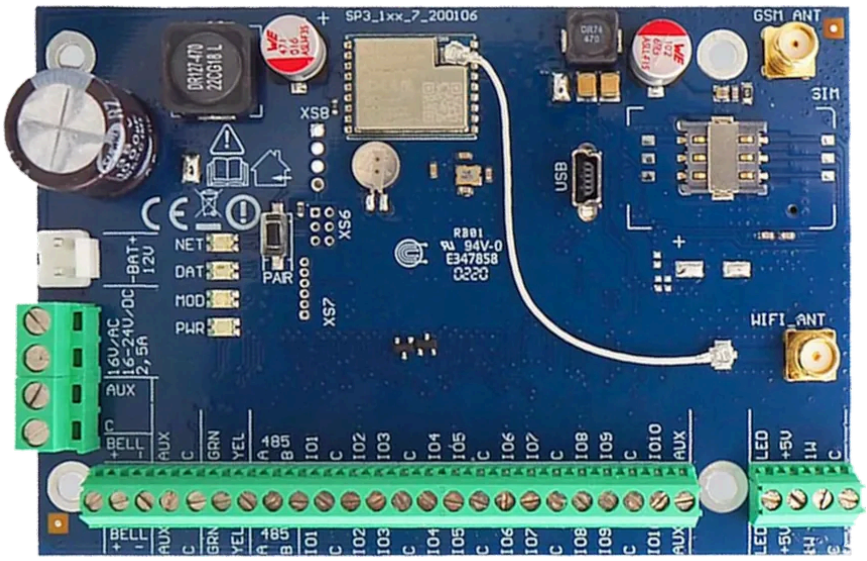
Central de alarma “FLEXi” SP3 – manual de instalación y programación

Manual de instalación y programación de la central de alarma Trikdis “FLEXi” SP3: alimentación, conexión de zonas y salidas PGM, teclados y expansores, programación en TrikdisConfig, transmisión a la CRA, la aplicación Protegus 2.



Edición: 2026-11-17
Versión web siempre actualizada: https://trikdis.es/manual-flexi-sp3

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Versiones y códigos de tipo
1.3 Datos técnicos
1.4 Módulos y teclados compatibles
1.5 Partes de la placa y bornes
1.6 Indicaciones de los LED
1.7 Versiones del firmware

2. Alimentación y puesta en marcha rápida

2.1 Fuente de alimentación de red
2.2 Batería
2.3 Contenido del embalaje, cajas: K01 y K02
2.4 Los pasos de la puesta en marcha, en resumen

3. Instalación y conexión

3.1 Orden recomendado de la instalación
3.1.1 Montaje de la placa en la caja
3.1.2 Orden de conexión de los equipos
3.2 Conexión de los detectores
3.2.1 Esquemas de conexión
3.3 Conexión de los detectores de humo
3.4 Conexión de la sirena
3.5 Conexión de teclados y lectores RFID
3.6 Conexión de los lectores de llaves TM17 y CZ-Dallas
3.7 Conexión de los sensores de temperatura
3.8 Conexión de un relé y de un piloto LED
3.9 Encendido de la central

4. Conexión de expansores y módulos vía radio

4.1 Módulo Ethernet E485
4.2 Receptor vía radio RF-SH (Crow)
4.3 Receptor vía radio RTX3 (Paradox)
4.4 Receptor vía radio RF-HW (Honeywell)
4.5 Receptor vía radio RF-S8
4.6 Receptor vía radio RF-LORA
4.7 Expansores LORA
4.8 Expansores de la serie iO
4.9 Transmisor vía radio T16
4.10 Módulo Sigfox SF485
4.11 Medición de tensión continua

5. Protegus 2 y control remoto

5.1 Vinculación con la cuenta de Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armado y desarmado en la aplicación
5.3 Configuración y control por SMS
5.4 Control por llamada telefónica

6. TrikdisConfig: la configuración en detalle

- 6.1 La barra de estado
- 6.2 System Options
  - 6.2.1 Pestaña System general
  - 6.2.2 Pestaña Partitions
  - 6.2.3 Pestaña Scheduler
  - 6.2.4 Pestaña Holidays
  - 6.2.5 Pestaña System troubles
  - 6.2.6 Pestaña Access
- 6.3 Reporting to CMS
  - 6.3.1 Pestaña Reporting
  - 6.3.2 Pestaña Settings
- 6.4 Users & Reporting
  - 6.4.1 Tarjetas y llaveros RFID
  - 6.4.2 Llaves iButton
  - 6.4.3 Pestaña Protegus
  - 6.4.4 Pestaña SMS answer texts
- 6.5 Modules
- 6.6 Wireless sensors
  - 6.6.1 Registro del RF-LORA
  - 6.6.2 Emparejamiento de detectores a distancia
  - 6.6.3 Emparejamiento con el botón LEARN
  - 6.6.4 RF-SH y equipos Crow
- 6.7 Zones
- 6.8 PGM
- 6.9 Sensors
- 6.10 System events
- 6.11 Events log
- 6.12 Restablecer la configuración de fábrica

7. Programación remota

8. Comprobación del funcionamiento del sistema

9. Actualización del firmware

10. Solución de problemas y preguntas frecuentes

11. Garantía e instrucciones de seguridad

- 11.1 Garantía y limitación de responsabilidad
- 11.2 Instrucciones de seguridad

Ver también

1. Descripción general

La "FLEXi" SP3 es la **central de alarma de intrusión e incendio** de Trikdis que ya lleva el comunicador integrado: a través de una conexión Wi-Fi y/o Ethernet, y con un módem 2G / 4G (por la red móvil, si tiene tarjeta SIM), transmite directamente cada evento producido a la CRA y a la aplicación Protegus 2 (nube Protegus). Tiene diez bornes IO de función seleccionable (zona o salida PGM), gestiona ocho particiones y, según la versión del firmware, se puede ampliar hasta 32 o 64 zonas con teclados, expansores iO y receptores vía radio. La configuración la haces con el software TrikdisConfig, por cable USB o a distancia; el usuario controla el sistema desde un teclado cableado o inalámbrico, con una llave iButton, con una tarjeta RFID, desde la aplicación Protegus 2 y, en las versiones con módem, también por SMS y por llamada telefónica, y puede cambiar a distancia el modo de protección de las distintas zonas del edificio (particiones). La central tiene certificación EN 50131 Grado 3.

1.1 Para qué sirve y cómo funciona

Para qué sirve sobre todo

- **Sistemas de alarma de edificios pequeños y medianos**, a ser posible con conexión a una CRA: admite detectores cableados e inalámbricos, transmite los eventos tanto a la CRA como al usuario, y ambos pueden controlarla a distancia.
- **Sustituir una central de alarma existente**: el valor de las resistencias de fin de línea de los detectores se puede ajustar en la central al de la central sustituida, así que no hace falta volver a cablear los detectores uno por uno.
- **Automatización** además de la seguridad: puerta de garaje y puerta del jardín, riego, iluminación, calefacción, ventilación, refrigeración y cualquier otra cosa que se pueda encender y apagar, desde las salidas PGM, con lógica de funcionamiento, programación horaria o en modo termostato.

Cómo funciona

- **Transmite a la CRA** por la conexión Wi-Fi, Ethernet o de red móvil integrada; con un módulo adicional, también por un canal Ethernet (E485), de radio VHF/UHF (T16) o Sigfox (SF485), con prioridad seleccionable. Puede recibirla cualquier CRA que tenga un receptor IP de software o de hardware de Trikdis, o un receptor IP compatible con el protocolo SIA DC-09. Puede enviar en paralelo a los receptores de dos empresas de seguridad distintas, cada una con receptor principal y de respaldo.
- **Avisa al usuario** en la aplicación Protegus 2 con una notificación push y una señal acústica propia, y las versiones con módem también por SMS a un máximo de 8 números de teléfono. Solo la antigua versión SP3_12xx, con firmware hasta la 1.13, puede avisar con una llamada con mensaje de voz pregrabado (a un máximo de 8 números de teléfono). Se puede configurar que el evento vaya primero a la CRA y solo después al usuario.
- **Se controla a distancia**: armado, desarmado, modos Stay (te quedas en casa) y Sleep (noche), conmutación de los equipos conectados a las salidas PGM y control de la temperatura desde la aplicación; en las versiones con módem, también por SMS y por llamada telefónica.
- **Entradas y salidas**: 10 bornes IO, cada uno utilizable como entrada (tipos NC, NO, EOL, ATZ, con valor de resistencia ajustable en los circuitos EOL y ATZ) o como salida de colector abierto; el número de entradas se puede aumentar hasta 64 con teclados y con los expansores iO, iO-8, iO8-LORA, iO-LORA e iO-WL, y el de salidas hasta 16 con esos mismos expansores; dos salidas dedicadas (BELL para la sirena, LED para el piloto indicador); siete modos de funcionamiento de las salidas, y a cada salida se le puede asignar una lógica de funcionamiento, una programación horaria predefinida o, por ejemplo, el modo

termostato; en el bus 1-Wire, hasta 8 sensores de temperatura, 1 sensor de temperatura y humedad o lectores iButton; en el bus de teclados GRN / YEL, 8 teclados del mismo tipo y el receptor vía radio Paradox RTX3 (4.3); en el bus RS485, expansores iO, receptores vía radio (RF-LORA, RF-SH, RF-S8, RF-HW) y los módulos E485, T16 y SF485.

- **Manejo**: 40 códigos de usuario (1 código maestro y 39 códigos normales, de 4 o 6 dígitos), que también se pueden usar como código de coacción: el código desarma la alarma, pero la CRA recibe una señal aparte de que el desarmado se hizo bajo coacción. Teclados Trikdis, Paradox y Crow, lectores iButton CZ-Dallas y TM17 (descatalogado), lectores RFID Wiegand 26/34.
- **Instalación y configuración**: kits en caja metálica con fuente de alimentación integrada, en varios tamaños, con transformador reductor o con fuente conmutada; la configuración de fábrica se puede usar sin cambios en la mayoría de las instalaciones pequeñas y medianas (siete de cada diez); la central anterior se puede sustituir sin cambiar las resistencias de los detectores; la configuración se puede guardar en un archivo; dos niveles de acceso (instalador y administrador); a distancia, TrikdisConfig no solo configura, sino que también muestra el funcionamiento de la central.

1.2 Versiones y códigos de tipo

La central es una única placa de circuito impreso que se vende en seis versiones según los módulos de comunicación integrados. La versión la indica la primera cifra (**y**) del código **SP3_yxxz** en el nombre del archivo de firmware; lo mismo ves en la barra de estado de TrikdisConfig, y al actualizar solo se puede cargar un firmware con esa misma cifra (apartado 1.7).

Versión	Conexión	Código (y)	Ranura SIM
SP3 WiFi	Wi-Fi	2	–
SP3 Ethernet	red cableada (Ethernet, RJ45)	3	–
SP3 WiFi + 2G	Wi-Fi + módem 2G (GSM/GPRS)	5	1 × nano-SIM
SP3 WiFi + 4G	Wi-Fi + módem 4G (LTE)	1	1 × nano-SIM
SP3 Ethernet + 4G	Ethernet + módem 4G (LTE)	6	1 × nano-SIM
SP3 Ethernet + 2 SIM 4G	Ethernet + módem 4G (LTE), con dos ranuras SIM	compruébalo en la barra de estado del equipo	2 × nano-SIM

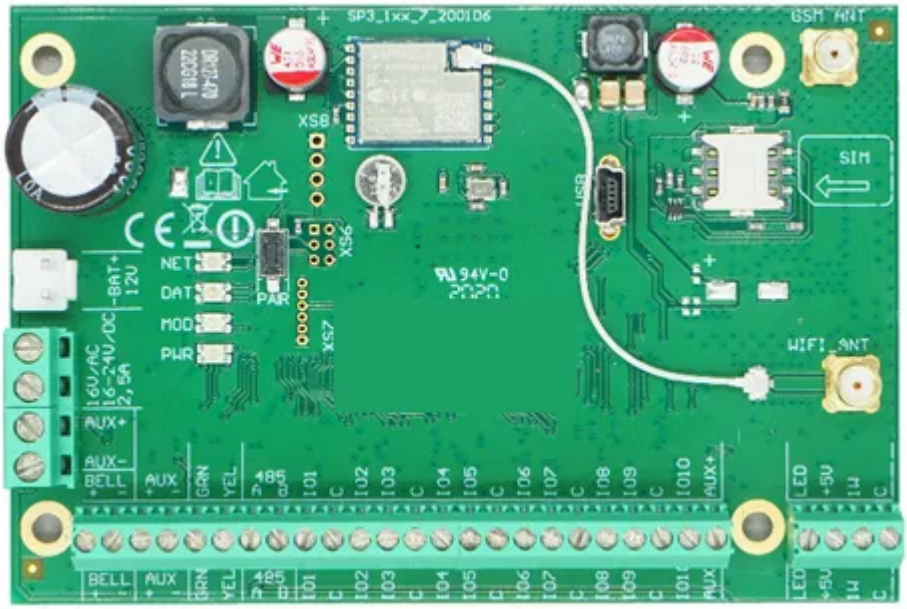


Figura 1. Placa de circuito impreso de la versión "FLEXi" SP3 WiFi + 2G: conectores SMA de las antenas Wi-Fi y de red móvil, ranura nano-SIM y bornes.

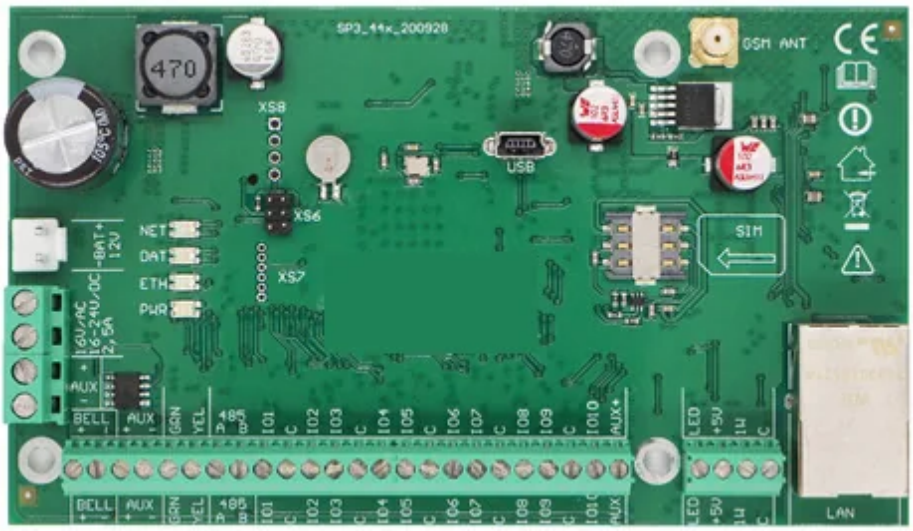


Figura 2. Versión "FLEXi" SP3 Ethernet + 4G: la toma Ethernet RJ45 está en el lugar del conector de la antena Wi-Fi.

Uno o dos canales de comunicación. Las versiones WiFi y Ethernet se comunican por un canal; las versiones con módem, por dos (dual path): además de la conexión cableada, también por la red móvil.

WiFiun canal
Ethernetun canal
WiFi + 2Gdos canales · 1 SIM
WiFi + 4Gdos canales · 1 SIM
Ethernet + 4Gdos canales · 1 SIM
Ethernet + 2 SIM 4Gdos canales · 2 SIM

- Por Wi-Fi y Ethernet el acceso desde el móvil es rápido y no hay coste de datos móviles.
- Si se corta internet por cable o el router se apaga durante un corte de luz, la central con módem pasa sola a la red móvil.
- Gracias a los dos canales que se respaldan mutuamente (dual path), la señal llega a su destino aunque falle una de las vías.

- Con una conexión Wi-Fi, Ethernet o 4G rápida, la programación remota y la actualización del firmware son cómodas.

El módem **2G** de las versiones con módem funciona en las bandas de 850 / 900 / 1800 / 1900 MHz, y el módem **4G (LTE)** en las bandas B1 / B3 / B7 / B8 / B20 / B28 usadas en Europa (EMEA); para otras regiones (Latinoamérica, Australia, Norteamérica) Trikdis también fabrica versiones con un módem de otra distribución de bandas (las bandas figuran en la tabla del apartado 1.3). El Wi-Fi es de 2,4 GHz, 802.11 b/g/n, con cifrado WPA / WPA2.

1.3 Datos técnicos

Característica	Valor
Tensión de alimentación [AC / DC]	16 V AC o 16–24 V DC, 2,5 A
Consumo	máximo 50 mA en reposo; máximo 200 mA durante poco tiempo, al transmitir
Alimentación de respaldo [BAT]	batería de plomo de 12 V, 4 Ah o 7 Ah
Corriente de carga de la batería	máximo 500 mA
Alimentación de equipos externos [AUX]	12 V DC, máximo 1 A
Salida de sirena [BELL]	1 A
Salida LED [LED]	0,1 A
Salida PGM (borne IO como salida)	colector abierto, máximo 0,1 A
Módulo Wi-Fi	integrado en las versiones Wi-Fi; 2,4 GHz, 802.11 b/g/n, WPA / WPA2 / WPA mixto
Configuración de red	DHCP o manual
Tarjeta SIM	en las versiones con módem 1 nano-SIM (en la versión de 2 SIM, 2)
Bandas del módem 2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz
Bandas del módem 4G (LTE) – "FLEXi" SP3_14E / SP3_24E, EMEA y Tailandia	B1 / B3 / B7 / B8 / B20 / B28
Bandas del módem 4G (LTE) – "FLEXi" SP3_24S, Latinoamérica / Australia / Nueva Zelanda	B1 / B3 / B4 / B5 / B7 / B8 / B28
Bandas del módem 4G (LTE) – "FLEXi" SP3_24A, Norteamérica	B2 / B4 / B12
Destinos de los eventos	receptores principal y de respaldo de 2 empresas de seguridad; la nube Protegus, la aplicación Protegus 2 para iOS / Android; SMS a 8 números de teléfono; llamada a 8 números de teléfono: si el usuario contesta, la central le dice con un mensaje de voz qué ha pasado (solo la versión SP3_12xx, con firmware hasta la 1.13)
Canales de envío de eventos	GPRS o 4G, Wi-Fi, Ethernet (integrado o con el módulo E485), SMS; llamada de voz a un máximo de 8 números de teléfono (solo la versión SP3_12xx, con firmware hasta la 1.13); radio VHF/UHF (con el comunicador T16); Sigfox (con el módulo SF485)
Conexión con la CRA	TCP/IP o UDP/IP, o SMS

Característica	Valor
Codificación de eventos	Contact ID
Cifrado	TRK AES-128, SIA IP AES-128
Reloj interno	sí
Búfer de mensajes	60 eventos
Registro de eventos	máximo 1000 eventos; cuando se llena, se borra el más antiguo
Códigos de usuario	40 (de 4 o 6 dígitos)
Código de coacción	se elige uno de dos modos de introducción al programar
Bornes de doble función [IO]	10; función IN u OUT al programar. Como entrada: NC, NO, EOL, EOL_T, 3EOL, ATZ, ATZ_T. Como salida: colector abierto (OC), máximo 100 mA
Particiones	8
Zonas	10 (20 con duplicación de zonas ATZ); hasta 64 con expansores (apartado 1.7)
Salidas PGM	2 (12 si los bornes IO están configurados como salidas; 16 con expansores)
Teclados	máximo 8 (los tipos se enumeran en el apartado 1.4)
Lectores RFID (Wiegand 26/34)	máximo 2
Longitud del bus 1-Wire [1 WIRE]	máximo 30 m
Sensores de temperatura	Maxim / Dallas DS18S20, DS18B20; serie AM2301
Número de sensores de temperatura en el bus 1-Wire	8 (Dallas) o 1 (AM2301)
Llaves electrónicas (iButton) [1 WIRE]	Maxim / Dallas DS1990A, máximo 40 llaves
Longitud del bus RS485	máximo 100 m
Equipos en el bus RS485	máximo 8
Entorno de funcionamiento	−10 °C … +50 °C, humedad relativa máxima del 80 % a +20 °C, sin condensación
Dimensiones de la placa	117 × 79 × 25 mm; las versiones Ethernet + 4G, 137 × 79 × 25 mm
Peso	0,1 kg

Las distancias «hasta … m» son máximos teóricos que se alcanzan en condiciones ideales. En la práctica, la calidad y el recorrido del cable, las fuentes de interferencias y, en los enlaces de radio, las paredes y el terreno dan un alcance bastante menor. Planifica con margen y, en tramos largos, comprueba la conexión durante la puesta en marcha.

