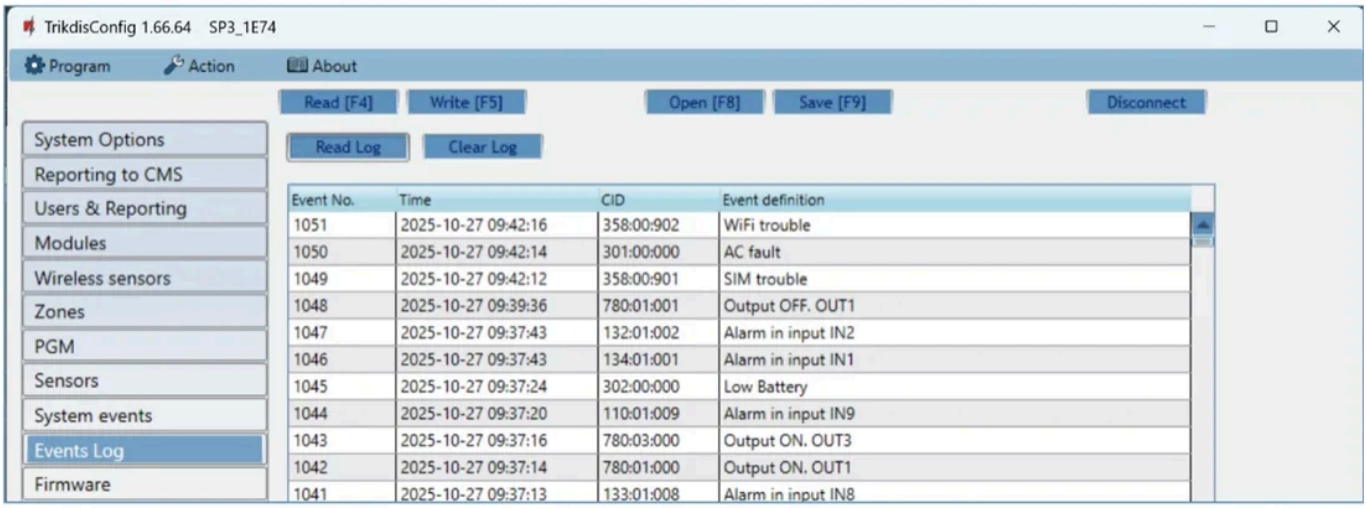


Figura 88. La finestra **Events log**: gli ultimi 1000 eventi della centrale.

Ricerca guasti dal registro

In caso di allarme contestato, leggi per prima cosa il registro: si vede quale zona ha segnalato, quando e con quale codice, e se la segnalazione è stata inviata.

6.12 Ripristino delle impostazioni di fabbrica

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

Con il codice installatore è possibile solo se l'amministratore non lo ha disabilitato nella scheda **System Options** → **Access** (6.2.6).

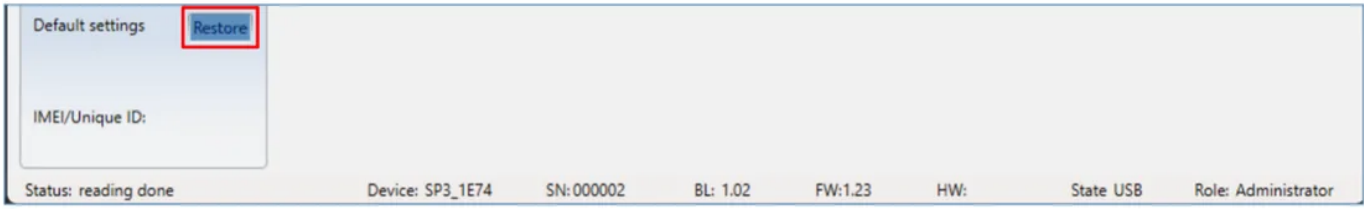


Figura 89. Il pulsante **Restore** del gruppo **Default settings** in basso a sinistra ripristina le impostazioni di fabbrica.

Dopo il ripristino

I codici tornano al valore di fabbrica (6.2.6), il PIN della SIM, l'APN, i dati WiFi, gli utenti e le zone vengono cancellati. Se prima hai salvato l'impostazione su file (**Save [F9]**), puoi ricaricarla con i pulsanti **Open [F8]** e **Write [F5]**.

7. Programmazione a distanza

TrikdisConfig raggiunge la “FLEXi” SP3 non solo tramite cavo USB, ma anche **a distanza, tramite il cloud Protegus**: puoi modificare le impostazioni della centrale già installata, leggere il registro eventi e perfino aggiornare il firmware senza recarti sul posto.

Per l'accesso a distanza serve:

1. La centrale deve essere accesa e avere una connessione di rete: il LED **PWR** lampeggia in verde, con la rete mobile il LED **NET** è acceso verde, con il Wi-Fi il LED **MOD**, con l'Ethernet il LED **ETH** è acceso verde (paragrafo 1.6). Nella versione con modem la scheda SIM è attiva e la richiesta del PIN è disattivata oppure il PIN è stato inserito.
2. Il **cloud Protegus** deve essere abilitato – impostalo nella finestra **Users & Reporting**, alla prima messa in servizio via USB (paragrafo 6.4).
3. Devi conoscere l'**identificativo univoco** della centrale (**IMEI / Unique ID** – si legge sull'etichetta della scheda e del contenitore, oltre che nella barra di stato di TrikdisConfig) e il codice amministratore o installatore.

Passaggi:

1. Avvia il software TrikdisConfig.
2. Nella sezione **Remote access** scrivi nel campo **Unique ID** l'identificativo univoco della centrale.
3. Se vuoi, dai un nome al sistema nel campo **System name** – il programma lo ricorda e la volta successiva puoi sceglierlo dall'elenco a tendina.
4. Premi il pulsante **Configure**.
5. Nella finestra che si apre fai clic sul pulsante **Read [F4]** e inserisci il codice amministratore o installatore. Con la spunta **Remember password** il programma lo ricorda.
6. Effettua le modifiche, poi inviale alla centrale con il pulsante **Write [F5]**.

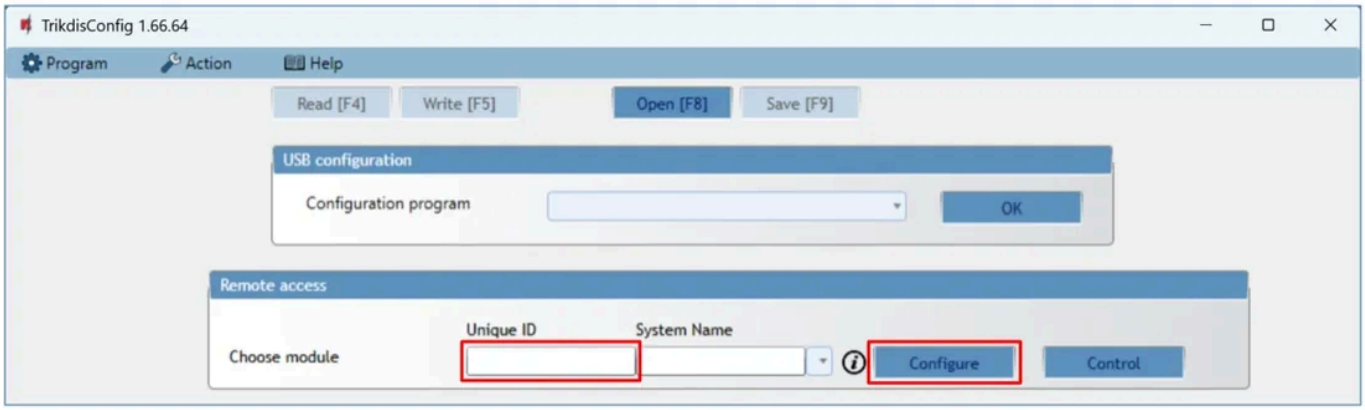


Figura 90. TrikdisConfig – Remote access: il campo Unique ID, il System name e il pulsante Configure.

Anche dall'app Protegus 2 si può avviare la programmazione a distanza con la password dell'installatore; per le impostazioni dettagliate serve però TrikdisConfig. La connessione remota sulla rete mobile comporta traffico dati – con l'aggiornamento del firmware anche diversi megabyte.

8. Verifica del funzionamento del sistema

Dopo il collegamento e la programmazione verifica sempre l'intera catena: rivelatore → centrale → centrale di vigilanza e/o Protegus 2.