1.4 Módulos y teclados compatibles

La salida AUX de la central da como máximo 1 A a los equipos externos; para dimensionar la batería de respaldo (apartado 2.1) hay que sumar el consumo total de los módulos conectados. La lista de Trikdis:

Módulo	Consumo
Teclado SK-LED TouchPad (Protegus SK232 LED W)	60–150 mA
Teclado SK-LCD TouchPad (FLEXi SK232LCD; en la tienda: teclado FLEXi LCD)	25–60 mA

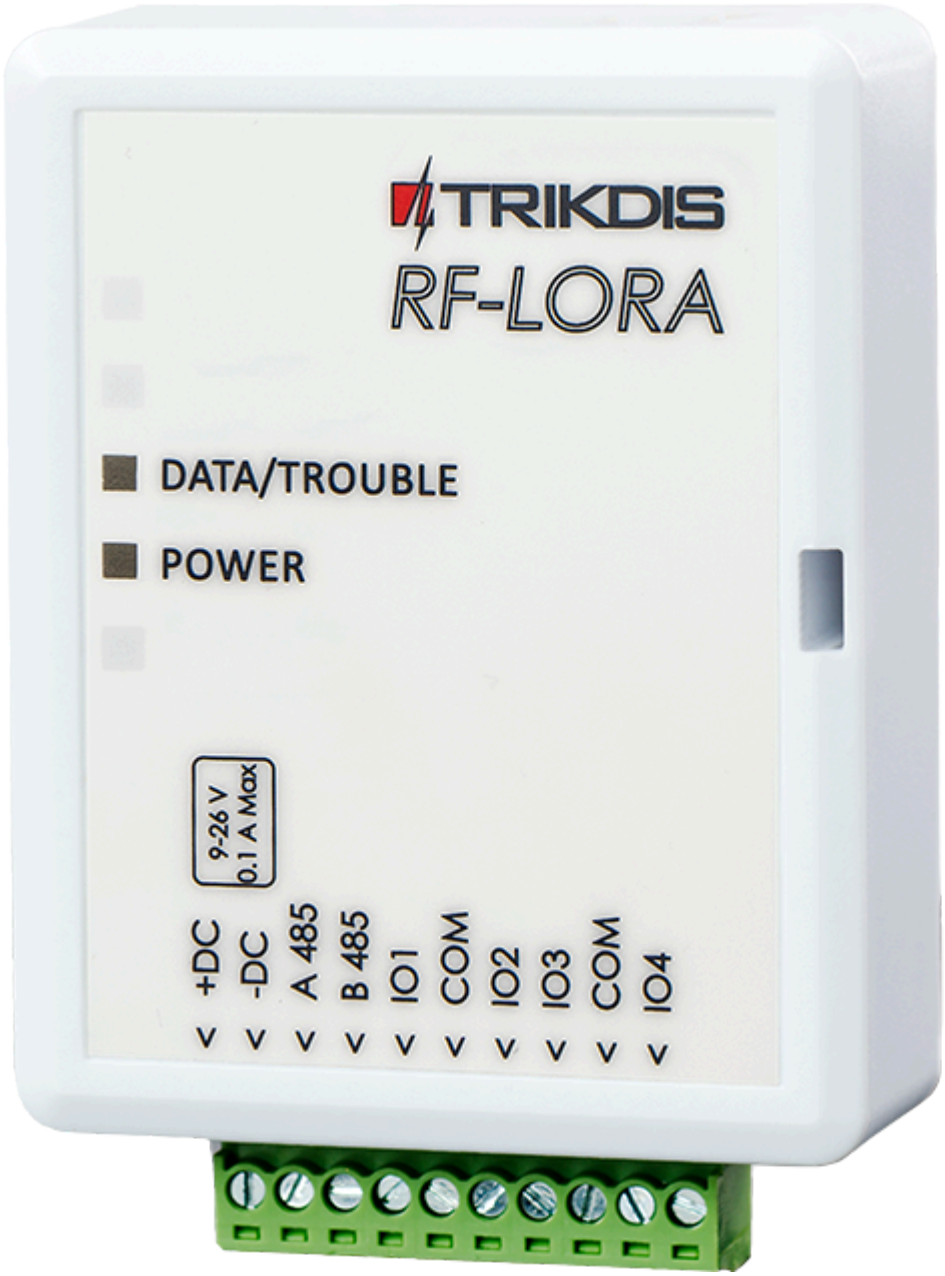
Módulo	Consumo
Teclado SK LCD Button	máximo 70 mA
Teclado SK LED Button	máximo 70 mA
Teclado Paradox K636	40–70 mA
Teclado Paradox K10H(V)	44–72 mA
Teclado Paradox K32 LED, K32+ LED	49–148 mA
Teclado Paradox K32LCD+	70–150 mA
Teclado Paradox K35	30–70 mA
Teclado Paradox TM50	100–230 mA
Teclado Paradox TM70	200–330 mA
Teclado Crow CR16, CR-LCD	40–75 mA
Expansor iO-8	máximo 20 mA
Expansor iO	máximo 50 mA
Transceptor vía radio iO-MOD – iO-WL	50–150 mA
Expansor inalámbrico iO-WL	máximo 200 mA
Receptor vía radio RF-SH (para detectores Crow)	máximo 100 mA
Transceptor vía radio Paradox RTX3	máximo 200 mA
Transceptor vía radio RF-HW (para detectores Honeywell)	máximo 100 mA
Transceptor vía radio RF-S8 (para detectores S8)	máximo 100 mA
Transceptor vía radio RF-LORA (para detectores y módulos LORA)	50–150 mA
Expansor iO-LORA, iO8-LORA	máximo 50 mA
Pulsador de pánico PB-LORA	pila propia, 3 V CR123A
Módulo de relé REL-LORA	máximo 45 mA
Módulo Ethernet E485	50–150 mA
Lector iButton TM17	máximo 50 mA
Lector iButton CZ-Dallas	máximo 25 mA
Comunicador vía radio VHF / UHF T16	100 mA – 1,2 A
Lector RFID (Wiegand 26/34)	máximo 100 mA

Teclados. Al bus GRN / YEL se pueden conectar hasta 8 teclados del mismo 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.

Equipos inalámbricos. El tipo de receptor vía radio depende de la versión del firmware de la central (apartado 1.7): una central trabaja con un solo tipo de receptor a la vez.

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 Partes de la placa y bornes

El dibujo muestra las partes principales de la placa; la función de los bornes figura en la tabla de debajo del dibujo.

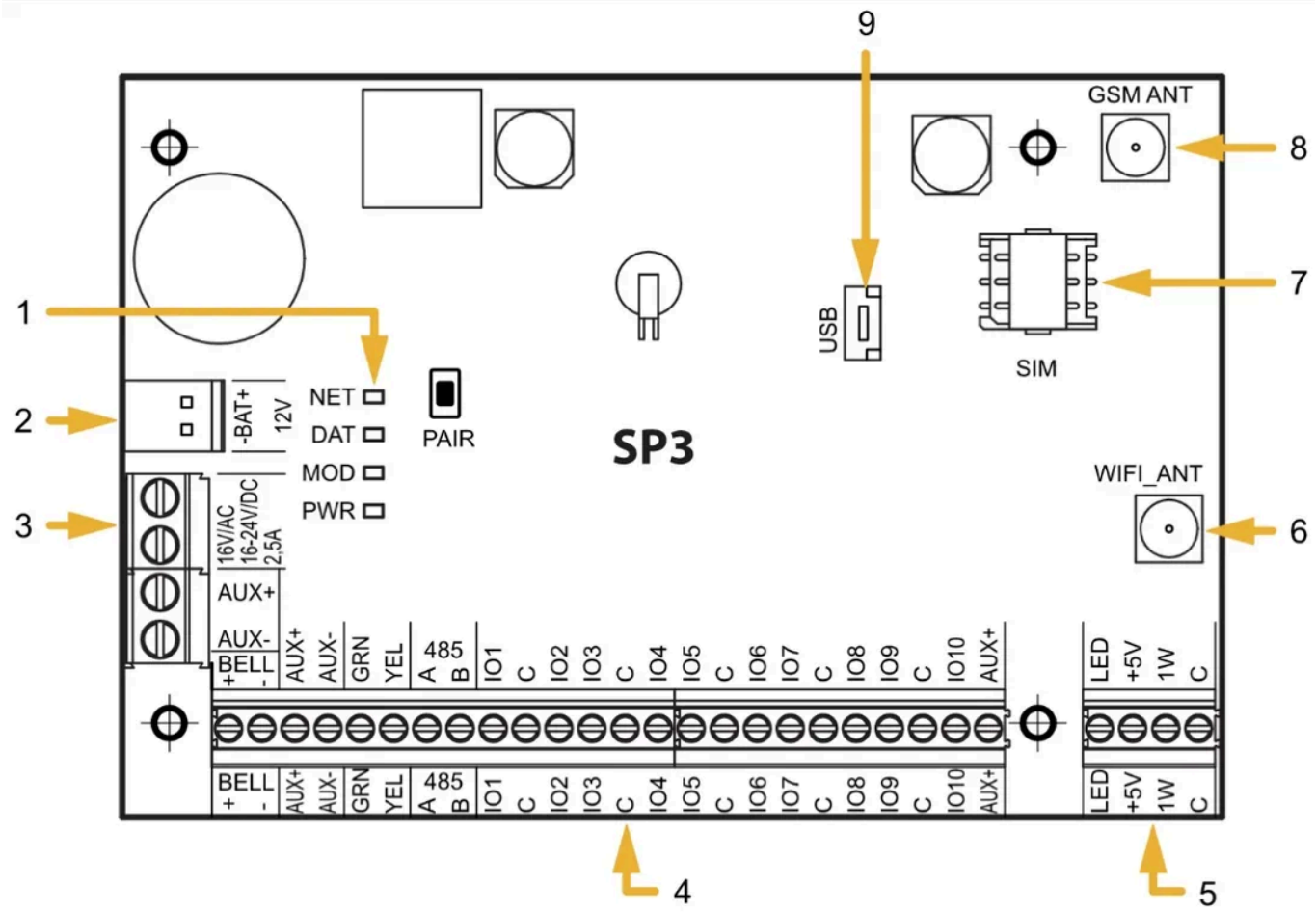


Figura 3. Placa de circuito impreso de la "FLEXi" SP3 (versión Wi-Fi + móvil). En la versión Ethernet, en el lugar del 6 hay una toma Ethernet RJ45.

- 1 LED indicadores de conexión y de funcionamiento (apartado 1.6)
- 2 Bornes de la alimentación de respaldo (batería)
- 3 Bornes de la alimentación principal
- 4 Bornes de los equipos externos
- 5 Bornes del bus de datos 1-WIRE
- 6 Conector SMA para la antena Wi-Fi
- 7 Ranura nano-SIM
- 8 Conector SMA para la antena de red móvil
- 9 Toma USB Mini-B para la programación

Borne	Función
AC/DC (2 bornes)	Alimentación principal: 16 V AC, o polo positivo y negativo de 16–24 V DC
BAT+	Polo positivo de la alimentación de respaldo (batería de 12 V)
BAT–	Polo negativo de la alimentación de respaldo
AUX+	+12 V para los equipos externos (máximo 1 A)
AUX–	Negativo común
BELL+	Salida de sirena: +12 V para la sirena
BELL–	Salida de sirena: polo negativo conmutado de la sirena (máximo 1 A)
GRN	Bus de teclados (datos)
YEL	Bus de teclados (datos)
A 485	Hilo A del bus RS485

Borne	Función
B 485	Hilo B del bus RS485
IO1 – IO9	Entradas/salidas (configuración de fábrica: entrada)
IO10	Entrada/salida (configuración de fábrica: salida PGM, reinicio de detectores de incendio)
C	Negativo común
LED	Salida PGM (configuración de fábrica: indicación del estado del sistema)
+5 V	Alimentación de +5 V para los equipos 1-Wire
1 WIRE	Bus de datos 1-Wire
C	Negativo común

Los bloques de bornes son extraíbles, así que puedes conectar los cables sin la placa, y la placa se puede sacar para el mantenimiento.

1.6 Indicaciones de los LED

LED	Indicación	Significado
NET	parpadea en verde	la tarjeta SIM se está registrando en la red móvil
	verde fijo	la tarjeta SIM se ha registrado en la red móvil
	parpadea en amarillo	intensidad de la señal móvil, de 0 a 5 destellos; 3 ya es suficiente
DAT	apagado	no hay eventos sin enviar
	verde fijo	envío de mensajes en curso
	amarillo fijo	hay eventos sin enviar esperando en el búfer
MOD (versión Wi-Fi)	parpadea en verde	conectando a la red Wi-Fi
	verde fijo	conectada a la red Wi-Fi
ETH (versión Ethernet)	parpadea en verde	no hay cable LAN, o error de DHCP
	verde fijo	conectada a la red cableada
PWR	parpadea en verde	no hay fallos de funcionamiento
	1 destello rojo	no hay tarjeta SIM
	2 destellos rojos	el PIN de la tarjeta SIM es incorrecto
	3 destellos rojos	no puede conectarse a la red móvil
	4 destellos rojos	no llega al receptor de la CRA por el canal 1
	5 destellos rojos	no llega al receptor de la CRA por el canal 2
	6 destellos rojos	el reloj interno no está en hora
	7 destellos rojos	tensión baja de la alimentación de respaldo (batería)
	8 destellos rojos	no hay alimentación de red (AC)
	9 destellos rojos	no puede conectarse a la red Wi-Fi

La solución de los fallos se trata en el capítulo 10.

1.7 Versiones del firmware

El nombre del archivo de firmware de la central tiene la forma **SP3_yxxz_NNNN.fw**. La **y** es la versión de hardware (apartado 1.2) y no se puede cambiar al actualizar. La **z** indica el tipo de receptor inalámbrico y, con ello, el número de zonas que se pueden gestionar; la eliges tú al actualizar, según el receptor vía radio que uses. **NNNN** es el número de versión del firmware; en general conviene usar la versión más alta.

Firmware (z)	Receptor inalámbrico	Detectores inalámbricos	Zonas	Teclados	Módulos
SP3_xxx0	RF-SH (descatalogado), 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, no se usa en 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

El firmware **SP3_xxx4** solo hace falta para los detectores inalámbricos: con él funcionan los equipos inalámbricos MAXIMUM (RF-LORA) y S8 (RF-S8), con 64 zonas. Hace falta como mínimo la versión 1.21, y para los equipos S8 la 1.22. Los expansores LORA conectados a través del RF-LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) funcionan con las cuatro versiones. El expansor Paradox RTX3 necesita **SP3_xxx1**, con 32 zonas. Carga siempre la versión más reciente: en noviembre de 2026 es la 1.27, con la comunicación mejorada, y en ella se ha corregido el envío de demasiados SMS. La codificación y las reglas para elegir se describen en un artículo aparte: Firmware de la FLEXi SP3: ¿cómo elegir el adecuado?. Los pasos de la actualización están en el capítulo 9.

2. Alimentación y puesta en marcha rápida

La central, y con ella todo el sistema de alarma, se alimenta de una fuente de alimentación de red; el respaldo lo da una batería de 12 V. En este capítulo encontrarás las reglas de la alimentación, los kits de Trikdis y el orden resumido de los pasos de la puesta en marcha; los detalles de la conexión están en los capítulos 3 y 4, y los de la configuración en los capítulos 5 y 6.

2.1 Fuente de alimentación de red

La central funciona con **16 V AC** o **16–24 V DC**, desde una fuente capaz de dar al menos **2,5 A**. En corriente alterna la alimenta desde la red un transformador reductor de Clase II; en corriente continua, una fuente conmutada de 16–24 V (en las cajas K01 y K02 que vendemos, una Mean Well APV-35-24). La alimentación principal se conecta a los dos bornes **AC/DC** de la placa; en corriente continua, el polo positivo y el negativo

en el orden marcado en los bornes. En los dos casos, con alimentación alterna y con alimentación continua, es obligatorio conectar la alimentación de respaldo, una batería de 12 V, para que la alimentación sea continua y sin cortes (apartado 2.2).

Magnetotérmico y toma de tierra

En el circuito de alimentación hay que instalar un interruptor automático magnetotérmico bipolar con una separación de al menos 3 mm entre sus contactos abiertos; el interruptor debe estar en un lugar conocido y accesible para el técnico que hace el mantenimiento de la central. Si la caja es metálica, conéctala a tierra. La caja, la fuente de alimentación, la batería y el equipo de programación deben cumplir la norma EN 60950.

Cálculo del consumo. Según la EN 50131, la alimentación de respaldo debe mantener el sistema en funcionamiento durante **12 horas** (Grado 2) o **60 horas** (Grado 3) después de un fallo de la alimentación de red. Para ello, suma la corriente en reposo de la central (50 mA) y el consumo de los teclados, módulos, detectores y señalizadores conectados (los datos de los equipos Trikdis y de los equipos compatibles de otras marcas están en la tabla del apartado 1.4), y elige según el resultado la capacidad de la batería. El borne **AUX+** puede dar en total como máximo 1 A a los equipos externos; si hace falta más, usa una fuente de alimentación aparte, con el negativo común.

2.2 Batería

La alimentación de respaldo es una **batería de plomo de 12 V, de 4 Ah o 7 Ah** (para el Grado 3, al menos 7 Ah), conectada a los bornes **BAT+ / BAT−** de la placa con el cable de conexión que viene en la caja. La central la carga con un máximo de 500 mA.

- Si falla la alimentación de red, la central envía el evento **AC Fault** (fallo de red) y pasa a la batería.
- A 11,5 V se genera el evento **Low Battery** (batería baja); por debajo de 9,5 V la central **desconecta** la batería para protegerla de la descarga profunda.
- Cuando vuelve la alimentación de red, envía el evento **AC Restore** y empieza a cargar; a 12,6 V envía el evento **Battery Restore** (batería correcta).

La batería debe cargarse en 72 horas para cumplir el requisito de Clase II y en 24 horas para el de Clase III; esto resulta de la capacidad de la batería junto con la corriente de carga de 500 mA.

2.3 Contenido del embalaje, cajas: K01 y K02

La central se vende sola (placa) o con una caja metálica preparada. En el embalaje de fábrica de la placa vienen: la placa "FLEXi" SP3, un cable de conexión de la batería, 20 resistencias de 2,2 kΩ y 10 de 4,7 kΩ, 4 separadores de plástico para la fijación y, para las versiones con módem, una antena ME301M de base magnética con 2,5 m de cable (según la lista de contenido de fábrica, 2 unidades). El **cable USB Mini-B** necesario para la programación y la batería no se incluyen.

En las versiones con caja, la central va montada en una caja metálica con interruptor antisabotaje (tamper) y con la alimentación preparada: fuente conmutada Mean Well APV-35-24, punto de conexión de la red de 230 V con fusible de 3,15 A, todo ya cableado. Hay dos tamaños de caja:

Caja	Tamaño	Observación
K01: caja metálica de tamaño normal	285 × 280 × 80 mm	para todas las versiones de la SP3
K02: caja metálica pequeña	200 × 210 × 80 mm	la versión Ethernet + 4G no cabe en ella

Caja metálica mediana con fuente de alimentación para FLEXi SP3

Caja metálica pequeña con fuente de alimentación para FLEXi SP3

Las dos cajas (K01 y K02) llevan una fuente conmutada Mean Well con un bloque de bornes con fusible de 3,15 A; las cajas K01 más antiguas todavía llevaban un transformador de 230 V / 16 V, 40 VA. Con los kits de fábrica (SP3 KIT, SP3 KITi), además de la placa montada en la caja metálica, vienen 2 antenas ME301M (con 2,5 m de cable), un cable de conexión de la batería, 20 resistencias de 2,2 kΩ y 10 de 4,7 kΩ, y un detector antisabotaje.

2.4 Los pasos de la puesta en marcha, en resumen

Qué vas a necesitar

Cable USB Mini-B · destornillador plano para los bornes · las resistencias de 2,2 kΩ y 4,7 kΩ que vienen en la caja · batería de 12 V 7 Ah · para la versión con módem, una nano-SIM activa con servicio de datos móviles (desactiva antes la petición del PIN en un teléfono) · para la versión Wi-Fi, el nombre y la contraseña de la red · el software TrikdisConfig en un ordenador con Windows.

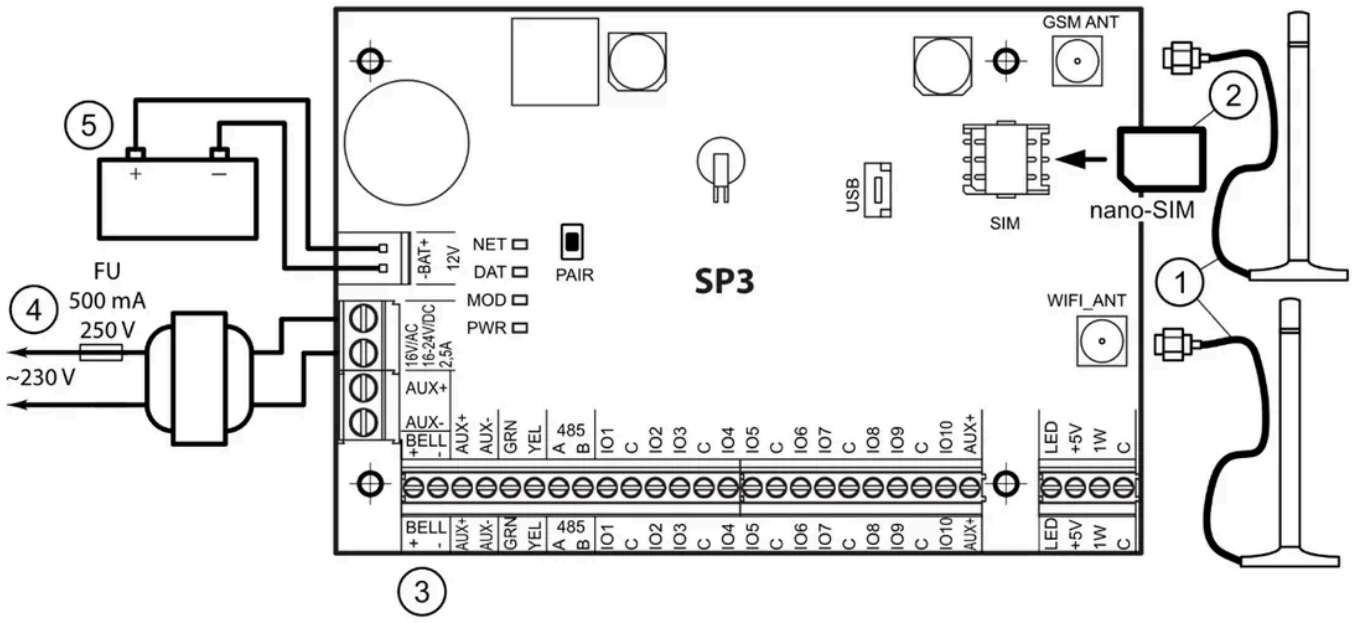


Figura 4. Conexión de la alimentación y orden de la puesta en marcha. Alimentación de red: transformador ("Transformer"), ~230 V / 16 V, 40 VA, 50 Hz, con un fusible de 500 mA / 250 V (FU) en la rama de 230 V, o una fuente de alimentación de corriente continua de 16–24 V, 2,5 A ("or DC power supply source 16-24 V, 2,5 A"); alimentación de respaldo: batería ("Battery"), 12 V, 7 Ah.

- 1 Enroscar las antenas móvil y Wi-Fi en los conectores de antena
- 2 Introducir la tarjeta nano-SIM en la ranura SIM
- 3 Conectar los equipos a los bornes
- 4 Conectar la alimentación de red a los bornes AC/DC
- 5 Conectar la batería a los bornes BAT+ / BAT−

1. **Planifica el sistema.** Decide dónde irán la caja, los teclados, los señalizadores acústicos y luminosos y los equipos controlados; según la zona que hay que proteger y las características de los detectores, decide el número, el tipo y la ubicación de los detectores.
2. **Monta la placa en la caja** con los separadores de plástico y conecta a tierra la caja metálica (apartado 3.1).
3. **Enrosca las antenas** (móvil y Wi-Fi) y coloca la tarjeta nano-SIM activada (versión con módem).

4. **Conecta los equipos** según los esquemas de conexión: detectores de apertura, de movimiento, de incendio y otros (3.2–3.3), sirena (3.4), teclados y lectores (3.5–3.6), sensor de temperatura (3.7), relés y piloto indicador (3.8), el interruptor antisabotaje de la caja; los expansores y receptores vía radio, según el capítulo 4.
5. **Conecta la alimentación de red** a los bornes AC/DC. Al encenderse, la central reconoce los teclados, expansores y lectores conectados correctamente al bus 1-WIRE y al bus GRN / YEL (apartado 3.9).
6. **Conecta la batería** a los bornes BAT+ / BAT−.
7. **Configura la central con TrikdisConfig** por el cable USB (capítulo 6). La configuración de fábrica sirve para la mayoría de las instalaciones pequeñas y medianas; lo que normalmente hay que revisar: las particiones y los datos básicos del sistema (**System Options**, 6.2), el tipo y el comportamiento de las zonas (**Zones**, 6.7), los usuarios, sus códigos y sus números de teléfono (**Users & Reporting**, 6.4), la hora exacta (6.2), los datos de la tarjeta SIM (6.2), los receptores de la CRA, desactivados de fábrica (**Reporting to CMS**, 6.3), la nube Protegus, activada de fábrica, y las notificaciones por SMS (6.4, 6.10), el funcionamiento de las salidas PGM (6.8). La configuración recomendada en detalle:
    - **Sistema.** Si quieres armar los grupos de zonas por separado, divide el sistema en particiones y ajusta las propiedades de las particiones (6.2.2). Configura cada zona según las características del detector y el comportamiento de alarma que quieras para el evento de la zona (6.7); en un sistema dividido en particiones, asignas cada zona a la partición deseada. Para el manejo desde el teclado, con una llave iButton o desde el teléfono (por SMS), hay que crear usuarios y darles permisos (6.4).
    - **Envío de mensajes.** La hora exacta hay que ajustarla para que los mensajes lleven la marca de tiempo correcta (6.2.1). La transmisión de eventos está activada de fábrica para todos los eventos: si se produce un evento, su aviso va a los destinatarios configurados por los canales configurados; la transmisión de eventos concretos la puedes desactivar en la ventana **System events** (6.10). Si la central envía por la red móvil, introduce los datos de la tarjeta SIM (6.2.1). La transmisión a la CRA está desactivada de fábrica (6.3). La nube Protegus está activada de fábrica; la notificación por SMS y la llamada están desactivadas de fábrica; el envío al teléfono del usuario se configura en el apartado 6.10.
    - **Control remoto.** Por llamada y por SMS puede controlar el sistema quien tenga su número de teléfono en la lista de usuarios (6.4). Por llamada no solo se puede armar y desarmar todo el sistema o una parte, sino también encender y apagar los equipos conectados a las salidas PGM; lo que hay que configurar en la salida para ello se describe en el apartado 5.4. Por SMS también se pueden cambiar algunos parámetros de funcionamiento de la central, armar y desarmar todo el sistema o una parte, y conmutar los equipos conectados a las salidas PGM; la lista de comandos está en el apartado 5.3.
8. **Cambia los códigos de fábrica** por valores que solo conozcas tú: el código maestro en la ventana **Users & Reporting**, la contraseña SMS en el campo **SMS Password** del grupo **System Options** → **Access**, y los códigos de acceso de TrikdisConfig en ese mismo grupo **Access**.
9. **Vincula el sistema con la aplicación Protegus 2** (apartado 5.1).
10. **Comprueba el funcionamiento** según el capítulo 8: evento desde el teclado, recepción en la CRA y en Protegus 2, salidas, armado remoto.

3. Instalación y conexión

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.

Este capítulo describe el montaje de la placa, el orden de la conexión y, después, la conexión de los detectores, los detectores de humo, las sirenas, los teclados y lectores, los sensores de temperatura y los relés. El significado de los bornes figura en la tabla del apartado 1.5; la conexión de los expansores y de los módulos vía radio está en el capítulo 4. En los dibujos, los nombres de los bornes de la SP3 están a la izquierda y los del equipo conectado, a la derecha.

3.1 Orden recomendado de la instalación

Planificación del sistema:

- Dibuja el plano de los locales y marca dónde irán la caja de la central, el teclado o los teclados, los señalizadores acústicos y luminosos, y los equipos que la central controlará de forma automática o a distancia.
- Según el lugar, la necesidad de protección y las características de los detectores que entran en consideración, decide el número, el tipo y la ubicación de los detectores.

3.1.1 Montaje de la placa en la caja

La placa va en una caja en la que ya están el transformador reductor (con fusible de 500 mA) y el sitio para la batería de respaldo. Fija la placa en la caja de plástico o metálica que hayas elegido con **separadores de plástico**; **la caja metálica hay que conectarla a tierra**. La caja debe cumplir los requisitos de las normas EN 60950 y EN 50131.

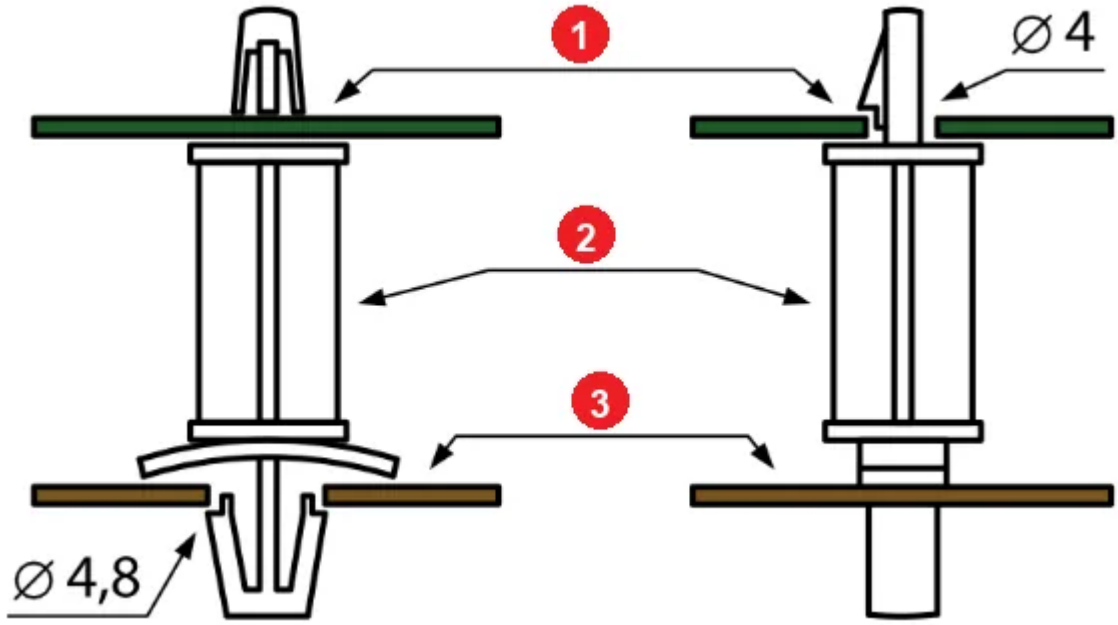


Figura 5. Fijación de la placa con un separador de plástico (a la izquierda, vista frontal: “Front view”; a la derecha, vista lateral: “Side view”). El taladro de la placa es de Ø4 mm y el de la caja, de Ø4,8 mm.

- 1 la placa de circuito impreso de la SP3 (“SP3 circuit board”)
- 2 separador (“Spacer”)
- 3 la caja (“Box housing”)

La placa mide 116,5 × 78,5 mm. Los centros de los cuatro taladros de fijación de Ø4 mm están a 93 mm en horizontal y a 61 mm en vertical entre sí; los taladros de la izquierda, a 5 mm del borde izquierdo, y los de abajo, a 10 mm del borde inferior.

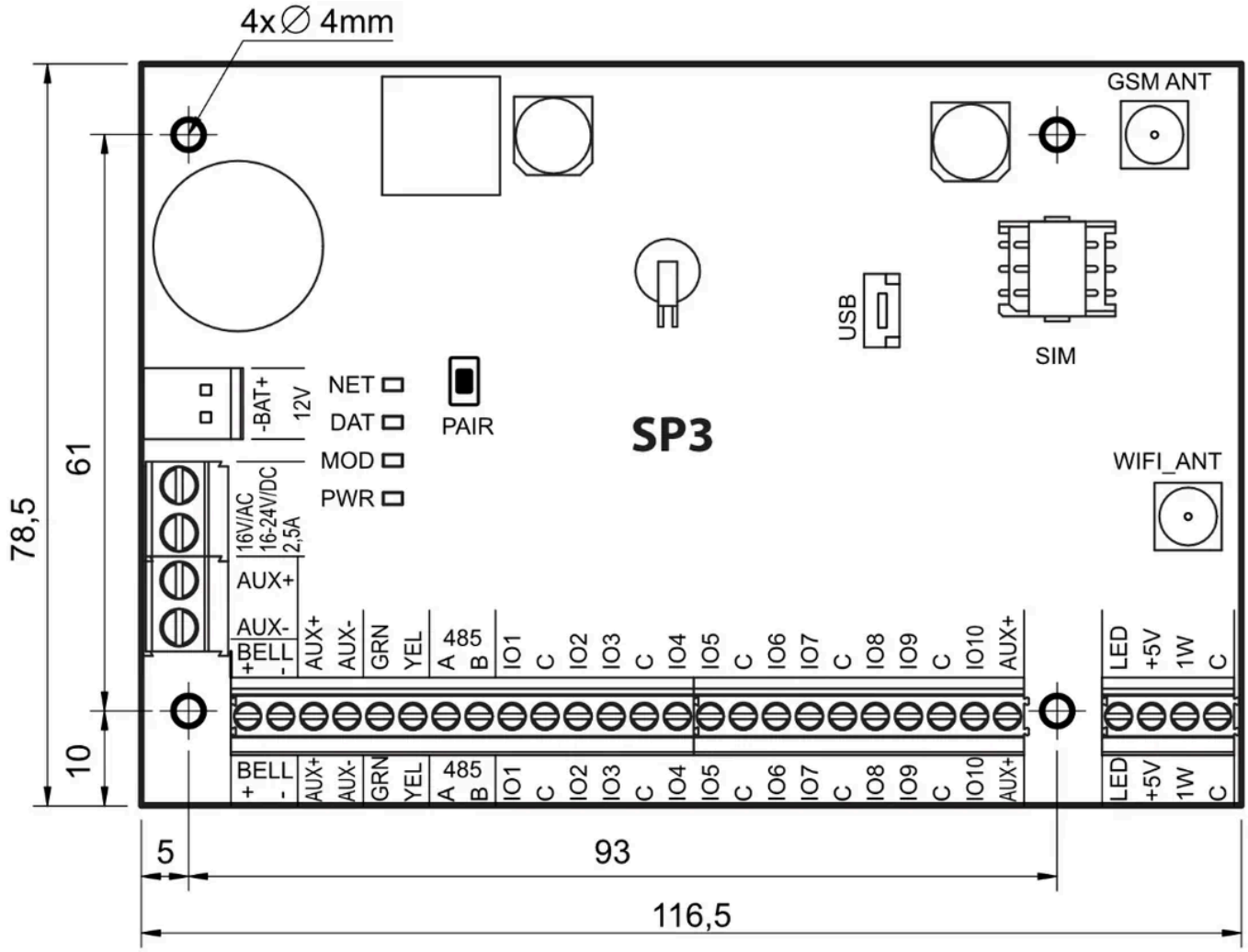


Figura 6. Medidas de la placa y de los taladros de fijación, en milímetros.

3.1.2 Orden de conexión de los equipos

Conecta los equipos en el orden siguiente; la alimentación y la batería, siempre al final.

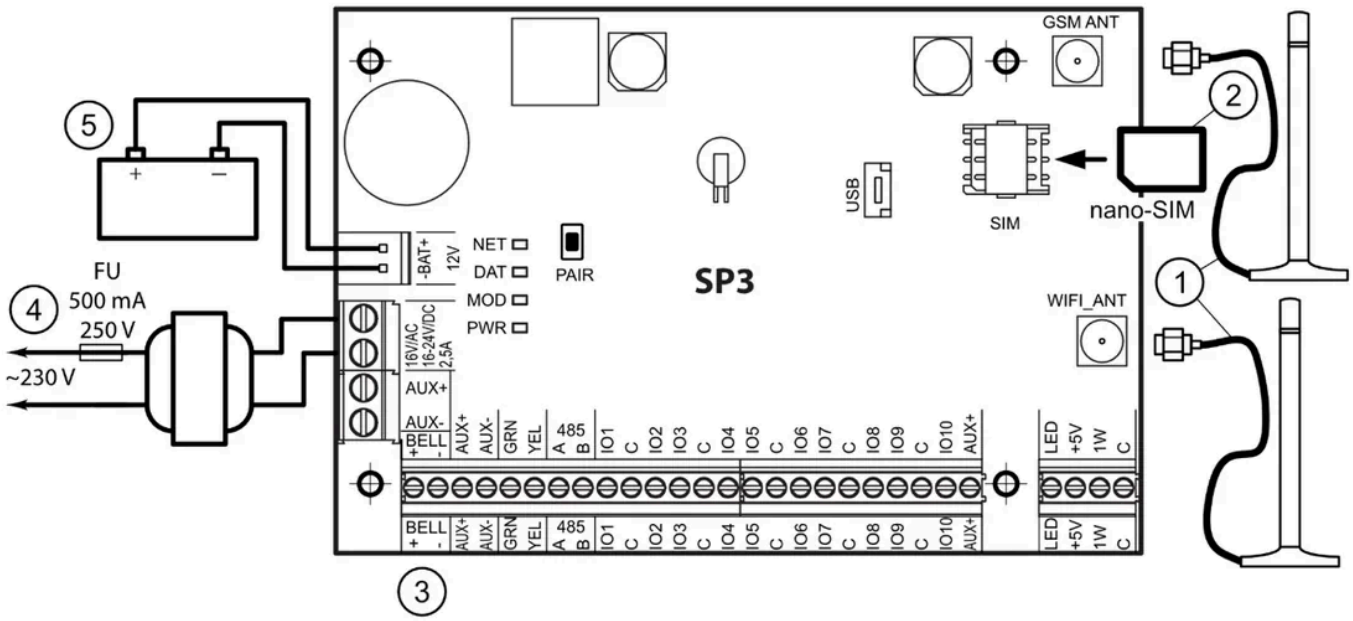


Figura 7. Vista general de la alimentación y de las conexiones. Alimentación de red: transformador de ~230 V / 16 V, 40 VA, 50 Hz ("Transformer"; con un fusible de 500 mA, 250 V en el lado de 230 V) o fuente de alimentación de corriente continua de 16–24 V, 2,5 A ("or DC power supply source 16-24 V, 2,5 A"); batería de respaldo ("Battery"), 12 V, 7 Ah.

- 1 antenas GSM y Wi-Fi en los conectores de antena
- 2 tarjeta nano-SIM en la ranura SIM
- 3 los equipos en el bloque de bornes externo
- 4 alimentación de red en los bornes AC/DC
- 5 batería en los bornes BAT+ / BAT−

1. Enrosca la **antena GSM** y la **antena Wi-Fi** en los conectores de antena (según la versión, una de ellas o las dos, apartado 1.2).
2. En la versión con módem, coloca la **tarjeta nano-SIM activada** en la ranura. Conviene desactivar antes la petición del PIN en un teléfono.
3. En la versión Ethernet (SP3_3E, SP3_44E), enchufa el **cable LAN** en el conector RJ45.
4. Según los esquemas de conexión de este manual, los esquemas de conexión propios de los equipos conectados y el proyecto, conecta los detectores de apertura de puertas y ventanas, los detectores de movimiento, de incendio y otros, los señalizadores acústicos y luminosos, los teclados y los equipos controlados. Conecta también a los bornes de la placa el **interruptor antisabotaje** de la puerta de la caja y de arranque de la pared.
5. Conecta los cables de la fuente de alimentación de red a los bornes **AC/DC** de la placa y da la alimentación. La central reconoce los teclados, expansores y adaptadores conectados correctamente al bus 1-WIRE y al bus YEL/GRN.
6. Coloca la batería en la caja y conecta sus terminales a los bornes **BAT+ / BAT−**.

La batería debe cargarse en 72 horas para que el sistema cumpla el grado de seguridad 2 (Grade 2), y en 24 horas para el grado 3 (Grade 3).

El bloque de bornes se puede extraer: así el equipo se puede dejar sin tensión o reiniciar con un solo movimiento, es más fácil de manejar durante el cableado y, para la programación por USB, el equipo se puede llevar al ordenador.

El orden recomendado de la configuración (particiones, zonas, usuarios, hora, transmisión, control remoto, cambio de códigos) se resume en el apartado 2.4, y los detalles están en el capítulo 6.

3.2 Conexión de los detectores

En la placa, **10 bornes IO** (IO1–IO10) reciben los circuitos de los detectores. De fábrica, IO1–IO9 son entradas e IO10 es una salida PGM (reinicio de los detectores de incendio, ver 3.3). El número de entradas se puede aumentar hasta un máximo de 64 con expansores (iO, iO-8, iO-WL, RF-SH, iO-LORA, iO8-LORA). Cualquier borne se puede configurar como entrada (zona), y en la página **Zones** (6.7) se ajustan las propiedades de la zona: el tipo de circuito (**NO, NC, EOL, EOL_T, 3EOL, ATZ, ATZ_T**), la sensibilidad a los eventos breves del circuito y la función de la zona (retardada, instantánea, instantánea stay, seguidora, seguidora stay, incendio, interruptor de llave, 24 horas, silenciosa, silenciosa 24 horas). Los expansores iO-8 e iO8-LORA admiten todos los tipos de circuito de la central.

Resistencias de fin de línea. Para los circuitos EOL, EOL_T, 3EOL, ATZ y ATZ_T puedes elegir en TrikdisConfig entre siete juegos de resistencias (**System Options** → **System general** → **EOL Type**, 6.2.1), así que, al sustituir una central antigua, las resistencias existentes pueden quedarse en los detectores. RT es la resistencia del circuito de sabotaje, R1 la del primer detector y R2 la del segundo (en 3EOL, la del circuito de enmascaramiento). Junto a cada juego figuran las centrales de alarma cuyos valores de resistencia de fábrica coinciden con él:

Juego	RT	R1	R2
1 – predeterminado de 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 (modo de 6 zonas, con sabotaje)	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

En las marcas indicadas coinciden la resistencia de sabotaje y la del detector (RT, R1); en la Satel INTEGRA, el cableado con una sola resistencia (EOL). Con la duplicación de zonas (ATZ) y con el cableado 3EOL también debe coincidir R2: esto se cumple en el juego 2 para Paradox y Hikvision AX Hybrid PRO, en el 3 para Eldes ESIM364 y en el 6 para Crow Runner. Donde en la central antigua el valor de la resistencia era ajustable (por ejemplo, Crow, Risco, Honeywell Galaxy, Pyronix, Texecom), decide la resistencia que hay en los detectores. El cableado de Honeywell VISTA (2 kΩ) y el de dos resistencias de Satel (2EOL, 2 × 1,1 kΩ) no coinciden con ninguno de los juegos.

3.2.1 Esquemas de conexión

En las figuras, **IOx** es el borne IO elegido y **C** el borne negativo común; NC es un contacto normalmente cerrado y NO, un contacto normalmente abierto.

Marcas en los dibujos. R1, R2, RT: resistencia; RT es la resistencia del circuito de sabotaje. La **T** roja marca el contacto antisabotaje y el número azul, el número de orden del detector; el significado de cada marca también figura debajo del dibujo correspondiente.

NO: normalmente abierto, sin resistencia de fin de línea. Cuando el detector se activa, cierra el circuito entre IOx y C.

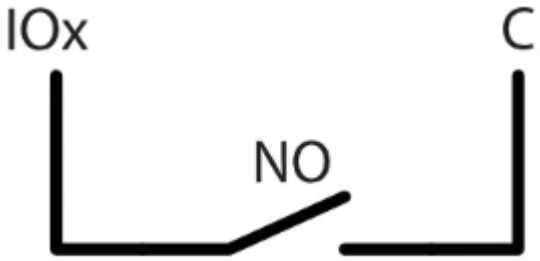


Figura 8. Zona NO: el contacto normalmente abierto entre los bornes IOx y C.

NC: normalmente cerrado, sin resistencia de fin de línea. Cuando el detector se activa, abre el circuito entre IOx y C.

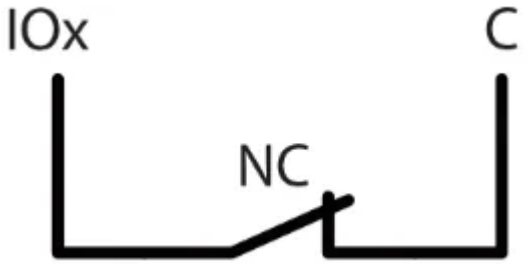


Figura 9. Zona NC: el contacto normalmente cerrado entre los bornes IOx y C.

EOL: con resistencia de fin de línea. Con un detector NO, R1 va en paralelo con el contacto; con un detector NC, en serie con él, entre IOx y C; así la central detecta también el corte y el cortocircuito del cable.

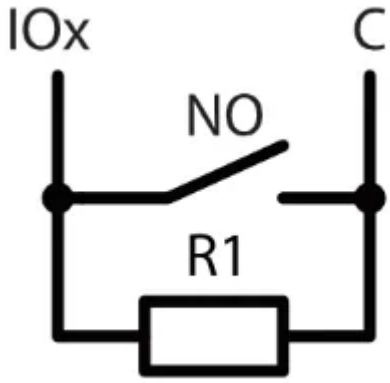


Figura 10. Zona NO con resistencia de fin de línea (EOL): R1 en paralelo con el contacto abierto, entre IOx y C.

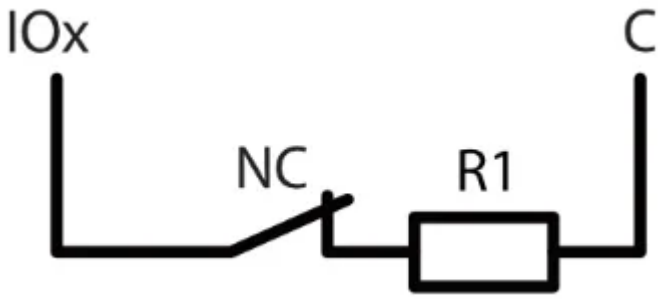


Figura 11. Zona NC con resistencia de fin de línea (EOL): R1 en serie con el contacto cerrado, entre IOx y C.

EOL_T: con resistencia de fin de línea, detección de sabotaje y de fallo del cableado. Partiendo de IOx, el contacto antisabotaje NC y RT en serie; después, el contacto de alarma NC en paralelo con R1, entre RT y C.

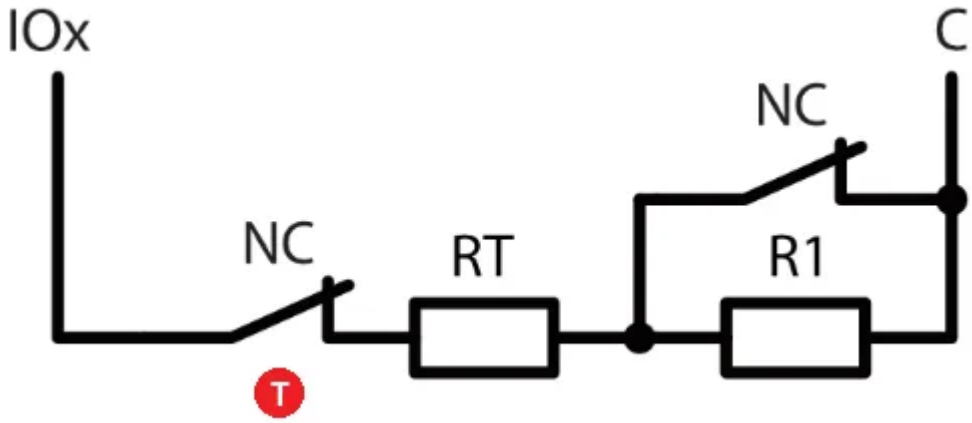


Figura 12. Zona EOL_T: IOx → contacto antisabotaje NC → RT → (contacto de alarma NC en paralelo con R1) → C.

- T contacto antisabotaje (“Tamper”), indica la apertura de la carcasa del detector

ATZ: duplicación de zonas. Dos detectores en un borne: entre IOx y C, dos circuitos en serie; en el primero, un contacto NC en paralelo con R1, y en el segundo, un contacto NC en paralelo con R2. Así, con los 10 bornes se pueden gestionar 20 zonas.

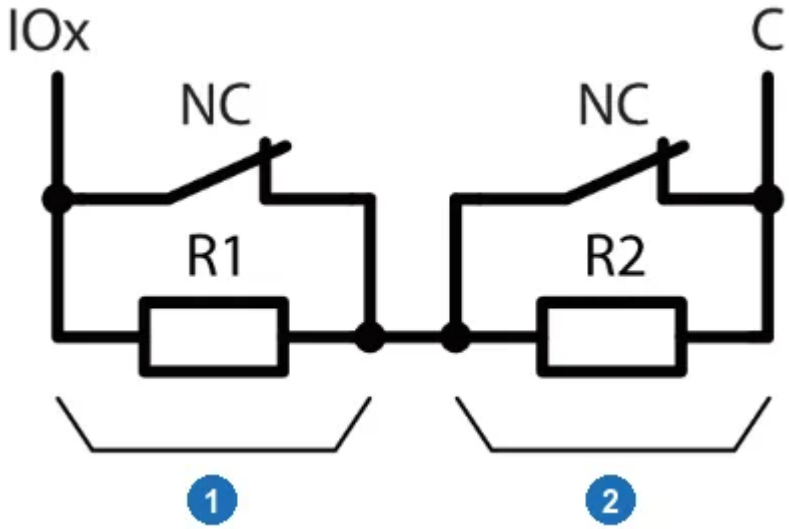


Figura 13. Zona ATZ: el contacto NC del detector 1 en paralelo con R1 y, en serie con él, el contacto NC del detector 2 en paralelo con R2, entre IOx y C.