1. **Guarda i LED.** Il LED **PWR** deve lampeggiare in verde senza lampeggi rossi, il LED di rete (**NET**, **MOD** o **ETH**) deve essere acceso verde, il LED **DAT** deve spegnersi dopo l'invio degli eventi (paragrafo 1.6). Se il PWR lampeggia in rosso, cerca il guasto secondo il capitolo 10.
2. **Genera un evento.** Inserisci e poi disinserisci il sistema dalla tastiera, oppure, a sistema inserito, viola una zona per generare un allarme.

3. **Verifica la ricezione.** L'evento deve comparire nel software della centrale di vigilanza e/o nell'elenco eventi dell'app Protegus 2 – con il numero di area, zona e utente corretto. Anche nel registro della centrale (**Events log**, paragrafo 6.11) puoi vedere se l'evento è stato generato e se è stato inviato.
4. **Zone una per una.** Viola in sequenza tutte le zone (apertura, movimento, pulsante di test del rivelatore di fumo, manomissione) e controlla che sulla tastiera e in Protegus 2 segnali la zona giusta.
5. **Uscite.** Comanda a distanza le uscite PGM da Protegus 2 e verifica che il dispositivo collegato (sirena, spia luminosa, relè) entri davvero in funzione.
6. **Inserimento a distanza.** Se il sistema viene controllato anche a distanza, inseriscilo e disinseriscilo anche dall'app Protegus 2 e osserva se lo stato della tastiera lo segue.
7. **Mancanza di alimentazione.** Scollega l'alimentazione di rete: la centrale deve continuare a funzionare con la batteria e devono arrivare l'evento **AC Fault** e, dopo il ripristino, l'evento **AC Restore** (paragrafo 2.2).

Di fabbrica la centrale non trasmette alla centrale di vigilanza (paragrafo 6.3), mentre il cloud Protegus è attivato di fabbrica. Se la centrale di vigilanza non riceve eventi, controlla prima le impostazioni di **Reporting to CMS** e i 4 / 5 lampeggi del LED PWR.

9. Aggiornamento del firmware

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

Quale file scegliere?

Il nome del file firmware è **SP3_yxxz_NNNN.fw** (paragrafo 1.7). La cifra **y** è la versione hardware: si può caricare solo il file della versione propria della centrale, con un'altra versione il programma segnala un errore. La cifra **z** è il tipo di rivelatori senza fili – **4** per i rivelatori MAXIMUM (RF-LORA) e S8 (RF-S8), **1** per il Paradox RTX3 –, sceglila in base all'installazione; da essa dipende anche il numero di zone gestibili (32 o 64). Le regole di scelta sono descritte nell'articolo FLEXi SP3 firmware: come scegliere quello giusto?.

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.