- 1 circuito del detector 1 (“Detector terminal 1”)
- 2 circuito del detector 2 (“Detector terminal 2”)

ATZ_T: duplicación de zonas con detección de sabotaje y de fallo del cableado. Como ATZ, pero en el circuito de los dos detectores va también en serie el contacto antisabotaje NC, y en el primer circuito, junto con la resistencia RT.

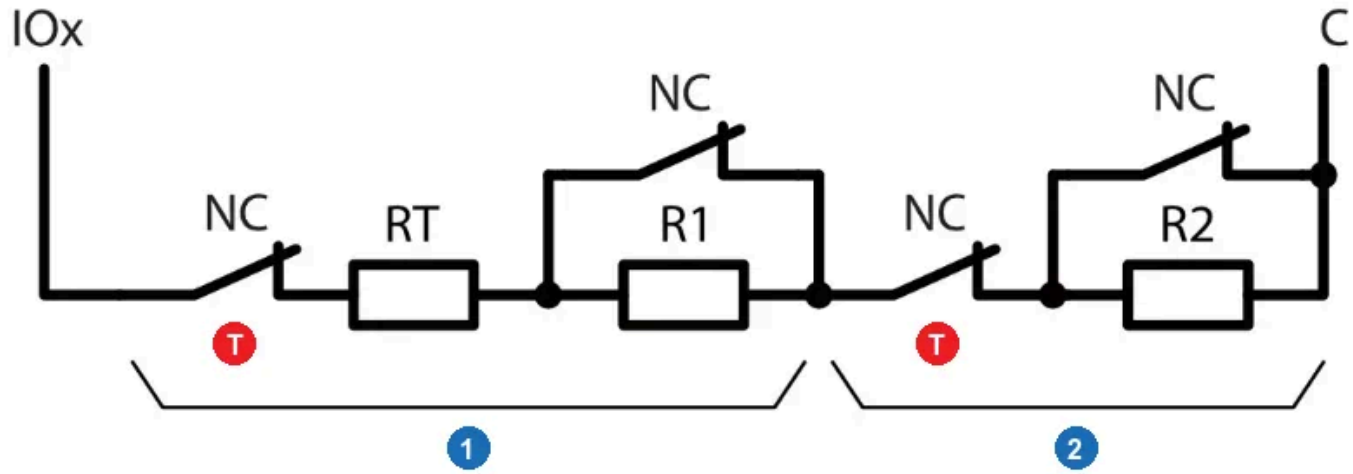


Figura 14. Zona ATZ_T: detector 1: contacto antisabotaje NC y RT en serie, y después contacto NC en paralelo con R1; detector 2: contacto antisabotaje NC en serie, y después contacto NC en paralelo con R2; los dos circuitos en serie entre IOx y C.

- T contacto antisabotaje ("Tamper"), indica la apertura de la carcasa del detector
- 1 circuito del detector 1 ("Detector terminal 1")
- 2 circuito del detector 2 ("Detector terminal 2")

3EOL: tres resistencias de fin de línea: alarma, sabotaje y enmascaramiento. Dentro de un mismo detector se pueden reconocer por separado el circuito de sabotaje, el de alarma y el antienmascaramiento (anti-masking).

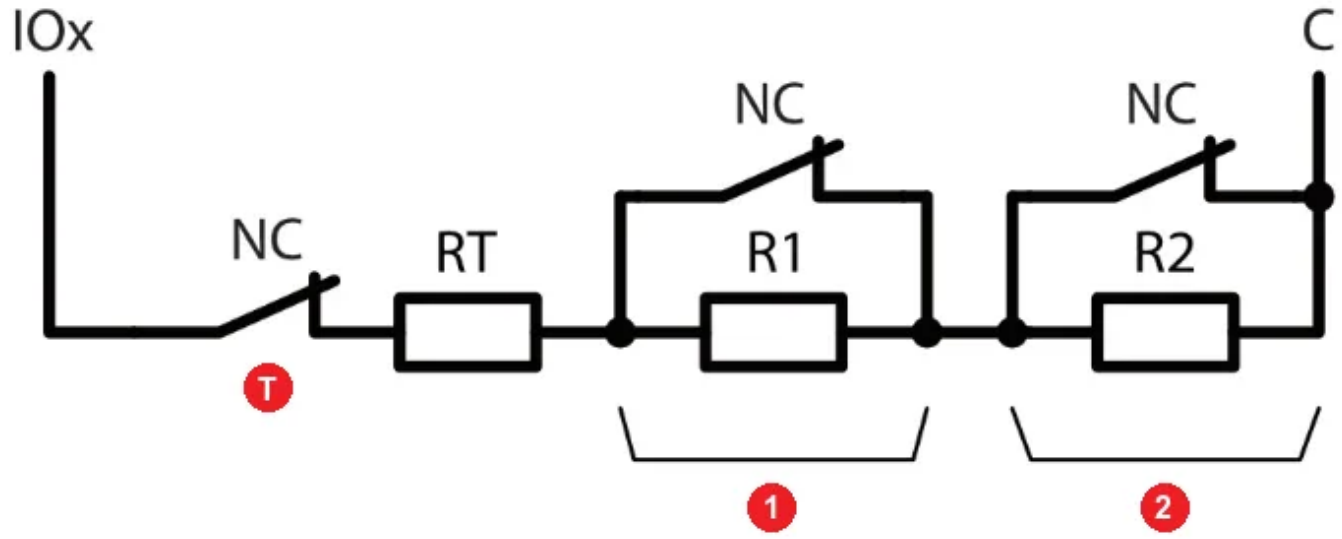


Figura 15. Zona 3EOL: IOx → contacto antisabotaje NC y RT en serie → circuito de alarma (contacto NC en paralelo con R1) → circuito de enmascaramiento (contacto NC en paralelo con R2) → C.

- T contacto antisabotaje ("Tamper"), indica la apertura de la carcasa del detector
- 1 circuito de alarma ("Alarm")
- 2 circuito antienmascaramiento ("Anti-masking"), indica que el detector se ha tapado

3.3 Conexión de los detectores de humo

Detectores de humo de dos hilos en la salida LED. Si conectas así los detectores de incendio, marca la casilla **LED out as 2Wire fire** en la página **System Options** (6.2).

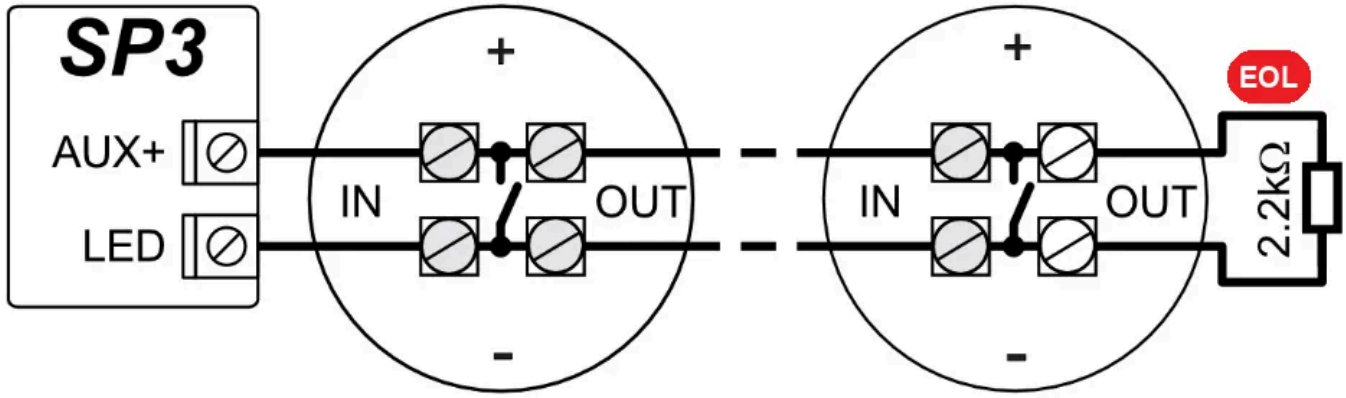


Figura 16. Detectores de humo de dos hilos en la salida LED: AUX+ → borne + IN del primer detector, LED → − IN; los bornes + OUT y − OUT de cada detector, al mismo borne IN del detector siguiente; después del último detector, una resistencia de fin de línea de 2,2 kΩ entre el hilo + y el hilo −.

- EOL resistencia de fin de línea de 2,2 kΩ (“End of line resistor”)

Detectores de humo de cuatro hilos. Asigna la función de zona **incendio** a la entrada (IOx) del circuito de los detectores de humo (6.7). La alimentación de los detectores de cuatro hilos la conmuta la salida PGM IO10, que tiene la función **Fire Sensor Reset** (reinicio de detectores de incendio) (6.8); esta es la configuración de fábrica de IO10. El relé K1 indica el corte del cable y la retirada de un detector.

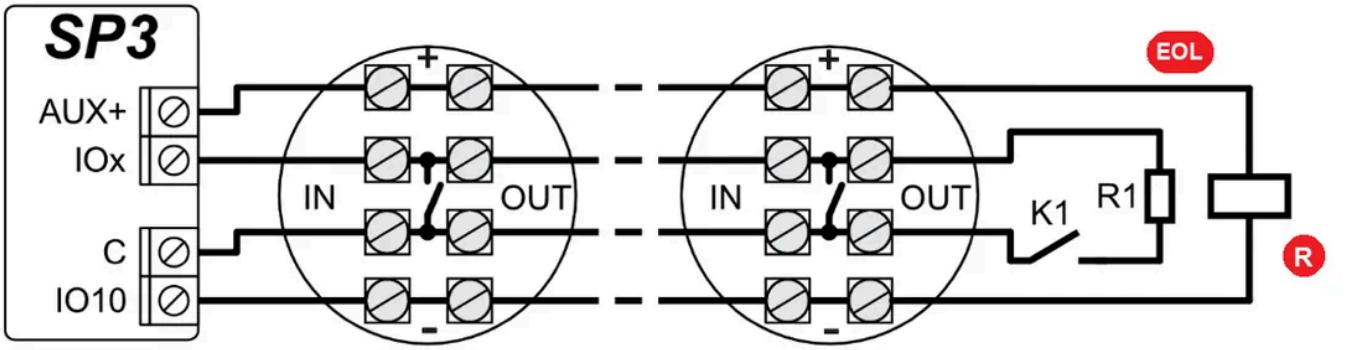


Figura 17. Detectores de humo de cuatro hilos con relé K1. De arriba abajo: AUX+ → borne + del primer detector, IOx → el contacto superior, C → el contacto inferior, IO10 → − IN; los cuatro bornes OUT, al mismo borne IN del detector siguiente; después del último detector, el contacto de K1 y la resistencia de fin de línea R1 en serie entre el hilo IOx y el hilo C; la bobina de K1, entre el hilo AUX+ y el hilo IO10.

- R relé **K1** (“Relay”)
- EOL la resistencia de fin de línea **R1** (“End of line resistor”)

Detectores de humo de dos hilos con el adaptador SM1. Con el adaptador SM1, los detectores de dos hilos se pueden conectar a una entrada IO; también aquí el relé K1 indica el corte del cable y la retirada de un detector. El circuito de supervisión se puede montar de dos maneras:

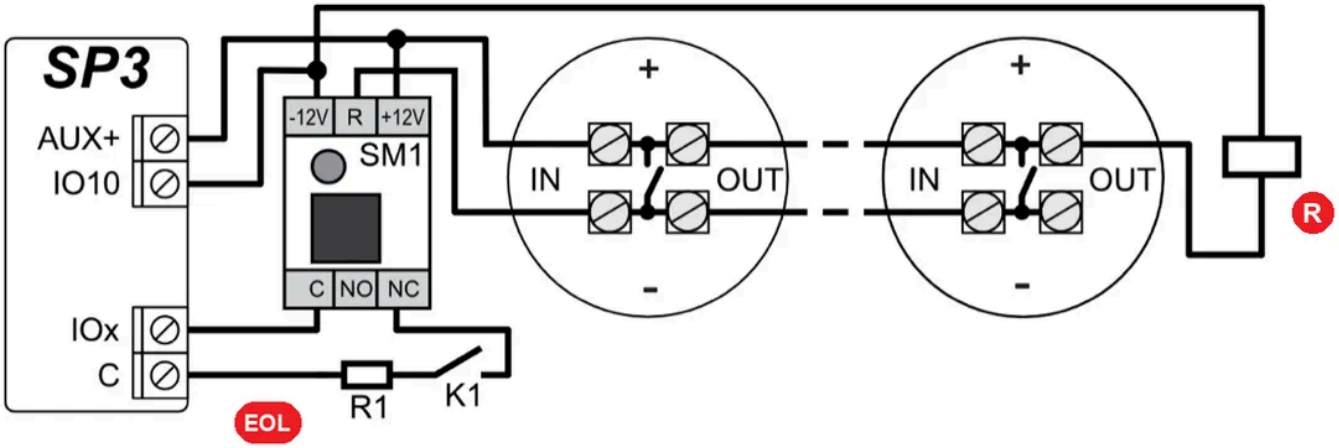


Figura 18. Detectores de humo de dos hilos con el adaptador SM1: AUX+ → +12V del SM1 y + IN del primer detector; IO10 → −12V del SM1 y la bobina de K1; R del SM1 → − IN del detector; los bornes IN/OUT de los detectores en cadena, el último + OUT a K1. Circuito de supervisión: IOx → C del SM1; el borne C de la SP3 → resistencia de fin de línea R1 → contacto de K1 → NC del SM1.

- R relé **K1** ("Relay")
- EOL la resistencia de fin de línea **R1** ("End of line resistor")

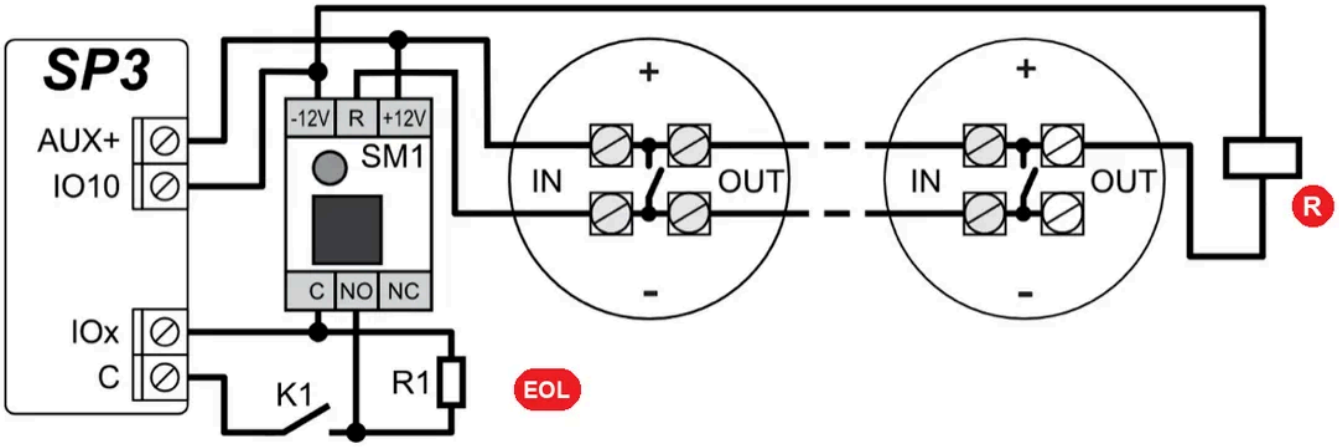


Figura 19. Lo mismo con el otro circuito de supervisión: R1 entre los bornes C y NO del SM1; el borne C de la SP3, a través del contacto de K1, al borne NO del SM1.

- R relé **K1** ("Relay")
- EOL la resistencia de fin de línea **R1** ("End of line resistor")

3.4 Conexión de la sirena

Conecta la sirena a la salida **BELL+ / BELL−** (la salida BELL admite 1 A; ver los datos técnicos en el apartado 1.3).

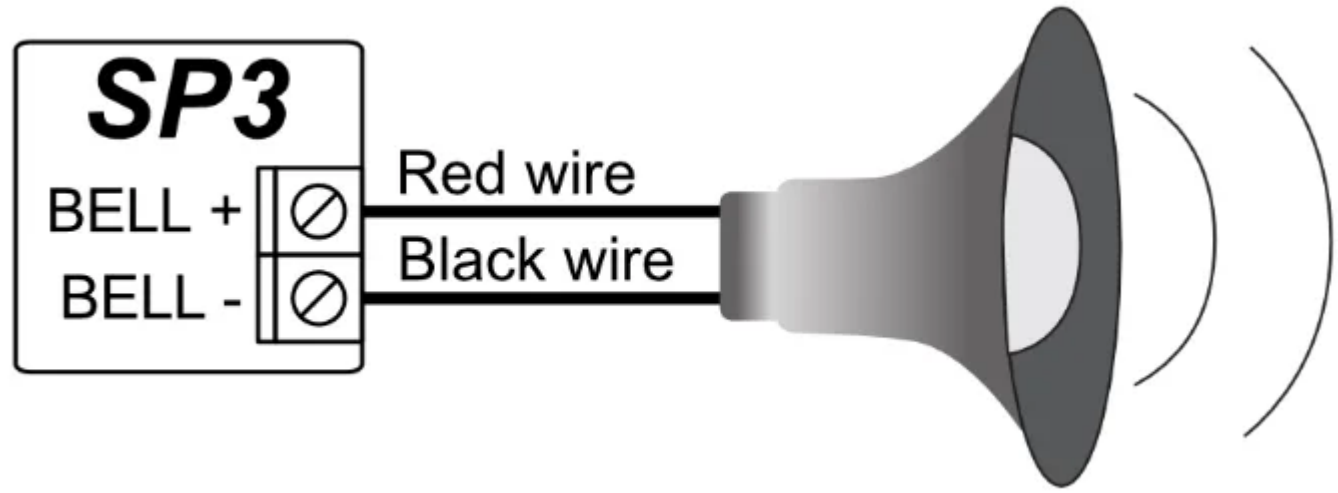


Figura 20. Sirena en la salida BELL: BELL+ → cable rojo, BELL− → cable negro.

Con la sirena exterior MR100, la central también supervisa el circuito de sabotaje (SAB): de fábrica, con una EOL de 2,2 kΩ, en la entrada **IO9**. De fábrica, IO9 es una zona de 24 horas, pero se puede cambiar libremente. Si en la central supervisas el circuito de sabotaje de la sirena con otro modo EOL, cierra los contactos JPS1 y conecta en serie en el circuito de sabotaje una resistencia del valor adecuado.

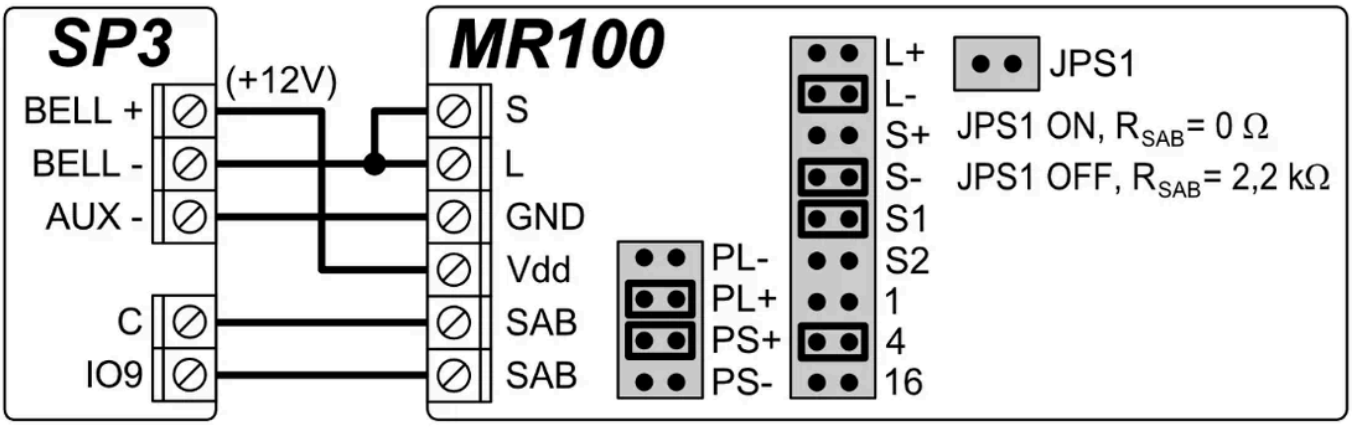


Figura 21. Sirena exterior MR100 ("Outdoor siren"): BELL+ (+12 V) → Vdd, BELL− → S y L, AUX− → GND, C e IO9 → los dos bornes SAB (sabotaje). Puntos puenteados en el dibujo: PL+, PS+, L−, S−, S1 y 4. JPS1 cerrado ("ON"): R_SAB = 0 Ω; JPS1 abierto ("OFF"): R_SAB = 2,2 kΩ.

3.5 Conexión de teclados y lectores RFID

Aquí entran los teclados del bus de teclados y los lectores RFID con protocolo Wiegand 26/34. Al bus de teclados (**GRN**, **YEL**) se pueden conectar como máximo **8 teclados del mismo tipo**. Indica el tipo de teclado en la página **Modules** (6.5); la central reconoce y asigna automáticamente los equipos conectados. El teclado también tiene su propia entrada de zona (ZONE): el otro extremo del detector conectado aquí va al borne AUX−. El manejo del sistema desde los teclados (códigos de usuario, anulación de zonas, iButton y RFID, llamada, SMS, salidas PGM) se describe en el manual de usuario de la SP3, aparte, para los teclados Protegus y Paradox.

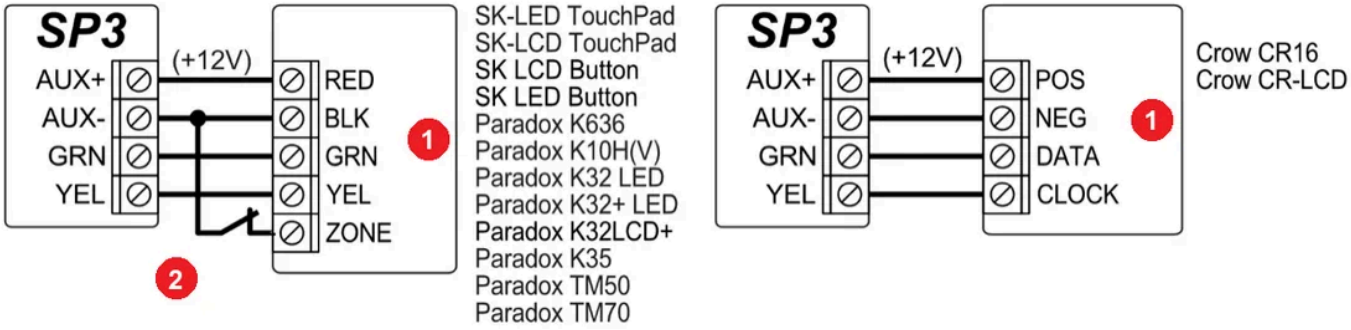


Figura 22. Conexión de los teclados. SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, y Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50, TM70: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; el borne ZONE del teclado, a través del contacto del detector, al borne AUX−. Crow CR16 y CR-LCD: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK.