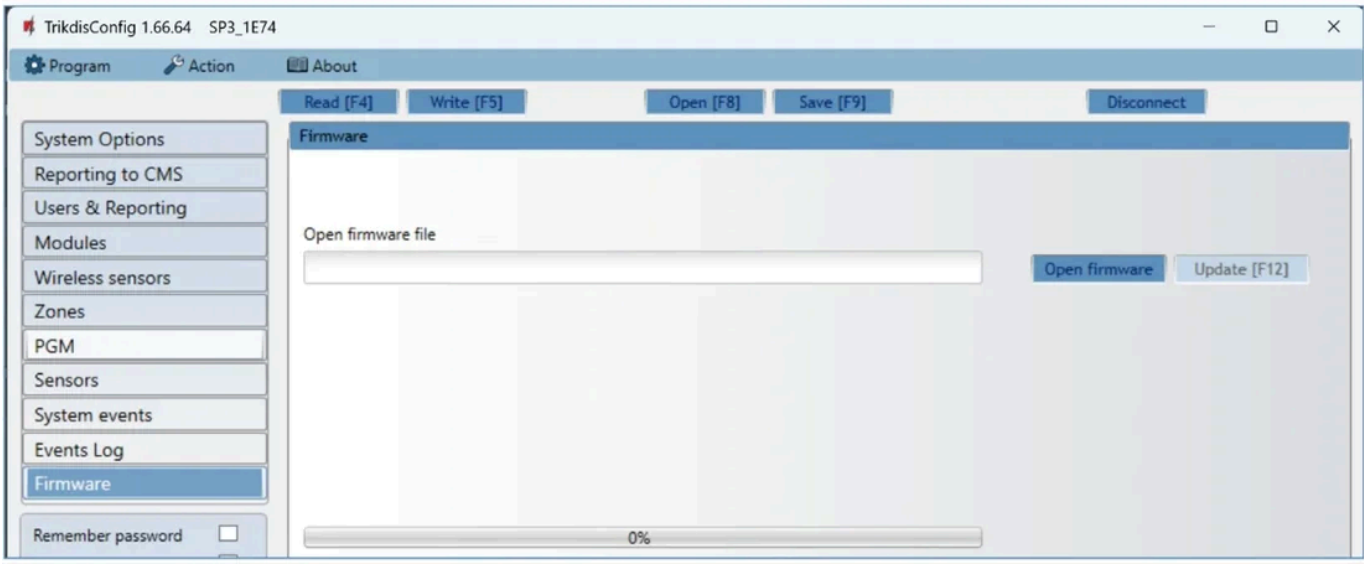


Figura 91. TrikdisConfig – pagina Firmware: Open firmware e Update [F12].

Dopo la connessione, TrikdisConfig propone automaticamente l'aggiornamento del firmware, se ce n'è uno più recente; per questo serve una connessione Internet. Un antivirus o un firewall possono impedire il download automatico del firmware; in tal caso consenti TrikdisConfig, oppure scarica il file manualmente (dopo la registrazione, dal sito di Trikdis) e aprilo nella pagina Firmware. Alla fine dell'aggiornamento fai clic sul pulsante **Write [F5]** e solo dopo scollega il cavo USB.

10. Ricerca guasti e domande frequenti

Le domande e i guasti più frequenti, partendo dai LED della scheda (il significato dei LED è nel paragrafo 1.6). Se la risposta rimanda al capitolo dettagliato, lì trovi la posizione esatta dell'impostazione.

Il LED PWR lampeggia in rosso – cosa significa il numero di lampeggi?

Durante il funzionamento normale il LED **PWR** lampeggia in verde. In caso di guasto lampeggia in rosso, e il numero di lampeggi dice qual è il problema:

Lampeggi	Guasto	Dove cercare
1	scheda SIM assente	nano-SIM nello slot, contatto (2.4, 6.2)
2	codice PIN della scheda SIM errato	il PIN nella pagina **System Options**, oppure disattiva la richiesta del PIN in un telefono (6.2)
3	impossibile connettersi alla rete mobile	antenna, intensità del segnale (lampeggi gialli del LED **NET**: 0–5, 3 sono già sufficienti), la SIM è attiva?
4	nessuna connessione con il ricevitore della centrale di vigilanza sul canale 1	**Reporting to CMS**: indirizzo, porta, TCP/UDP, chiave di crittografia, identificativo dell'impianto (6.3)
5	nessuna connessione con il ricevitore della centrale di vigilanza sul canale 2	lo stesso per il ricevitore di riserva (6.3)
6	l'orologio interno non è impostato	impostazione dell'ora nella pagina **System Options** (6.2)
7	la tensione dell'alimentazione di riserva non è sufficiente	batteria e capicorda, età della batteria, corrente di carica (2.2)

Lampeggi	Guasto	Dove cercare
8	manca l'alimentazione di rete (AC)	alimentatore, interruttore automatico, morsetto dell'alimentazione principale (2.1)
9	impossibile connettersi alla rete Wi-Fi	nome e password della rete, rete a 2,4 GHz (vedi la domanda successiva)

La centrale non trova la rete Wi-Fi

1. Il modulo Wi-Fi della “FLEXi” SP3 si collega **solo a reti a 2,4 GHz** (802.11 b/g/n, WPA / WPA2). Non vede le reti a 5 GHz; se il router usa un nome comune per le due bande, la banda a 2,4 GHz deve essere attiva.
2. Controlla il nome e la password della rete nella pagina **System Options** (6.2), e che il router non filtri i dispositivi in base all'indirizzo MAC.
3. Il LED **MOD** lampeggia in verde mentre si connette, e resta acceso verde fisso quando la connessione è stabilita.
4. In un contenitore metallico il segnale Wi-Fi può essere debole: la centrale funziona in modo affidabile con un'antenna fuori dal contenitore, con un router vicino al contenitore o con un segnale più forte.