- 1 teclado (“Keypad”)
- 2 la zona del teclado (“Keypad zone”)

Lector RFID (Wiegand 26/34). A la central se pueden conectar como máximo **2 lectores**. Los hilos de datos del lector (D0, D1) van o al bus de teclados (GRN, YEL) o a los bornes **IO1** e **IO2**, según las figuras. Si hay dos lectores (lado de entrada y lado de salida), ya no se puede conectar ningún teclado a la central.

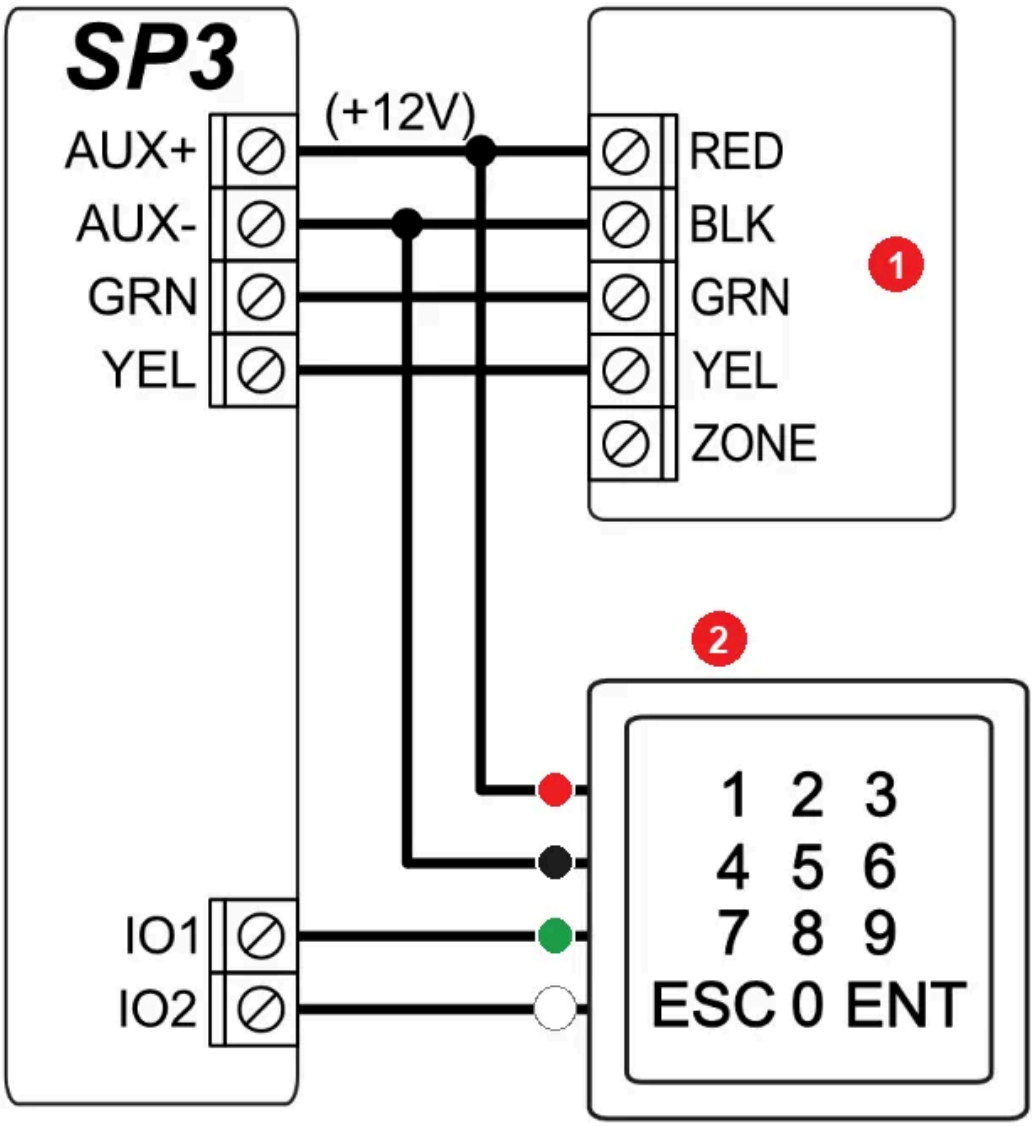


Figura 23. Teclado y lector de entrada juntos. El teclado (SK-LED TouchPad, SK-LCD TouchPad, SK LCD Button, SK LED Button, Paradox K636, K10H(V), K32 LED, K32+ LED, K32LCD+, K35, TM50 o TM70) en el bus, según la figura anterior: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL; el cable rojo del lector (+U) → AUX+, el negro (GND) → AUX−, el verde (D0) → IO1, el blanco (D1) → IO2.

- 1 teclado (“Keypad”)
- 2 lector de entrada: lector RFID con teclado, Wiegand 26/34 (“Entry reader”, “RFID reader with keypad (Wiegand 26/34)”)
- cable rojo, +U (“R - red wire (+U)”)
- cable negro, GND (“B - black wire (GND)”)
- cable verde, D0 (“G - green wire (D0)”)
- cable blanco, D1 (“W - white wire (D1)”)

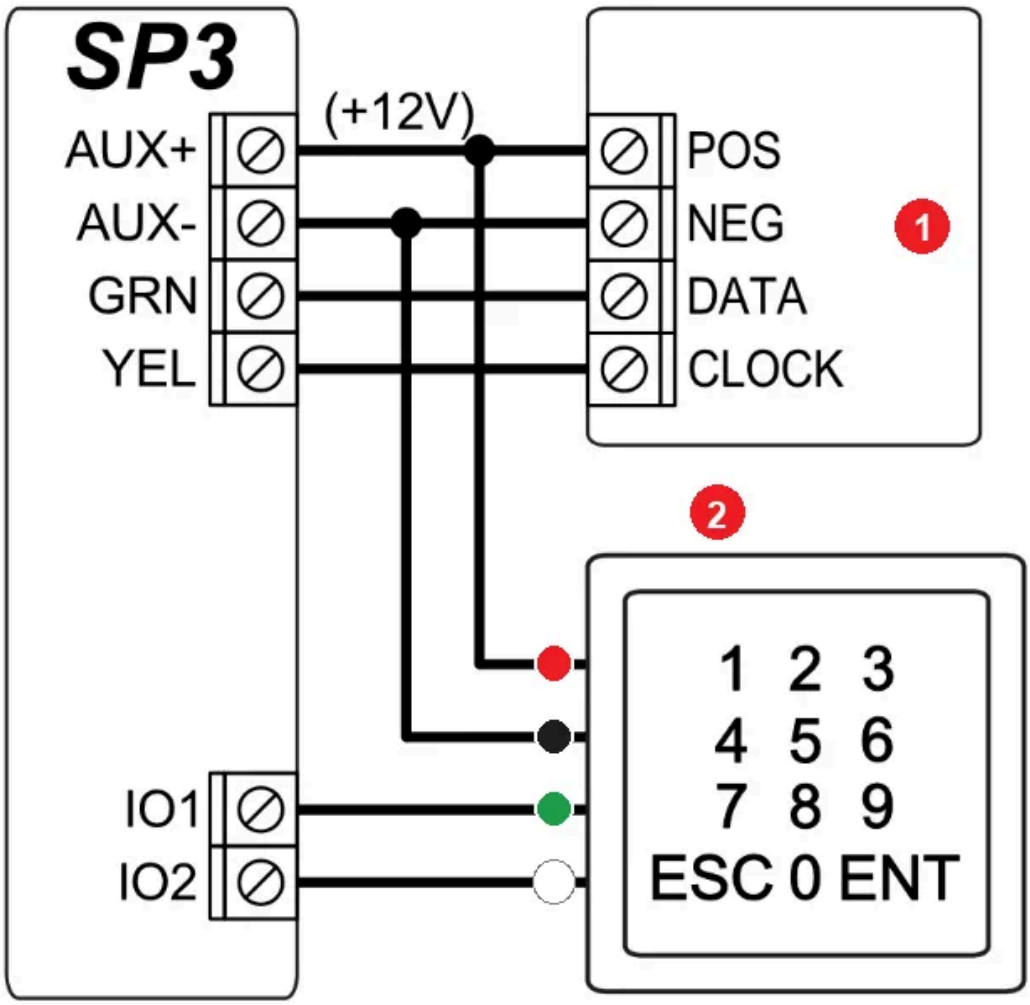


Figura 24. Teclado Crow CR16 o Crow CR-LCD y lector de entrada juntos. El teclado en el bus: AUX+ (+12 V) → POS, AUX− → NEG, GRN → DATA, YEL → CLOCK; el cable rojo del lector (+U) → AUX+, el negro (GND) → AUX−, el verde (D0) → IO1, el blanco (D1) → IO2.

- 1 teclado (“Keypad”)
- 2 lector de entrada: lector RFID con teclado, Wiegand 26/34 (“Entry reader”, “RFID reader with keypad (Wiegand 26/34)”)
- cable rojo, +U (“R - red wire (+U)”)
- cable negro, GND (“B - black wire (GND)”)
- cable verde, D0 (“G - green wire (D0)”)
- cable blanco, D1 (“W - white wire (D1)”)

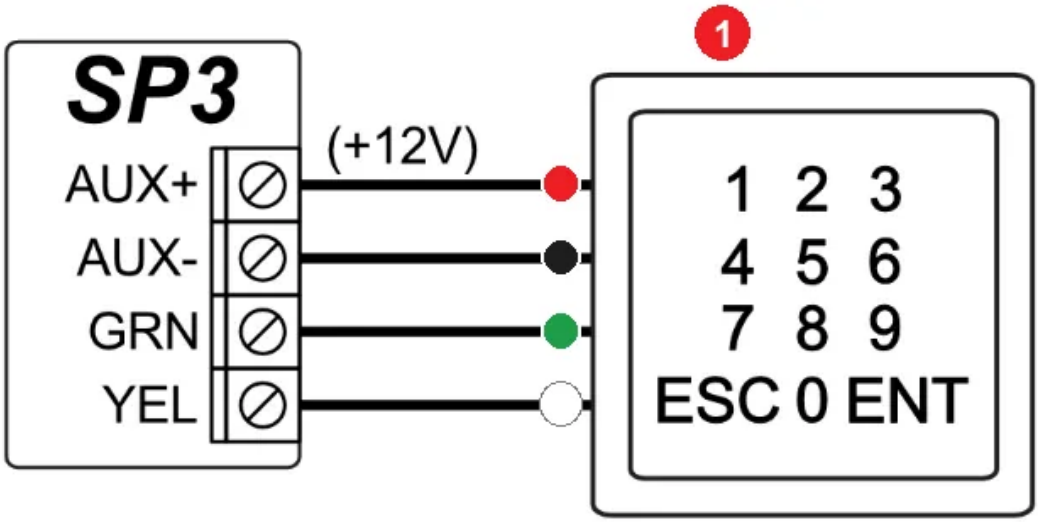


Figura 25. Un solo lector en el bus de teclados, sin teclado: el cable rojo del lector (+U) → AUX+, el negro (GND) → AUX−, el verde (D0) → GRN, el blanco (D1) → YEL.

- 1 lector de entrada: lector RFID con teclado, Wiegand 26/34 (“Entry reader“, “RFID reader with keypad (Wiegand 26/34)“)
- cable rojo, +U (“R - red wire (+U)“)
- cable negro, GND (“B - black wire (GND)“)
- cable verde, D0 (“G - green wire (D0)“)
- cable blanco, D1 (“W - white wire (D1)“)

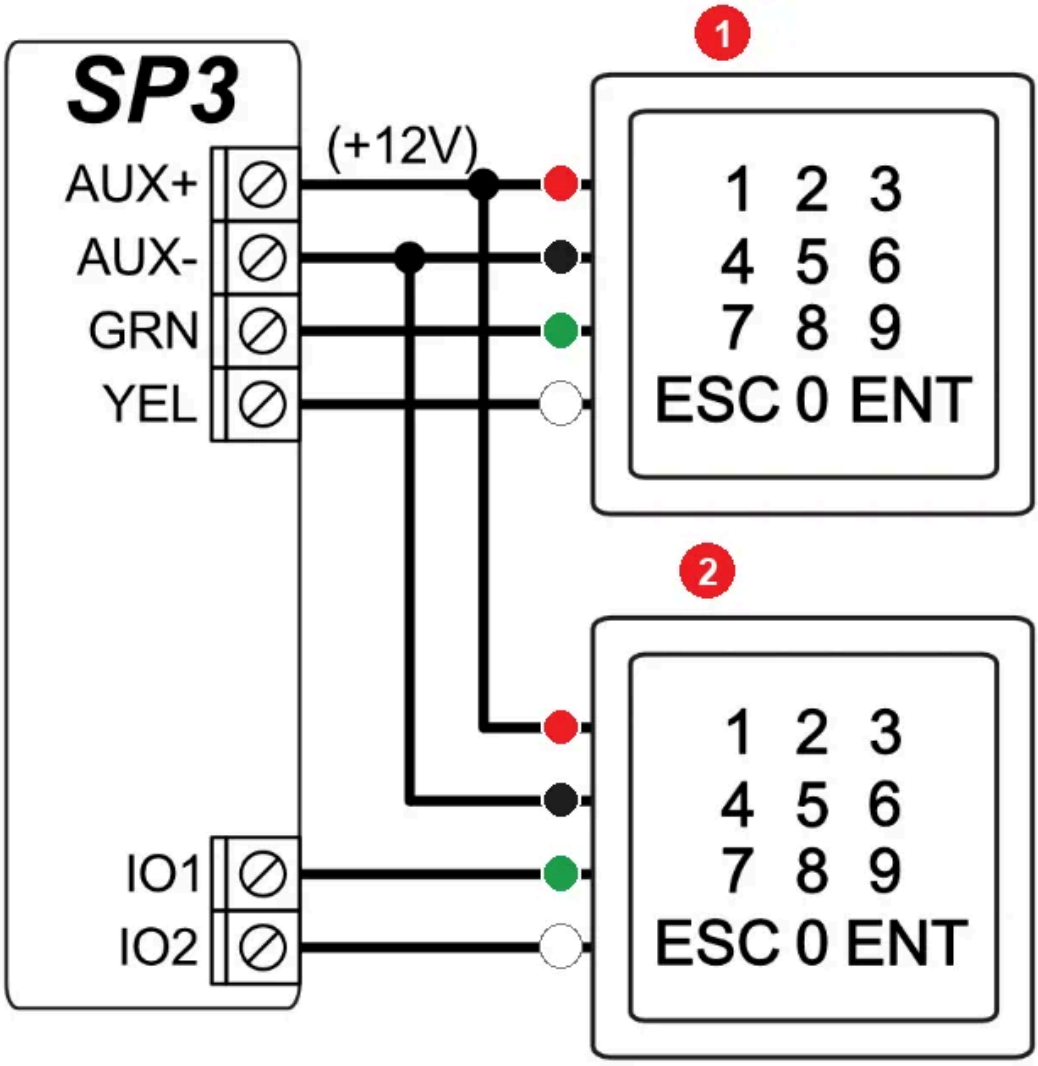


Figura 26. Dos lectores, los dos lectores RFID con teclado, Wiegand 26/34 ("RFID reader with keypad (Wiegand 26/34)"). Lector de entrada: cable rojo (+U) → AUX+, negro (GND) → AUX−, verde (D0) → GRN, blanco (D1) → YEL. Lector de salida: rojo (+U) → AUX+, negro (GND) → AUX−, verde (D0) → IO1, blanco (D1) → IO2.

- 1 lector de entrada ("Entry reader")
- 2 lector de salida ("Exit reader")
- cable rojo, +U ("R - red wire (+U)")
- cable negro, GND ("B - black wire (GND)")
- cable verde, D0 ("G - green wire (D0)")
- cable blanco, D1 ("W - white wire (D1)")

3.6 Conexión de los lectores de llaves TM17 y CZ-Dallas

Accesorio descatalogado

El lector de llaves iButton **TM17** es un accesorio descatalogado que ya no está a la venta. La descripción se mantiene para los sistemas existentes.

El lector de llaves iButton **CZ-Dallas** se conecta al bus **1 WIRE**, con un cable de 30 m como máximo. El lector **TM17** se conecta al bus **RS485**, con un cable de 100 m como máximo.

Los valores "30 m como máximo" y "100 m como máximo" son máximos teóricos, en condiciones ideales: ver la nota del apartado 1.3.

Para la indicación luminosa del CZ-Dallas, ajusta el tipo de la salida **LED** al valor **System state** (estado del sistema) (6.8): con el sistema armado el aro del lector es rojo, y con el sistema desarmado, amarillo.

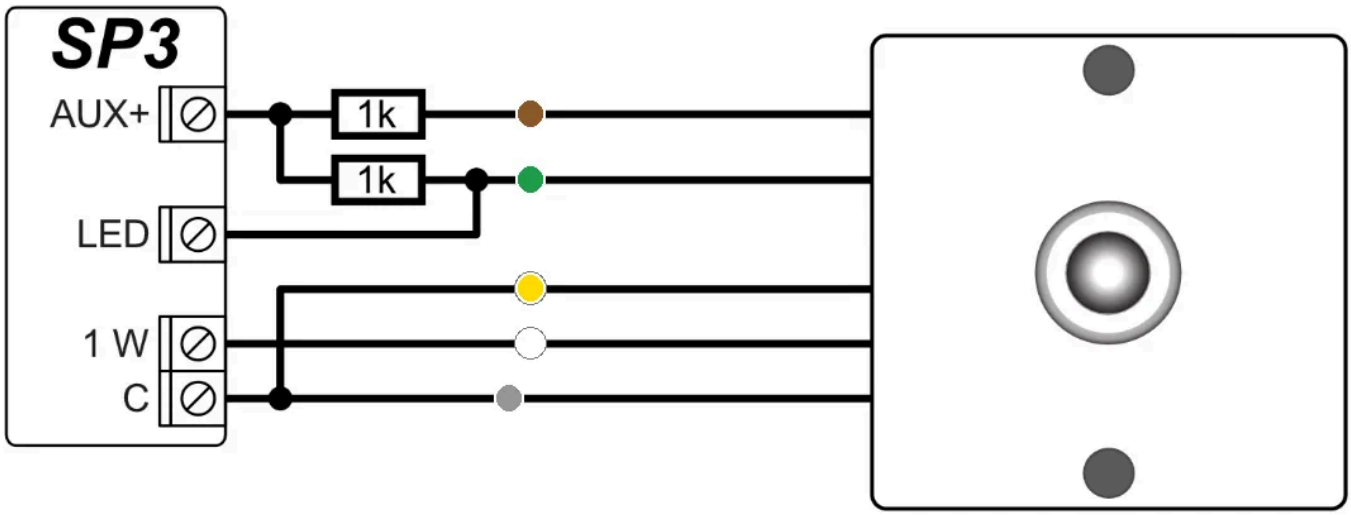


Figura 27. Lector CZ-Dallas (“CZ-Dallas reader”): AUX+ → a través de sendas resistencias de 1 kΩ, a los cables marrón (RED LED+) y verde (GREEN LED+); la salida LED al cable verde, después de la resistencia; 1 W → cable blanco; C → cables amarillo (LED−) y gris. La salida LED hay que ajustarla al tipo **System state** (estado del sistema) (“The output LED must be set to the »System state« type.”): con la alarma armada, la luz del lector iButton es roja (“Security alarm system is arm - the iButton reader light is red.”), y desarmada, amarilla (“Security alarm system is disarm - the iButton reader light is yellow.”).

- cable marrón, RED LED+ (“Brown wire”, “RED LED+”): la luz roja
- cable verde, GREEN LED+ (“Green wire”, “GREEN LED+”): la luz verde
- cable amarillo, LED− (“Yellow wire”, “LED-”)
- cable blanco (“White wire”)
- cable gris (“Gray wire”)

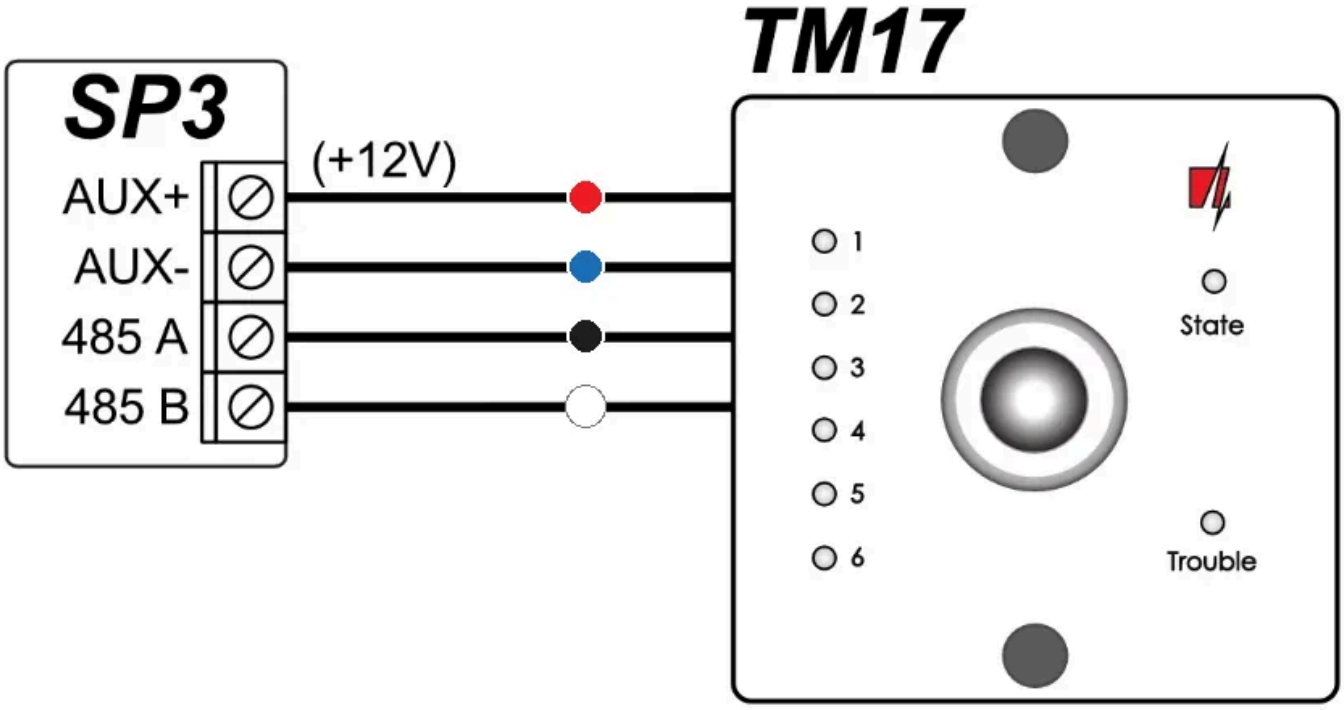


Figura 28. Lector TM17: AUX+ (+12 V) → cable rojo, AUX− → azul, 485 A → negro, 485 B → blanco.

- cable rojo (“Red wire”)
- cable azul (“Blue wire”)
- cable negro (“Black wire”)
- cable blanco (“White wire”)

3.7 Conexión de los sensores de temperatura

Al bus 1 WIRE se pueden conectar como máximo **8 sensores de temperatura Maxim / Dallas DS18S20 o DS18B20**, o **1 sensor de temperatura y humedad AM2301**; la central los reconoce y los asigna automáticamente, y los valores se ven en la página **Sensors** (6.9). Para cables de más de medio metro, usa cable de pares trenzados (UTP 4×2×0,5 o STP 4×2×0,5). El borne **+5V** de la placa alimenta los equipos conectados al bus 1 WIRE: 5 V DC, máximo 0,2 A, protegido contra sobrecarga; si se supera la corriente admitida, la salida se desconecta automáticamente.

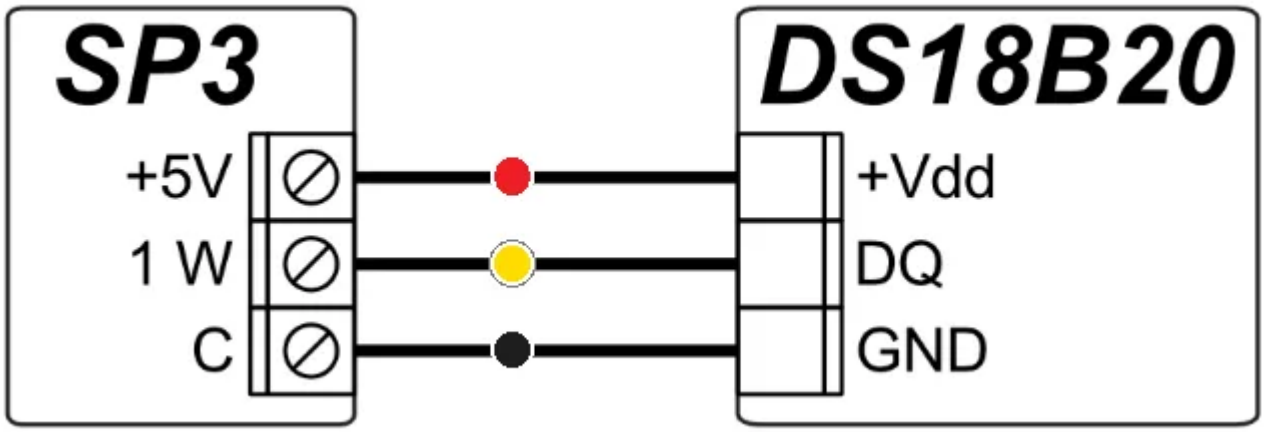


Figura 29. Sensor de temperatura DS18B20 (“Temperature sensor”): +5V → +Vdd (rojo), 1 W → DQ (amarillo), C → GND (negro).

- cable rojo (“Red wire”)
- cable amarillo (“Yellow wire”)
- cable negro (“Black wire”)

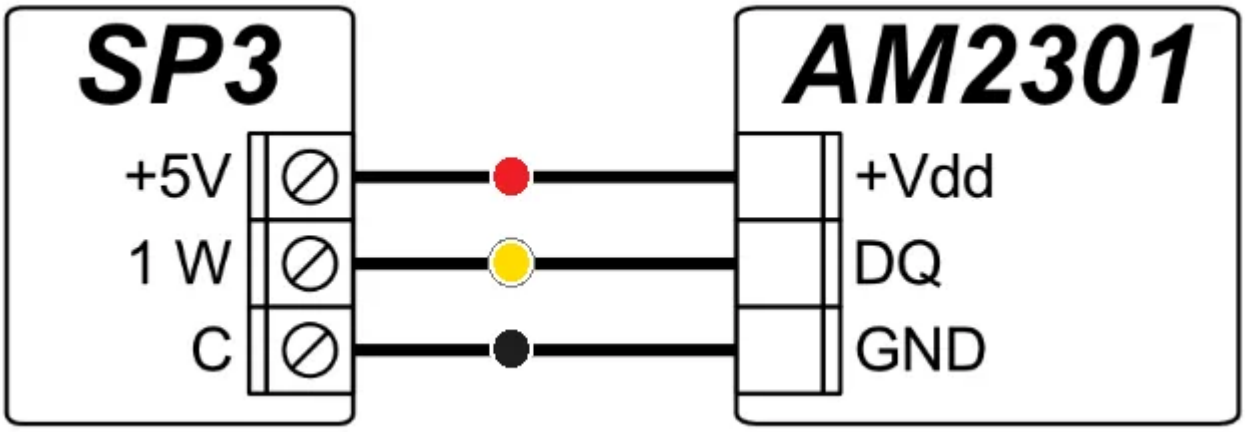


Figura 30. Sensor de temperatura y humedad AM2301 (“Temperature and humidity sensor”): +5V → +Vdd (rojo), 1 W → DQ (amarillo), C → GND (negro).

- cable rojo (“Red wire”)
- cable amarillo (“Yellow wire”)
- cable negro (“Black wire”)

3.8 Conexión de un relé y de un piloto LED

Con los contactos del relé se pueden conmutar a distancia distintos equipos eléctricos. El borne IO elegido hay que configurarlo como salida (OUT), con la función **Remote control** (control remoto) (6.8). La salida IO es de colector abierto y admite como máximo 100 mA, así que los consumos mayores conmútalos siempre a través de un relé.

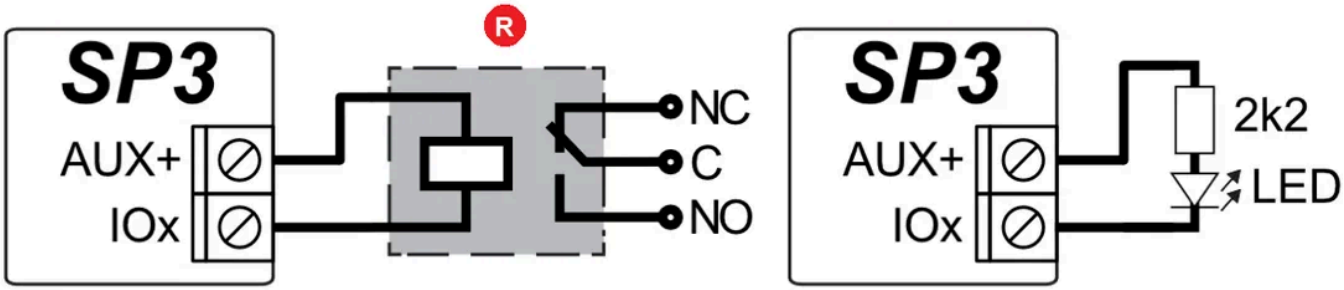


Figura 31. A la izquierda, relé: la bobina entre AUX+ e IOx; los contactos del relé, NC, C, NO. A la derecha, piloto LED: AUX+ → resistencia de 2,2 kΩ → LED → IOx.

- R relé (“Relay”)

3.9 Encendido de la central

Da la alimentación de red. Los LED de la placa muestran lo siguiente (la tabla completa está en el apartado 1.6):

- el LED **PWR** parpadea en verde: la tensión de alimentación es correcta;
- en la versión con módem, el LED **NET** está verde fijo y de vez en cuando destella en amarillo al menos tres veces: el verde indica que la tarjeta SIM se ha conectado a la red móvil, y el número de destellos amarillos (0–5), la intensidad de la señal;
- en la versión Wi-Fi, el LED **MOD** parpadea en verde mientras la central se conecta a la red Wi-Fi, y queda verde fijo cuando la conexión se ha establecido.

La intensidad de señal móvil adecuada es **3** (tres destellos amarillos del LED NET). Si destella menos veces, la intensidad de la señal de la red móvil no es suficiente: elige otro lugar para la central o para la antena, o usa una antena más sensible. Si los LED muestran otra cosa, la causa se encuentra en la tabla del apartado 1.6. Si no se enciende ningún LED de la central, comprueba la alimentación y las conexiones.

4. Conexión de expansores y módulos vía radio

La mayoría de los expansores y de los módulos de comunicación se conectan al bus de datos **RS485**. La alimentación del módulo la dan los bornes **AUX+** (+12 V) y **AUX−**; los hilos de datos van a los bornes **485 A** y **485 B**, siempre A → A, B → B. Al bus se pueden conectar como máximo **8 equipos**, y la longitud del cable del bus es de **100 m** como máximo. La excepción es el receptor Paradox RTX3, que se conecta al bus de teclados (GRN, YEL) (4.3). Los módulos se configuran en la página **Modules** (6.5), y los equipos vía radio se añaden en la página **Wireless** (6.6).

El valor "100 m como máximo" es un máximo teórico, en condiciones ideales: ver la nota del apartado 1.3.

De los receptores vía radio, cada versión del firmware solo admite el suyo; la tabla completa de las versiones y de los módulos admitidos está en el apartado 1.7.

Módulo	Sistema vía radio	Firmware necesario (1.7)
RF-SH	Crow	SP3_xxx0, versión 1.01 o posterior (SP3_xxx0_0101)
RTX3	Paradox	SP3_xxx1, versión 1.12 o posterior (SP3_xxx1_0112)
RF-HW	Honeywell	SP3_xxx2, versión 1.14 o posterior (SP3_xxx2_0114)
RF-S8	S8	SP3_xxx4, versión 1.22 o posterior (SP3_xxx4_0122)
RF-LORA	equipos LoRa "Maximum"	para los equipos inalámbricos MAXIMUM, SP3_xxx4, versión 1.21 o posterior (SP3_xxx4_0121); para los expansores LORA, cualquier versión
E485, T16, SF485, iO, iO-8, iO-WL, iO-MOD, expansores LORA	–	cualquier versión

4.1 Módulo Ethernet E485

Con el módulo E485, la central envía y recibe los informes de eventos y los comandos de control por internet por cable. Si hay un E485 conectado a la central, los informes a la CRA y a Protegus 2 van por internet por cable y no se usa internet móvil; si la conexión por cable se corta, la central pasa a internet móvil y, cuando se restablece la conexión por cable, vuelve a ella automáticamente. La prioridad de los canales (SIM, Wi-Fi, LAN – E485) se ajusta en la página **Reporting to CMS** (6.3), y la configuración del E485 en la página **Modules** (6.5). Con el E485, la central no necesita tarjeta SIM.

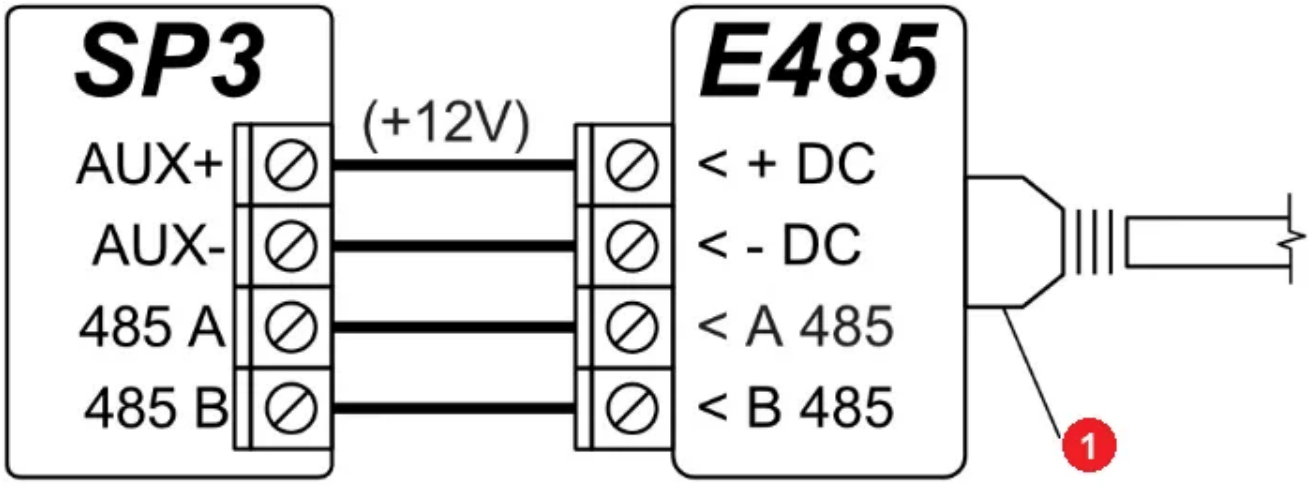


Figura 32. Módulo Ethernet E485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; en el conector RJ45 del E485, el cable LAN. Conexión RS485 (“RS485 connection”), hasta 100 m (“up to 100 m”).

- 1 cable LAN (“LAN cable”)

Las distancias «hasta … m» son máximos teóricos que se alcanzan en condiciones ideales. En la práctica, la calidad y el recorrido del cable, las fuentes de interferencias y, en los enlaces de radio, las paredes y el terreno dan un alcance bastante menor. Planifica con margen y, en tramos largos, comprueba la conexión durante la puesta en marcha.

4.2 Receptor vía radio RF-SH (Crow)

Con el receptor RF-SH, la central gestiona los equipos inalámbricos Crow: como máximo 32 detectores, 16 sirenas, 42 mandos a distancia y 8 teclados vía radio. Firmware necesario: SP3_xxx0_0101 o posterior (1.7).

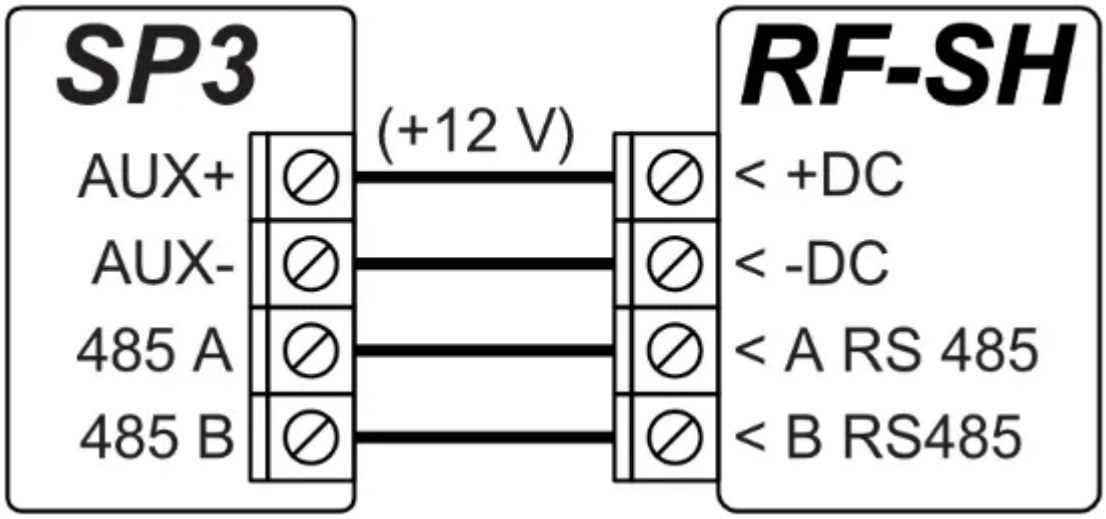


Figura 33. RF-SH: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

4.3 Receptor vía radio RTX3 (Paradox)

El receptor RTX3 no se conecta al bus RS485, sino al **bus de teclados**. Con él, la central gestiona los equipos inalámbricos Paradox: detectores de apertura, detectores de movimiento, el detector de rotura de cristal G550, el detector de humo SD360, los mandos a distancia REM2 y REM25, las sirenas SR230 y SR250, el teclado K37,

el expansor de PGM y zonas 2WPGM y el repetidor RPT1. Firmware necesario: SP3_xxx1_0112 o posterior (1.7). El firmware del RTX3, su conexión y el alta y la baja de los equipos Paradox se tratan en un artículo aparte: FLEXi SP3 y el módulo de expansión inalámbrico Paradox RTX3.

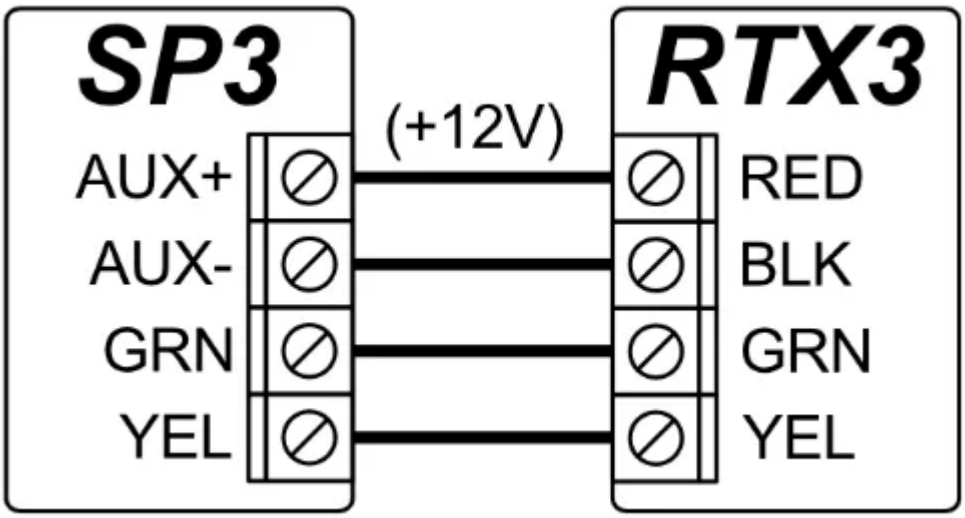


Figura 34. RTX3 en el bus de teclados: AUX+ (+12 V) → RED, AUX− → BLK, GRN → GRN, YEL → YEL.

4.4 Receptor vía radio RF-HW (Honeywell)

Con el receptor RF-HW, la central gestiona los detectores, sirenas, teclados y mandos a distancia inalámbricos de Honeywell. Firmware necesario: SP3_xxx2_0114 o posterior (1.7).

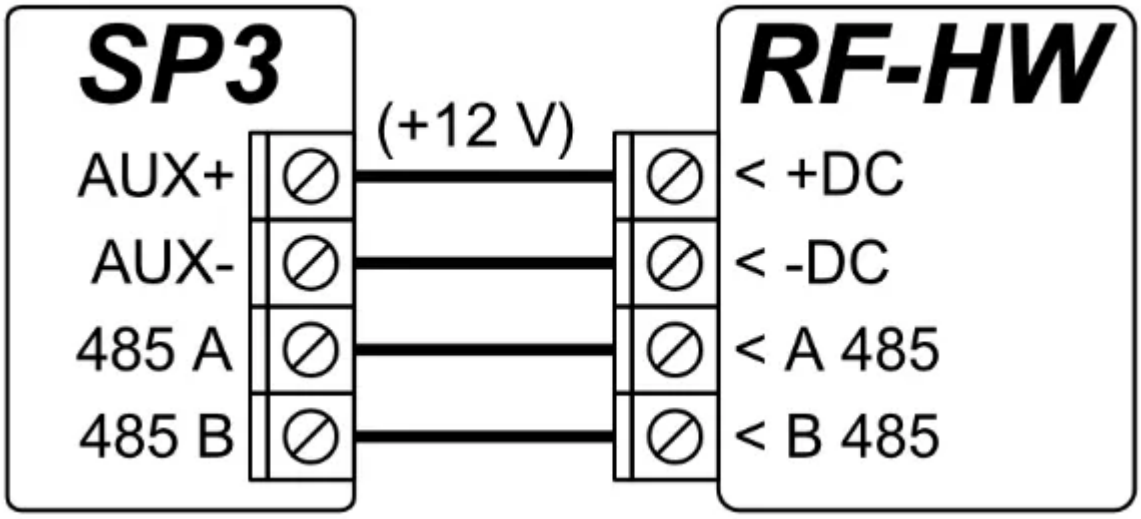


Figura 35. RF-HW: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.5 Receptor vía radio RF-S8

Con el receptor RF-S8, la central gestiona los detectores, sirenas y mandos a distancia inalámbricos S8. Firmware necesario: SP3_xxx4_0122 o posterior (1.7). El registro del RF-S8, el cambio de su firmware y el emparejamiento de los equipos S8 se describen en un manual aparte: Manual del transceptor RF-S8 y de los detectores S8.

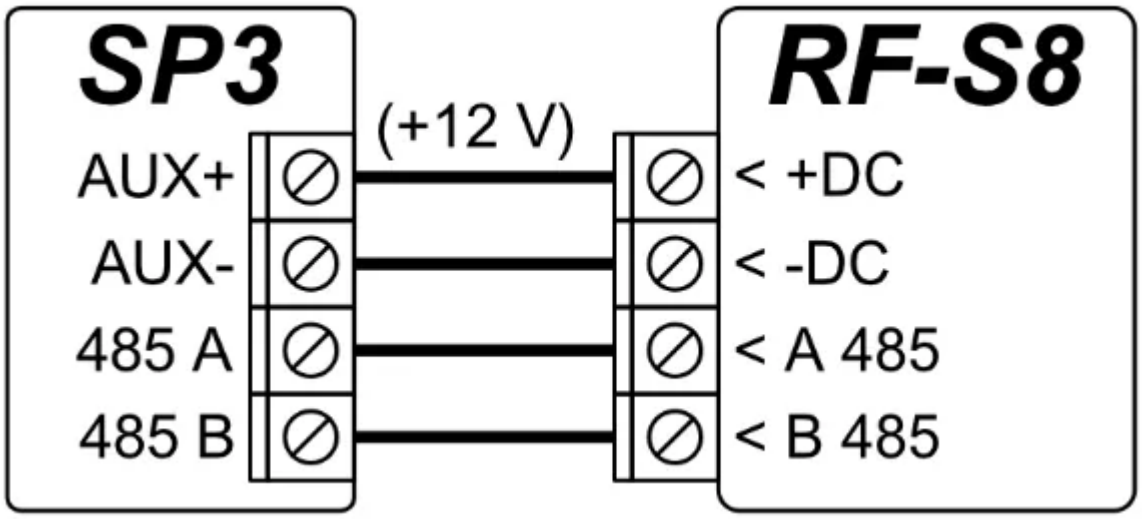


Figura 36. RF-S8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.6 Receptor vía radio RF-LORA

Con el receptor RF-LORA, la central gestiona los equipos vía radio LoRa de "Maximum": como máximo 32 detectores, 16 sirenas y 32 mandos a distancia, además de los expansores LORA (4.7). Para los detectores, sirenas y mandos a distancia MAXIMUM hace falta el firmware SP3_xxx4, versión 1.21 o posterior; los expansores LORA funcionan con cualquier versión del firmware (1.7). El receptor se configura en la página **Modules** (6.5), y los equipos se añaden en la página **Wireless** (6.6).