La rete c'è, ma in Protegus 2 non arrivano eventi

1. Il LED **DAT** è acceso giallo se in memoria ci sono messaggi non inviati: in tal caso il guasto è la connessione, non l'impostazione. Guarda il LED **NET** / **MOD** e i lampeggi del PWR.
2. La connessione verso il cloud Protegus è abilitata di fabbrica; se è stata disattivata, riattivala con la casella **Enable cloud service** nella scheda **Users & Reporting** → **Protegus** (6.4.3). Nella scheda **Reporting to CMS** → **Settings** si imposta solo su quale via (SIM, Wi-Fi, LAN) passa il traffico Protegus.
3. Nella pagina **System events** l'invio dell'evento in questione deve essere abilitato (6.10) – ciò che qui è disabilitato, la centrale non lo invia su nessun canale.
4. Il dispositivo è collegato all'account Protegus 2 (5.1)? Per aggiungere un nuovo sistema serve l'identificativo univoco del dispositivo.

La centrale di vigilanza non riceve eventi

1. La trasmissione alla centrale di vigilanza è **disattivata di fabbrica**; va attivata nella pagina **Reporting to CMS** inserendo i dati del ricevitore (6.3).
2. 4 o 5 lampeggi rossi del LED PWR indicano che sul canale 1 o sul canale 2 non c'è connessione con il ricevitore: indirizzo, porta, protocollo (TCP/UDP), chiave di crittografia, identificativo dell'impianto.
3. Se sono impostati sia la centrale di vigilanza sia Protegus 2, l'evento va prima al ricevitore, poi all'utente – un evento che compare in Protegus 2 non significa quindi che l'abbia ricevuto anche il ricevitore.

Quale firmware devo caricare? Cosa significano i numeri nel nome del file?

Il nome del file firmware è `SP3_yxxz_NNNN.fw`. Il **primo** numero (y) è la versione hardware – 1: Wi-Fi + 4G, 2: Wi-Fi, 3: LAN / LAN + Wi-Fi, 5: Wi-Fi + 2G, 6: LAN + 4G –, non si può cambiare durante l'aggiornamento; TrikdisConfig segnala se hai scelto un file non adatto all'hardware. L'**ultimo** numero (z) indica il tipo di ricevitore radio e quindi il numero di zone: 0 RF-SH (32 zone), 1 Paradox RTX3 (32), 2 Honeywell (64, non usato in Europa), 4 rivelatori MAXIMUM (RF-LORA) o S8 (RF-S8) (64; per le espansioni LORA non serve). Questo si può cambiare: per un altro ricevitore serve un firmware con un altro numero z (1.7 e capitolo 9). Il numero a quattro cifre alla fine è la versione; come regola generale usa la più alta.

Quante zone posso avere, e da cosa dipende?

Sulla scheda ci sono **10** morsetti IO, ciascuno può essere una zona (ingresso) o un'uscita PGM. Con il raddoppio zone (ATZ) si possono collegare due rivelatori a un morsetto, quindi **20** zone. Con tastiere, espansioni della serie iO e LORA, oltre a un ricevitore radio, il numero di zone si espande **a 32 o a 64** – quale dei due lo decide l'ultimo numero del firmware (domanda precedente). Il numero di aree è 8.

Sostituisco una vecchia centrale – devo cambiare le resistenze dei rivelatori?

No. Nella "FLEXi" SP3 il valore delle resistenze di fine linea è impostabile, quindi i rivelatori esistenti possono restare con le resistenze usate per la vecchia centrale. Il tipo di zona (NC, NO, EOL, 3EOL, ATZ) e i valori delle resistenze si impostano nella pagina **Zones** (3.2 e 6.7).

Vorrei collegare a un'uscita un carico maggiore (sirena, serratura, cancello)

Il morsetto IO, come uscita, è open collector e sopporta **al massimo 100 mA** – direttamente si possono collegare solo una spia luminosa o la bobina di un piccolo relè. Per carichi maggiori usa un relè secondo il paragrafo 3.8. L'uscita **BELL** sopporta 1 A, l'uscita **AUX** fornisce ai dispositivi esterni al massimo 1 A a 12 V DC – somma l'assorbimento di tastiere, espansioni e rivelatori dalla tabella 1.4 e non superarlo.