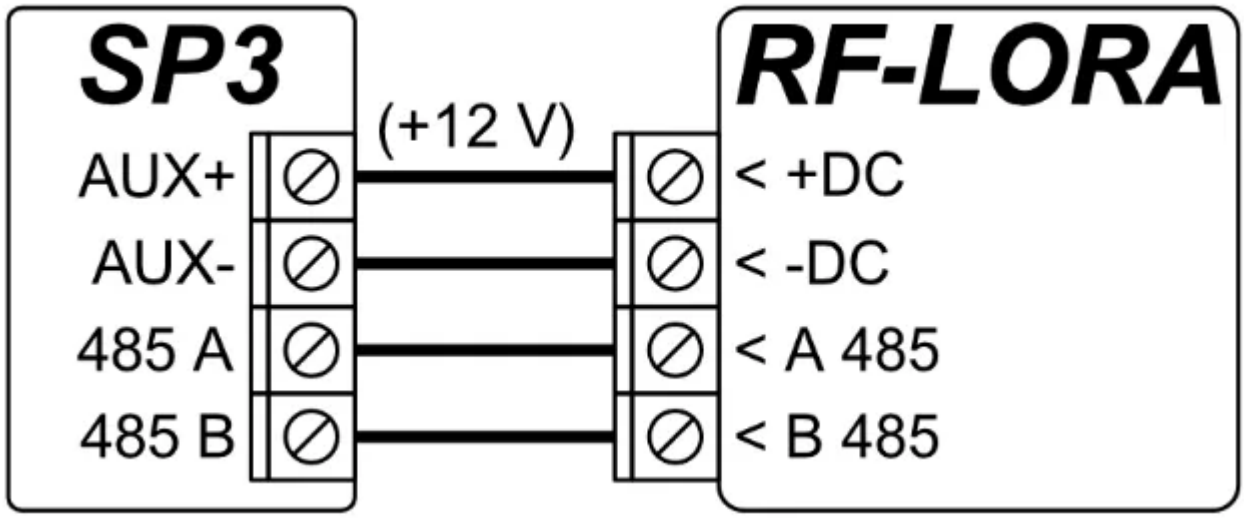


Figura 37. RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.7 Expansores LORA

Los expansores LORA (iO-LORA, iO8-LORA, PB-LORA, REL-LORA) se conectan a la central vía radio a través del receptor RF-LORA, desde un máximo de 5000 m. **iO-LORA**: expansor de entradas y salidas con conexión para lector iButton CZ-Dallas, alimentado a 12 V DC; un lector Wiegand conectado a él no funciona con la SP3. **iO8-LORA**: expansor de ocho entradas/salidas, alimentado a 12–26 V, con todos los tipos de circuito de la central (3.2). **PB-LORA**: pulsador de pánico. **REL-LORA**: módulo de relé, alimentado a 100–230 V AC.

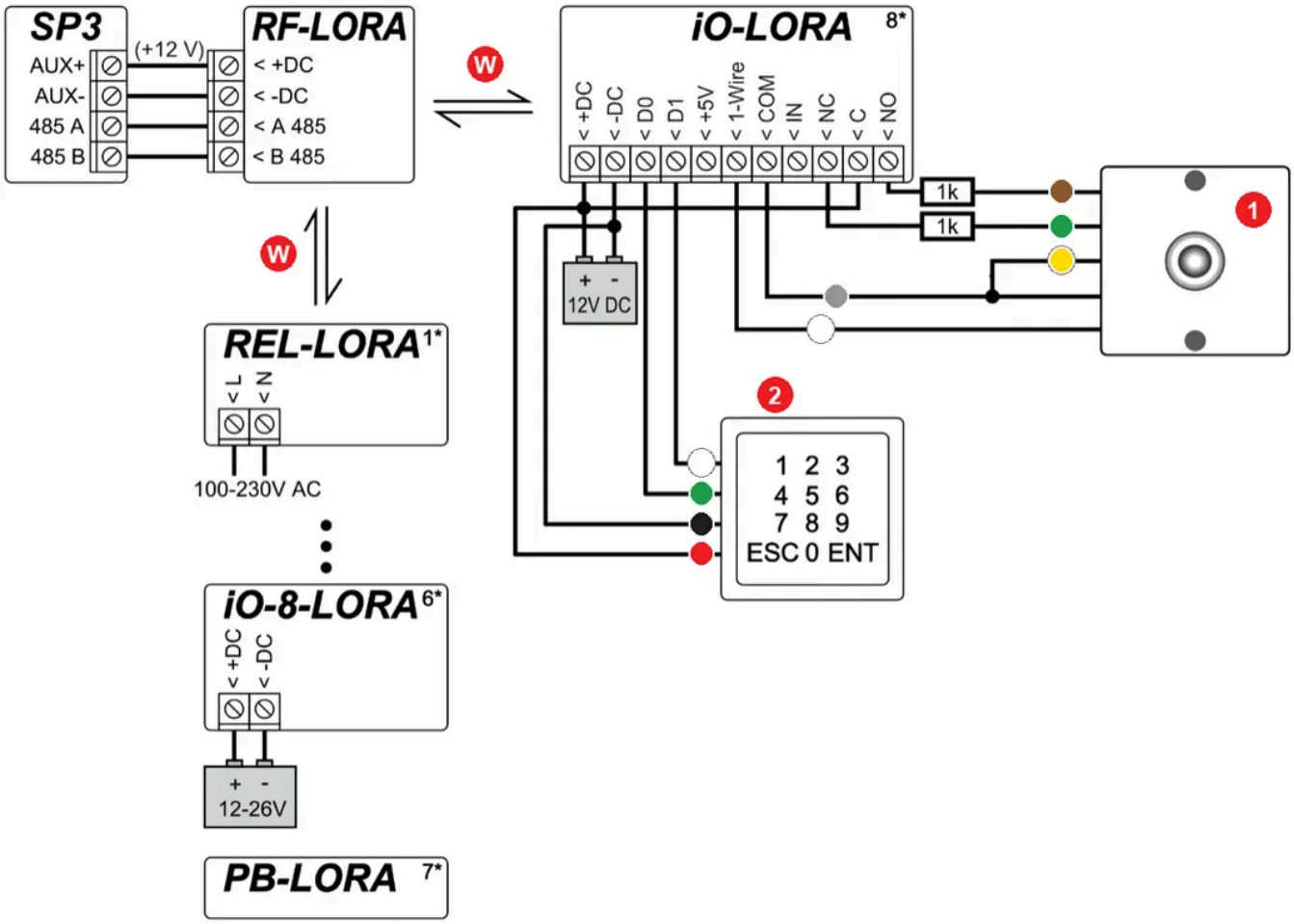


Figura 38. Expansores LORA a través del receptor RF-LORA. SP3 → RF-LORA: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485; el RF-LORA llega vía radio, desde un máximo de 5000 m, a las unidades iO-LORA, iO8-LORA, PB-LORA y REL-LORA. REL-LORA: L, N → 100–230 V AC. iO8-LORA: +DC, −DC → 12–26 V. iO-LORA: +DC, −DC → 12 V DC; el cable rojo del lector de entrada (+U) → +DC, el negro (GND) → −DC, el verde (D0) → D0, el blanco (D1) → D1; la conexión 1-Wire del lector CZ-Dallas, hasta 30 m ("1-Wire connection up to 30 m"): 1-Wire → blanco, COM → gris y amarillo (LED−), C → +DC, NO → 1 kΩ → marrón (RED LED+), NC → 1 kΩ → verde (Green LED+). La salida xOUT hay que ajustarla al tipo **System State** (estado del sistema) ("The output xOUT must be set to the »System State« type."): con la alarma armada, la luz del lector iButton es roja ("Security alarm is on - the iButton reader light is red."), y desarmada, verde ("The security alarm is off - the iButton reader light is green.").

- 1 lector iButton CZ-Dallas ("CZ-Dallas reader")
- 2 lector de entrada: lector RFID con teclado, Wiegand 26/34 ("Entry reader", "RFID reader with keypad (Wiegand 26/34)"); con la FLEXi SP3 no funciona así
- W conexión inalámbrica ("Wireless connection"), hasta 5000 m ("up to 5000 m")
- cable marrón, RED LED+ ("Brown wire", "RED LED+"): la luz roja
- cable verde: en el lector CZ-Dallas, Green LED+, la luz verde ("Green wire", "Green LED+"); en el lector de entrada, D0 ("G - green wire (D0)")
- cable amarillo, LED− ("Yellow wire", "LED-")
- cable gris ("Gray wire")
- cable blanco ("White wire"); en el lector de entrada, D1 ("W - white wire (D1)")
- cable rojo, +U ("R - red wire (+U)")
- cable negro, GND ("B - black wire (GND)")

El lector de entrada (2) conectado al iO-LORA en el dibujo no funciona con la FLEXi SP3. Conecta el lector RFID directamente a la central (3.5).

Las distancias «hasta … m» son máximos teóricos que se alcanzan en condiciones ideales. En la práctica, la calidad y el recorrido del cable, las fuentes de interferencias y, en los enlaces de radio, las paredes y el terreno dan un alcance bastante menor. Planifica con margen y, en tramos largos, comprueba la conexión durante la puesta en marcha.

4.8 Expansores de la serie iO

Si la central necesita más entradas (IN) o salidas (OUT), conéctale un expansor Trikdis de la serie iO, cableado o inalámbrico (iO, iO-8, iO-WL, iO-MOD). **iO**: expansor de entradas/salidas con conexión 1-Wire. **iO-8**: expansor de ocho entradas/salidas, con todos los tipos de circuito de la central (3.2). **iO-WL**: expansor inalámbrico que se conecta a la central a través del transceptor **iO-MOD**, desde un máximo de 300 m; también se puede conectar por cable al bus RS485. En el sistema puede haber como máximo 8 módulos de expansión y como máximo 4 iO-MOD. Los expansores se configuran en la página **Modules** (6.5).

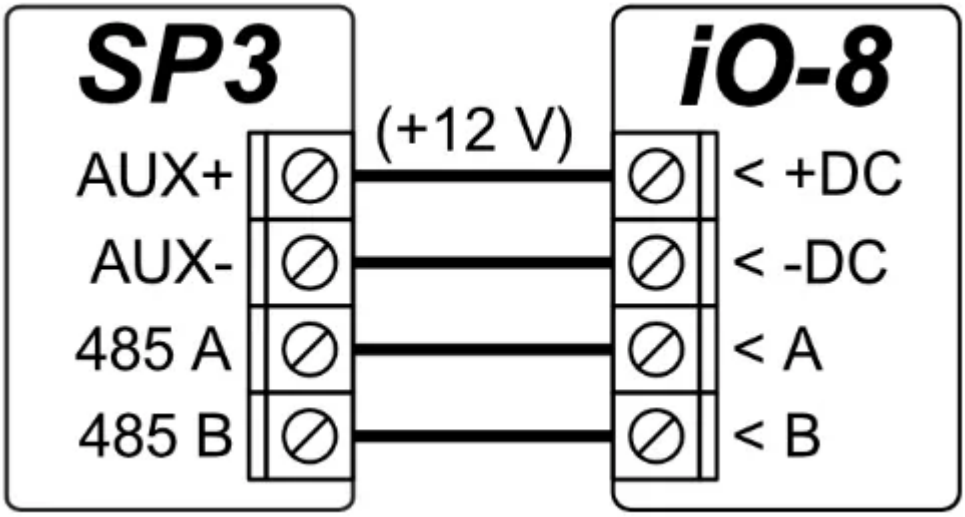


Figura 39. iO-8: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A, 485 B → B.

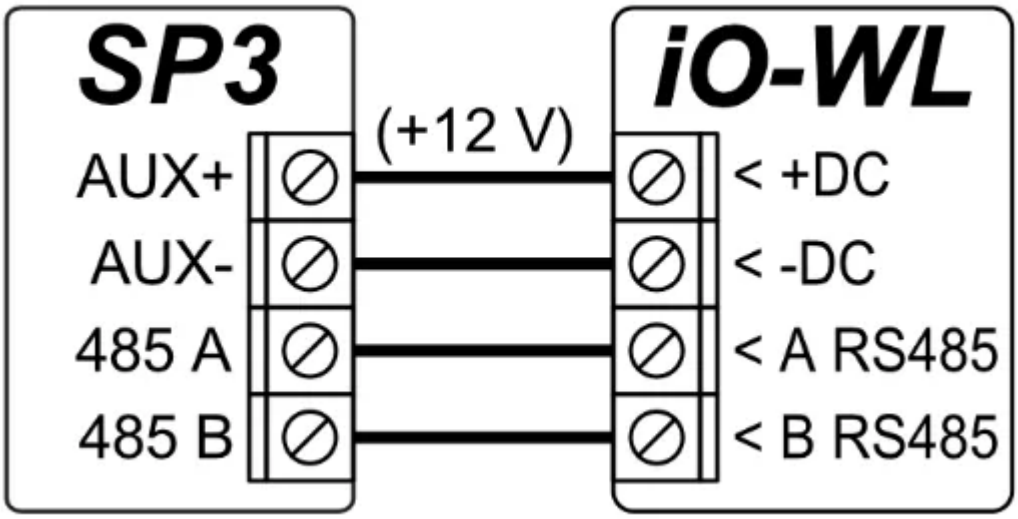


Figura 40. iO-WL por cable: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A RS485, 485 B → B RS485.

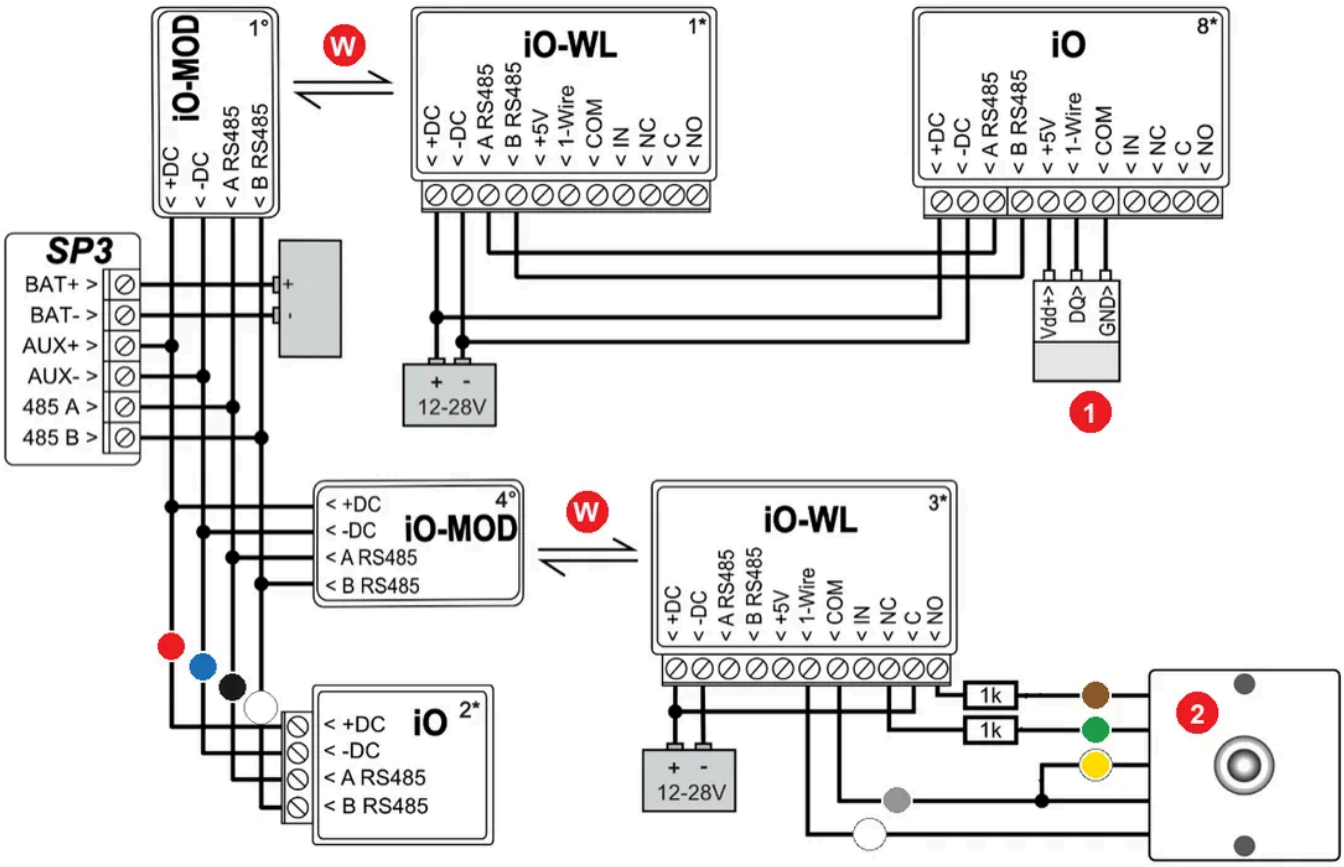


Figura 41. Vista general del sistema iO. SP3: BAT+ / BAT− → batería de 12 V (“Battery 12V”); AUX+ (rojo) y AUX− (azul) → +DC y −DC de las unidades iO-MOD e iO; 485 A (negro) y 485 B (blanco) → A RS485 y B RS485. Cada uno de los dos iO-MOD llega vía radio, desde un máximo de 300 m, a una unidad iO-WL. El iO-WL y el iO de arriba funcionan con una alimentación común de 12–28 V, con conexión RS485 entre ellos (“RS485 connection”), hasta 300 m (“up to 300 m”); los bornes +5V, 1-Wire y COM del iO → Vdd+, DQ y GND de un sensor de temperatura DS18B20 / DS18S20. El iO-WL de abajo (12–28 V) gestiona un lector CZ-Dallas, con la conexión 1-Wire hasta 30 m (“1-Wire connection up to 30 m”): 1-Wire → blanco, COM → gris y amarillo (LED−), C → +DC, NO → 1 kΩ → marrón (RED LED+), NC → 1 kΩ → verde (Green LED+). La salida xOUT hay que ajustarla al tipo **System State** (estado del sistema) (“The output xOUT must be set to the »System State« type.”): con la alarma armada, la luz del lector iButton es roja (“Security alarm is on - the iButton reader light is red.”), y desarmada, verde (“The security alarm is off - the iButton reader light is green.”). De las unidades marcadas con asterisco puede haber como máximo 8 módulos de expansión del sistema (“* up to 8 system expansion modules”), y de las marcadas con °, como máximo 4 módulos iO-MOD (“° up to 4 iO-MOD modules”).

- 1 sensor de temperatura, DS18B20 o DS18S20 (“Temperature sensor: DS18B20 or DS18S20”)
- 2 lector iButton CZ-Dallas (“CZ-Dallas reader”)
- W conexión inalámbrica (“Wireless connection”), hasta 300 m (“up to 300 m”)
- cable rojo (“Red wire”)
- cable azul (“Blue wire”)
- cable negro (“Black wire”)
- cable blanco (“White wire”)
- cable marrón, RED LED+ (“Brown wire”, “RED LED+”): la luz roja
- cable verde, Green LED+ (“Green wire”, “Green LED+”): la luz verde
- cable amarillo, LED− (“Yellow wire”, “LED-”)
- cable gris (“Gray wire”)

Las distancias «hasta … m» son máximos teóricos que se alcanzan en condiciones ideales. En la práctica, la calidad y el recorrido del cable, las fuentes de interferencias y, en los enlaces de radio, las paredes y el terreno dan un alcance bastante menor. Planifica con margen y, en tramos largos, comprueba la conexión durante la puesta en marcha.

4.9 Transmisor vía radio T16

El transmisor vía radio VHF/UHF T16 transmite los eventos de la central a la CRA por la red de radio de Trikdis: envía tanto sus propios eventos como los que recibe de la central, y la CRA puede reenviarlos al usuario.

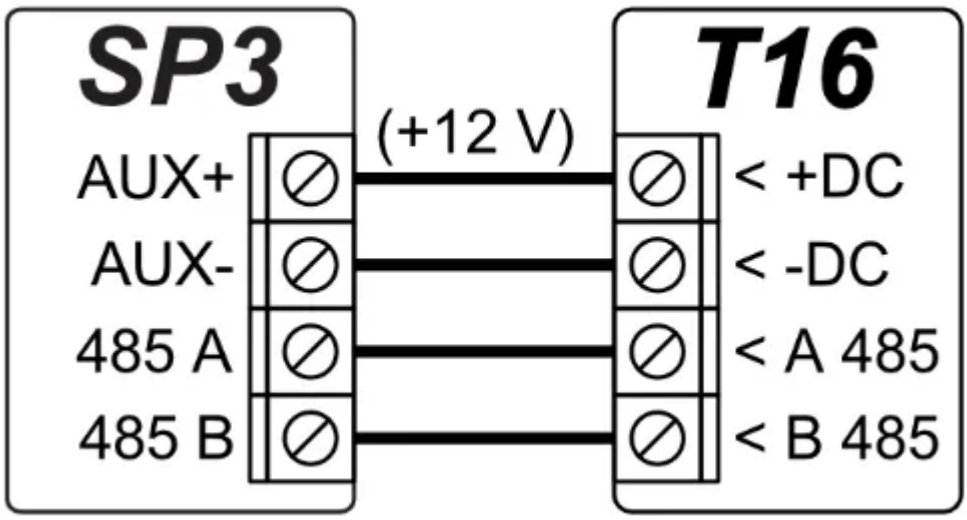


Figura 42. T16: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.10 Módulo Sigfox SF485

El SF485 es un canal de respaldo: si falla el canal principal, envía los eventos de la central por la red Sigfox a la CRA o a la aplicación Protegus 2, en formato Contact ID.

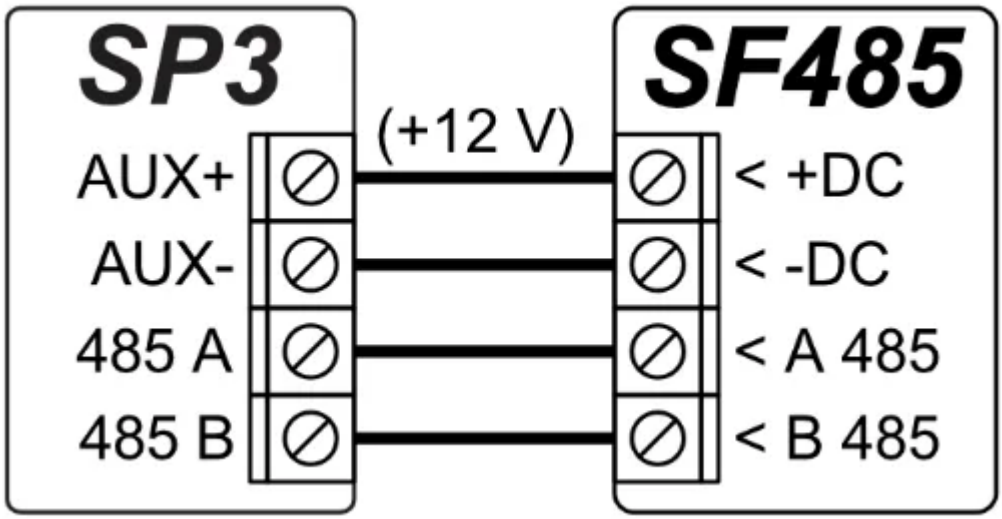


Figura 43. SF485: AUX+ (+12 V) → +DC, AUX− → −DC, 485 A → A 485, 485 B → B 485.

4.11 Medición de tensión continua

La central puede medir una tensión continua de 0–30 V; **por encima de 30 V la placa se daña**. El polo positivo de la tensión medida va a IO1 (en el dibujo de Trikdis, IN1) y el negativo, al borne C.