Quale tastiera posso usare, e quante?

La centrale supporta le tastiere Trikdis FLEXi / SK e le tastiere Paradox e Crow elencate (l'elenco e gli assorbimenti sono nel paragrafo 1.4). Su un bus **al massimo 8 tastiere**, e devono essere **dello stesso tipo**. Le tastiere a LED gestiscono solo le prime due aree; per più aree serve una tastiera LCD. La tastiera FLEXi LCD memorizza quattro lingue contemporaneamente; se l'italiano non è tra queste, occorre aggiornare il firmware della tastiera: https://trikdis.it/processo-di-aggiornamento-firmware-della-tastiera-flexi-lcd .

Vorrei usare un ricevitore Paradox RTX3

Per l'RTX3 l'ultimo numero del firmware deve essere **1** (`SP3_xxx1_NNNN.fw`); il file si trova nella cartella di installazione di TrikdisConfig, nella sottocartella `Firmwares\SP3\RTX3`, la procedura di aggiornamento è nel capitolo 9. Dopo la sostituzione, la pagina **Wireless** segnala se non è ancora registrato un RTX3. La frequenza dell'RTX3 e dei dispositivi senza fili deve coincidere (433 o 868 MHz) – verificalo prima dell'acquisto. Dettagli: https://trikdis.it/flexi-sp3-modulo-di-espansione-wireless-paradox-rtx3 .

La centrale non risponde ai comandi SMS

1. Via SMS e con chiamata telefonica si possono controllare solo le versioni **con modem** (2G / 4G); le centrali solo Wi-Fi e solo Ethernet no.
2. La struttura del messaggio e l'elenco dei comandi sono nel paragrafo 5.3; la password SMS di fabbrica è `123456`, che conviene cambiare subito nel gruppo **System Options** → **Access** (6.2).
3. Con chiamata e SMS può controllare solo l'utente il cui numero di telefono è presente nell'elenco utenti della pagina **Users & Reporting** (6.4).

Cosa devo impostare in ogni caso alla prima messa in servizio?

Con le impostazioni di fabbrica funziona la maggior parte dei sistemi piccoli e medi, ma non saltare questi punti: la modifica del **codice master** e dei codici di accesso installatore / amministratore (6.2, 6.4), l'impostazione dell'**ora** (6.2), il tipo e le resistenze delle zone (6.7), gli utenti e i loro numeri di telefono (6.4), i dati del ricevitore della centrale di vigilanza, se presente (6.3), e il collegamento del sistema all'account Protegus 2 (5.1). Alla fine esegui la verifica del capitolo 8.

11. Garanzia e 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.

11.1 Garanzia e limitazione di responsabilità

La centrale d'allarme è coperta da una garanzia di **24 mesi** dalla data di acquisto; durante questo periodo il produttore ripara gratuitamente i difetti a lui imputabili. Condizione della garanzia è che la centrale sia installata da una persona qualificata in conformità a questo manuale e alle norme relative alle apparecchiature elettriche, e che anche l'esercizio avvenga secondo queste. Per la riparazione la centrale va spedita nell'imballaggio del produttore, con la descrizione del difetto riscontrato; dopo la scadenza della garanzia la manutenzione e la riparazione si possono richiedere a pagamento.

La garanzia decade anticipatamente se

- la centrale è stata riparata o si è tentato di ripararla da parte di una persona non autorizzata;
- è stata usata per scopi diversi da quelli previsti;
- è stata conservata o installata in un luogo non adatto (condizioni climatiche non idonee, ambiente chimicamente aggressivo);
- ha subito danni meccanici o è stata danneggiata intenzionalmente;
- è stata danneggiata da forza maggiore (ad esempio un fulmine).

Il produttore non risponde

- del funzionamento difettoso della centrale, se non è stata installata o usata secondo il manuale;
- del funzionamento difettoso della centrale, se la causa è un guasto o un'interruzione della connessione di rete mobile o Internet, oppure un guasto della rete dell'operatore;
- della limitazione, cessazione o interruzione del servizio di rete mobile o Internet, oppure della fornitura di energia elettrica, e dei danni patrimoniali o non patrimoniali che ne derivano;
- dei danni patrimoniali o non patrimoniali subiti dall'acquirente o dall'utente a causa di rapina, effrazione, furto, incendio o altro evento dannoso.

11.2 Norme di sicurezza

- Prima di usare la centrale leggi questo manuale. La “FLEXi” SP3 è un'apparecchiatura elettrica: può essere installata e sottoposta ad assistenza solo da una persona qualificata, nel rispetto del manuale e delle norme relative all'installazione delle apparecchiature elettriche.
- **Durante l'installazione la centrale deve essere priva di tensione**; prima di ogni collegamento e intervento di assistenza scollegala dall'alimentazione: dalla rete con l'interruttore automatico, dalla batteria staccando i capicorda.

- Monta la centrale in un luogo inaccessibile ai non autorizzati, a distanza di sicurezza dalle apparecchiature elettroniche sensibili. La scheda non resiste a vibrazioni, sollecitazioni meccaniche, umidità e ambienti chimicamente aggressivi; corrisponde alla classe ambientale II della norma EN 50131.
- Il contenitore, il trasformatore, la batteria e il dispositivo di programmazione devono soddisfare i requisiti di sicurezza della EN 60950.
- La centrale funziona dalla rete 230 V, 50 Hz tramite un trasformatore riduttore di Classe II (16–18 V AC) o da un alimentatore 16–24 V DC; come alimentazione di riserva serve una batteria da 12 V con capacità di almeno 7 Ah. L'assorbimento dipende dai dispositivi esterni collegati (paragrafo 2.1).
- Nel circuito di alimentazione si deve installare un interruttore automatico bipolare con una distanza di almeno 3 mm tra i contatti aperti; l'interruttore deve trovarsi in un punto noto e accessibile al tecnico che esegue l'assistenza sulla centrale.
- I guasti derivanti da installazione o uso non corretti, nonché le modifiche e le riparazioni non autorizzate dal produttore, invalidano la garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare il dispositivo guasto, la batteria e i componenti nei rifiuti domestici.

Vedi anche

- FLEXi SP3 firmware: come scegliere quello giusto? – il significato del codice hardware e del codice ricevitore, quale firmware per quale sistema.
- FLEXi SP3 + modulo di espansione senza fili Paradox RTX3 – rivelatori senza fili Paradox con l'SP3.
- Ricetrasmettitore RF-S8 e rivelatori S8 – manuale di installazione e accoppiamento – i dispositivi senza fili S8 con l'SP3: collegamento, firmware, accoppiamento.
- Controllo accessi flessibile e senza fili con il sistema GATOR RF-LoRa – i moduli RF-LORA e iO-LORA in un sistema.
- La Trikdis FLEXi SP3 ha ottenuto la certificazione GRADE 3 – cosa significa la certificazione.
- Trikdis FLEXi SP3 – presentazione della centrale d'allarme intelligente – presentazione della centrale, sostituzione di una vecchia centrale.
- La procedura di aggiornamento del firmware della tastiera FLEXi LCD – le lingue della tastiera e il suo aggiornamento.
- Tastiera Trikdis FLEXi Keypad SK-LED button – breve manuale utente e tastiera SK-LCD button – breve manuale utente – per l'utente.
- Inserimento a distanza con interruttore a chiave dall'app Protegus 2 – se l'uscita PGM dell'SP3 inserisce un'altra centrale.
- Aggiungere una telecamera IP a Protegus 2 – immagine dal vivo nella schermata iniziale di Protegus 2.
- Documentazione in inglese: docs.trikdis.com – Security control panel “FLEXi” SP3.

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

Prodotti correlati

Trikdis FLEXi SP3 Ethernet centrale d'allarme intelligente

Trikdis FLEXi SP3 WiFi centrale d'allarme intelligente

Trikdis FLEXi SP3 WiFi + 4G centrale d'allarme intelligente

Trikdis FLEXi SP3 WiFi + 2G centrale d'allarme intelligente

Trikdis FLEXi SP3 Ethernet + 4G centrale d'allarme intelligente

Trikdis FLEXi SP3 Ethernet + 2 SIM 4G centrale d'allarme intelligente

Scatola metallica media con alimentatore per FLEXi SP3

Scatola metallica piccola con alimentatore per FLEXi SP3 **Trikdis FLEXi tastiera LCD**

Trikdis FLEXi tastiera LED

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-flexi-sp3