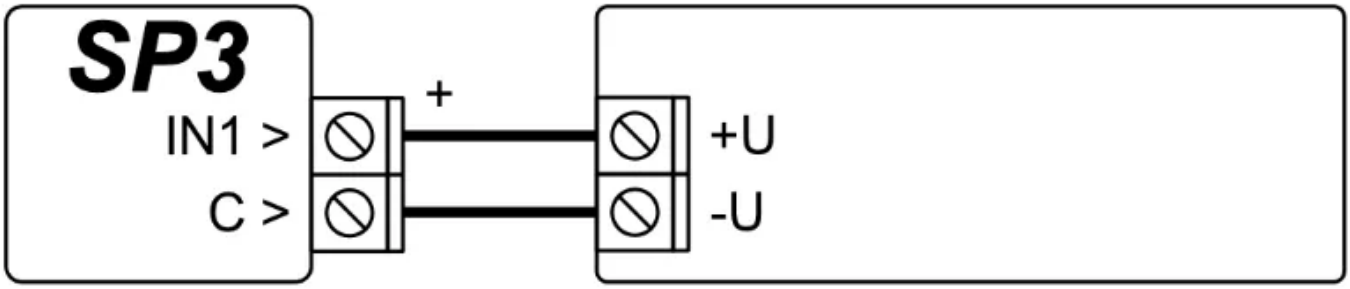


Figura 44. Medición de tensión: el equipo medido (“Equipment whose voltage is measured”) +U → IO1 (en el dibujo, IN1), −U → C.

Conecta la central al ordenador con el cable USB e inicia TrikdisConfig (capítulo 6); el programa reconoce automáticamente la central conectada y abre su ventana de configuración. En la página **Sensors**, añade el sensor **In1 Voltage** y los valores límite:

- **Max**: por encima de esta tensión se genera un evento, si la casilla **High** está marcada;
- **Min**: por debajo de esta tensión se genera un evento, si la casilla **Low** está marcada.

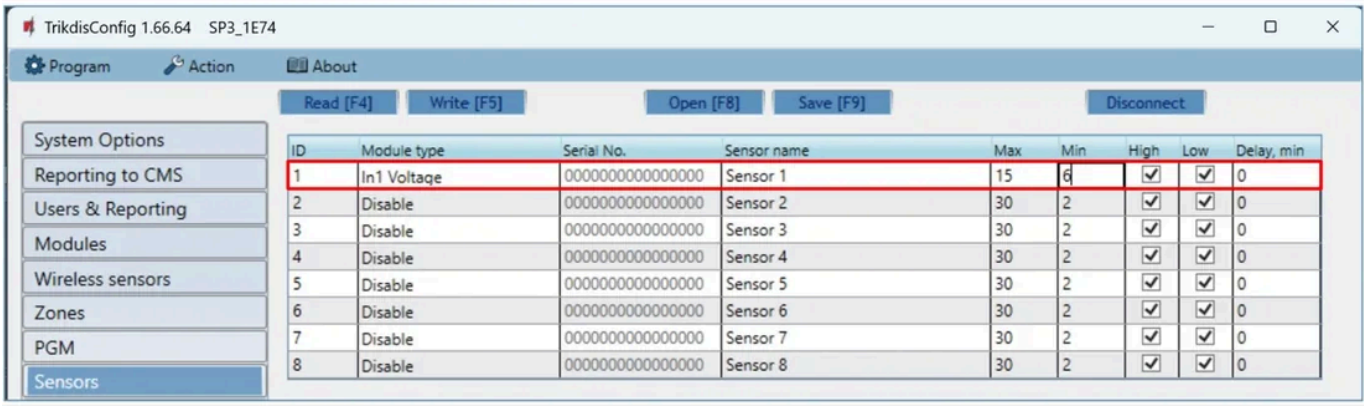


Figura 45. La página Sensors: el sensor In1 Voltage con el identificador 1, Max 15, Min 6, High y Low marcadas, Delay 0 minutos.

La tensión medida también puede controlar una salida PGM. En la pestaña **Outputs** de la página **PGM**, pon la salida en el modo **Remote Control** y, después, en la pestaña **Set Action**, indica la condición:

- **Enable**: activa la PGM;
- **PGM No.**: la salida PGM controlada;
- **Action**: el funcionamiento de la salida: **PGM OFF** (se apaga), **PGM ON** (se enciende), **Pulse OFF** (con el comando se apaga durante el tiempo del impulso y después vuelve a encenderse), **Pulse ON** (se enciende durante el tiempo del impulso y después se apaga);
- **Pulse time, s**: la duración del impulso, 0–9999 s;
- **Factor**: el origen de la condición: **Sensor**;
- **Factor No.**: la entrada de medición de tensión (S1);
- **Start when**: la condición: **Higher than set** (por encima del valor ajustado) o **Lower than set** (por debajo);
- **Set value**: la tensión vigilada (V).

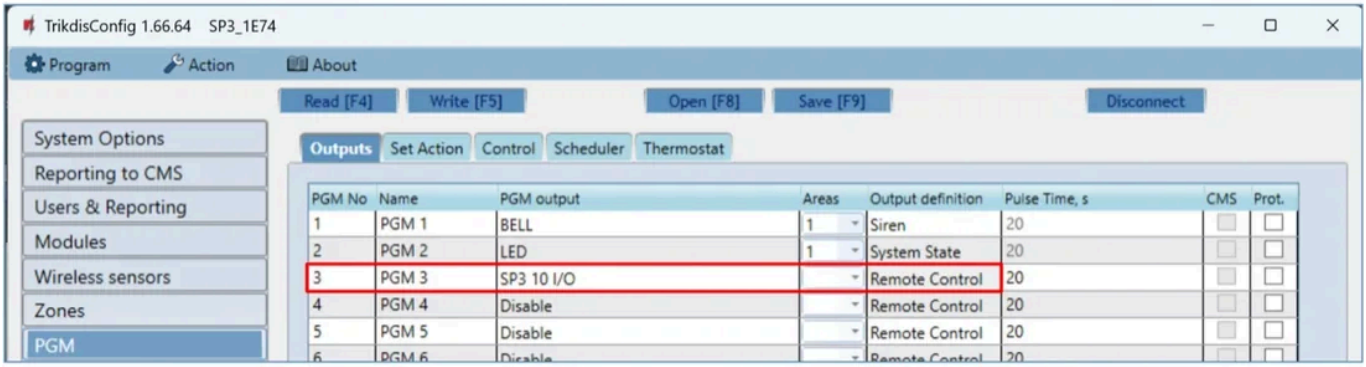


Figura 46. La pestaña Outputs de la página PGM: la PGM 3 en el borne de E/S 10 de la SP3, con el tipo Remote Control y un tiempo de impulso de 20 s.

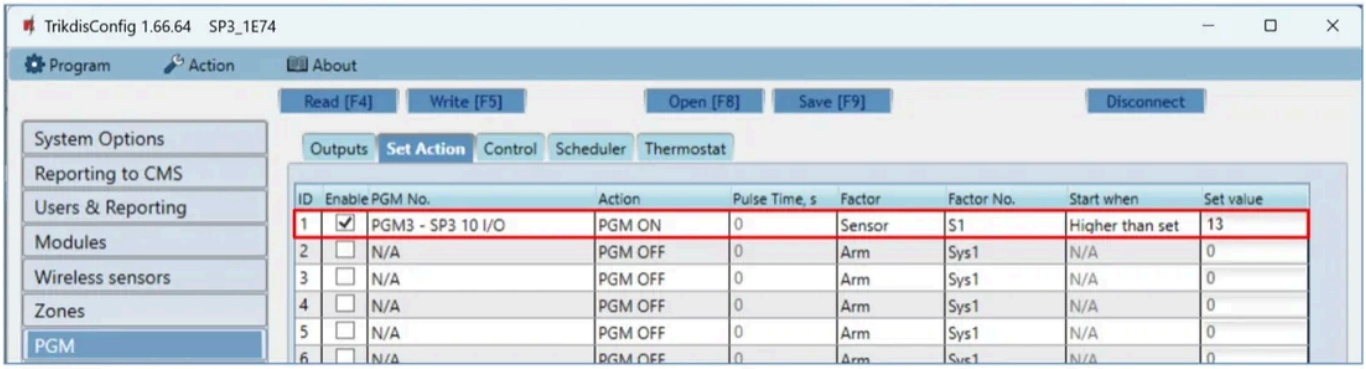


Figura 47. La pestaña Set Action: Enable marcada, PGM No. PGM3, Action PGM ON, Pulse Time 0, Factor Sensor, Factor No. S1, Start when Higher than set, Set value 13 V.

5. Protegus 2 y control remoto

La "FLEXi" SP3 se puede controlar a distancia de tres maneras: desde la aplicación Protegus 2, por SMS y por llamada telefónica. La aplicación funciona en todas las versiones que tienen acceso a internet (WiFi, Ethernet o red móvil). Los comandos SMS y el control por llamada solo están disponibles en las versiones con módem de red móvil (por ejemplo, SP3_24E, SP3_44E, SP3_12E) y solo con una tarjeta SIM operativa. La versión SP3_3E (WiFi + Ethernet) no tiene módem.

5.1 Vinculación con la cuenta de Protegus 2

En Protegus 2, el usuario arma y desarma el sistema, ve el estado de las zonas y de las particiones y recibe avisos de los eventos. Antes de añadir la central a la cuenta, comprueba lo siguiente:

- **Alimentación**: el LED **POWER** está verde fijo.
- **Red**: el LED **NET** está verde fijo (red móvil) y/o el LED **MOD** está verde fijo (módulo WiFi o Ethernet). El significado de los LED se describe en el apartado 1.6.
- **Tarjeta SIM**: en la versión con módem, la SIM está activa y has introducido el código PIN en TrikdisConfig (**System Options** → **SIM** → **PIN**), o has desactivado la petición del PIN en la tarjeta.
- **Servicio en la nube**: en la pestaña **Users & Reporting** → **Protegus** de TrikdisConfig está marcada la casilla **Enable cloud service** (6.4). El valor de fábrica del **Cloud access code** es 123456; si lo cambias, la aplicación te pedirá el código nuevo al añadir el sistema.
- **Identificador único**: el número **IMEI/Unique ID** de la central lo encontrarás en la etiqueta del embalaje y de la placa, y también se ve en la esquina inferior izquierda de TrikdisConfig después de leer la central.

Si todavía no tienes una cuenta de Protegus, créala en www.protegus.app con el enlace **Sign up** y actívala haciendo clic en el enlace que recibirás por correo electrónico; después instala la aplicación Protegus 2 en tu teléfono y entra con tu nombre de usuario y tu contraseña.

A rendszer létrehozása a Protegus 2 alkalmazásban

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

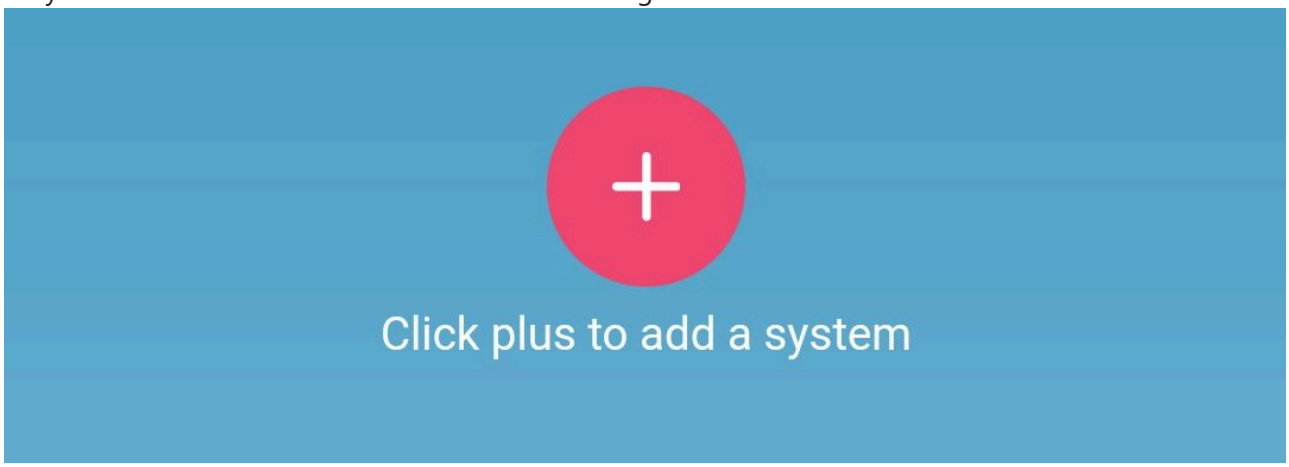
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

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

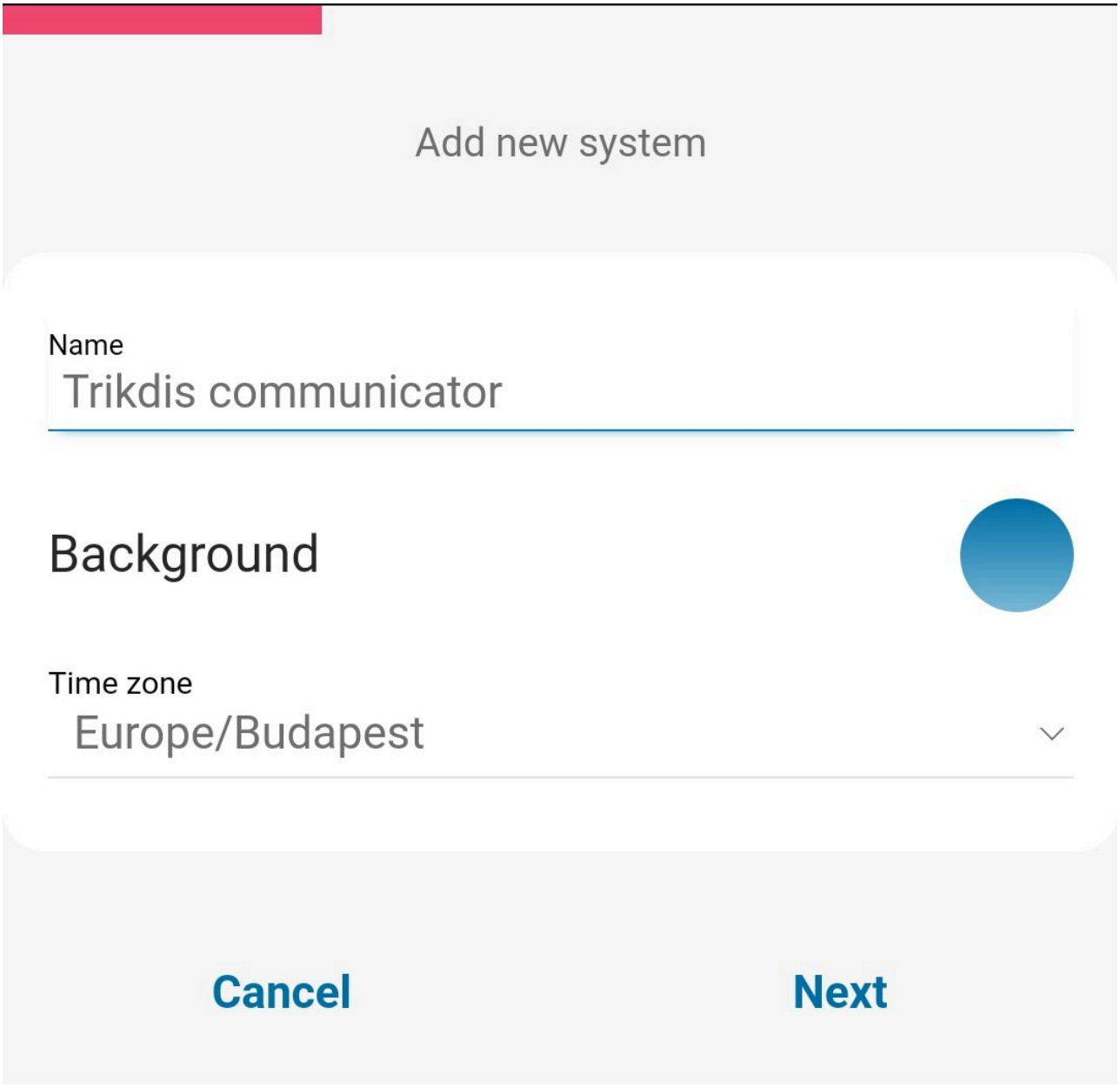


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán

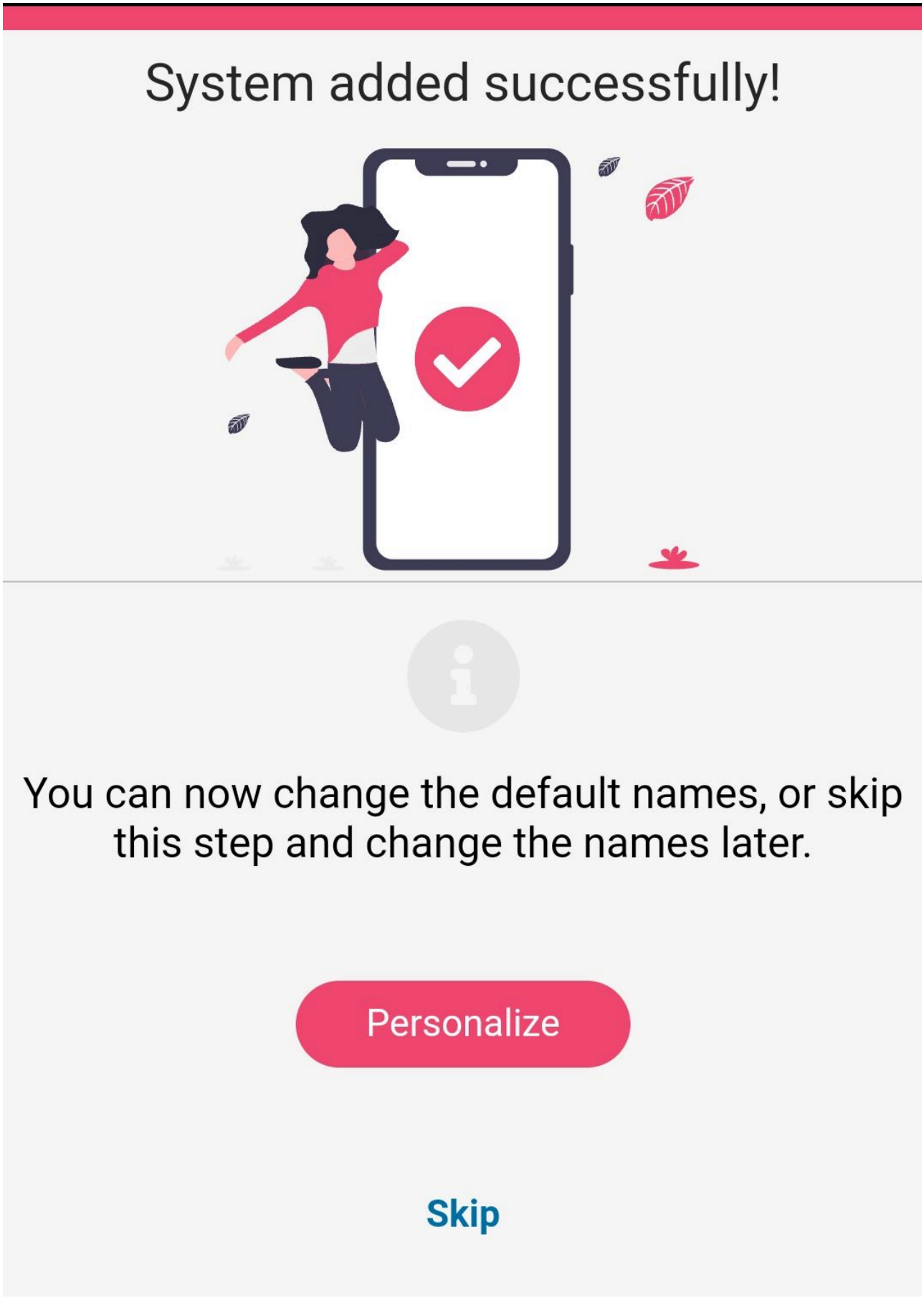
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



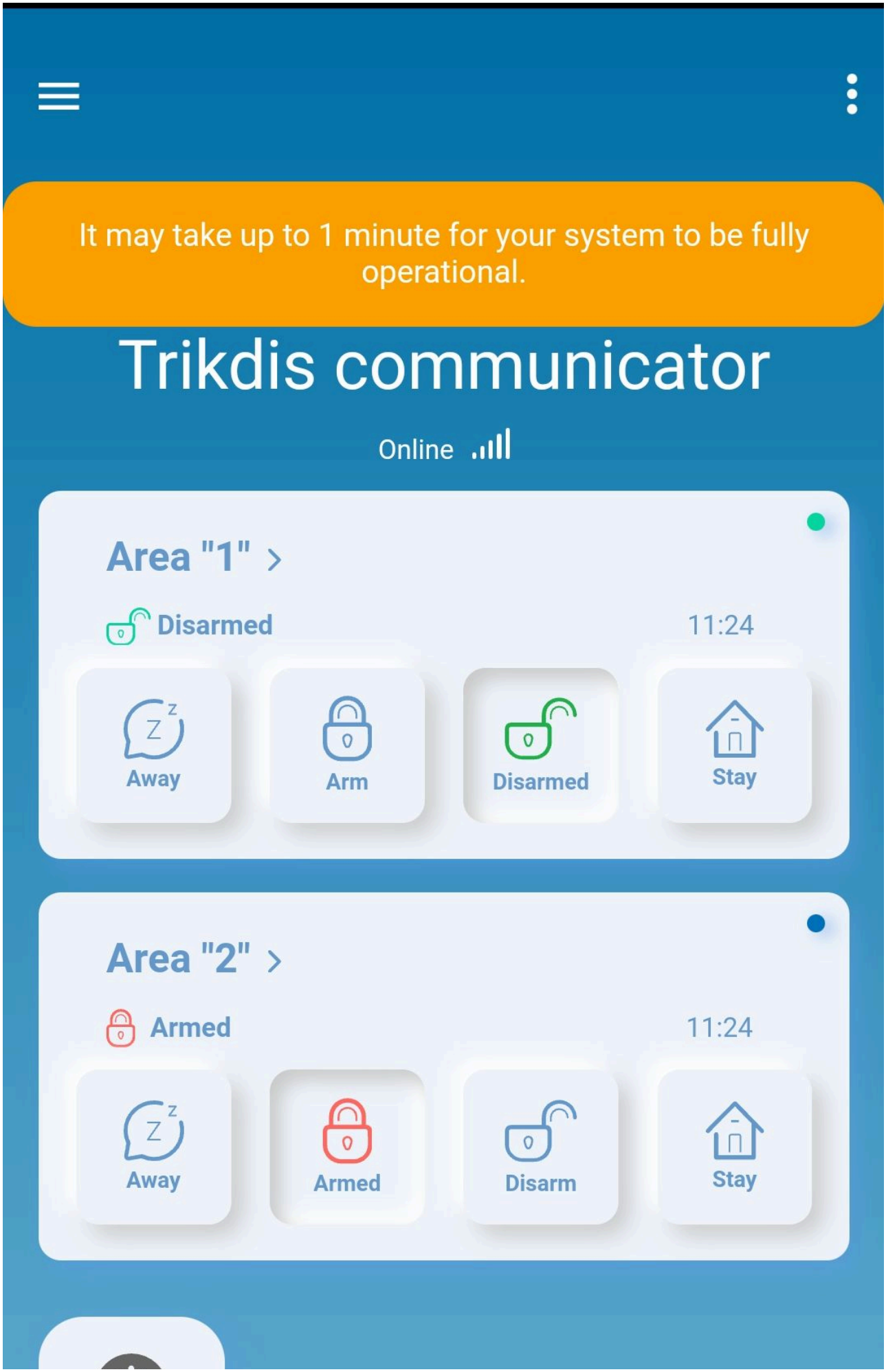
6. Add meg a rendszer nevét és válassz idozónát



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



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


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

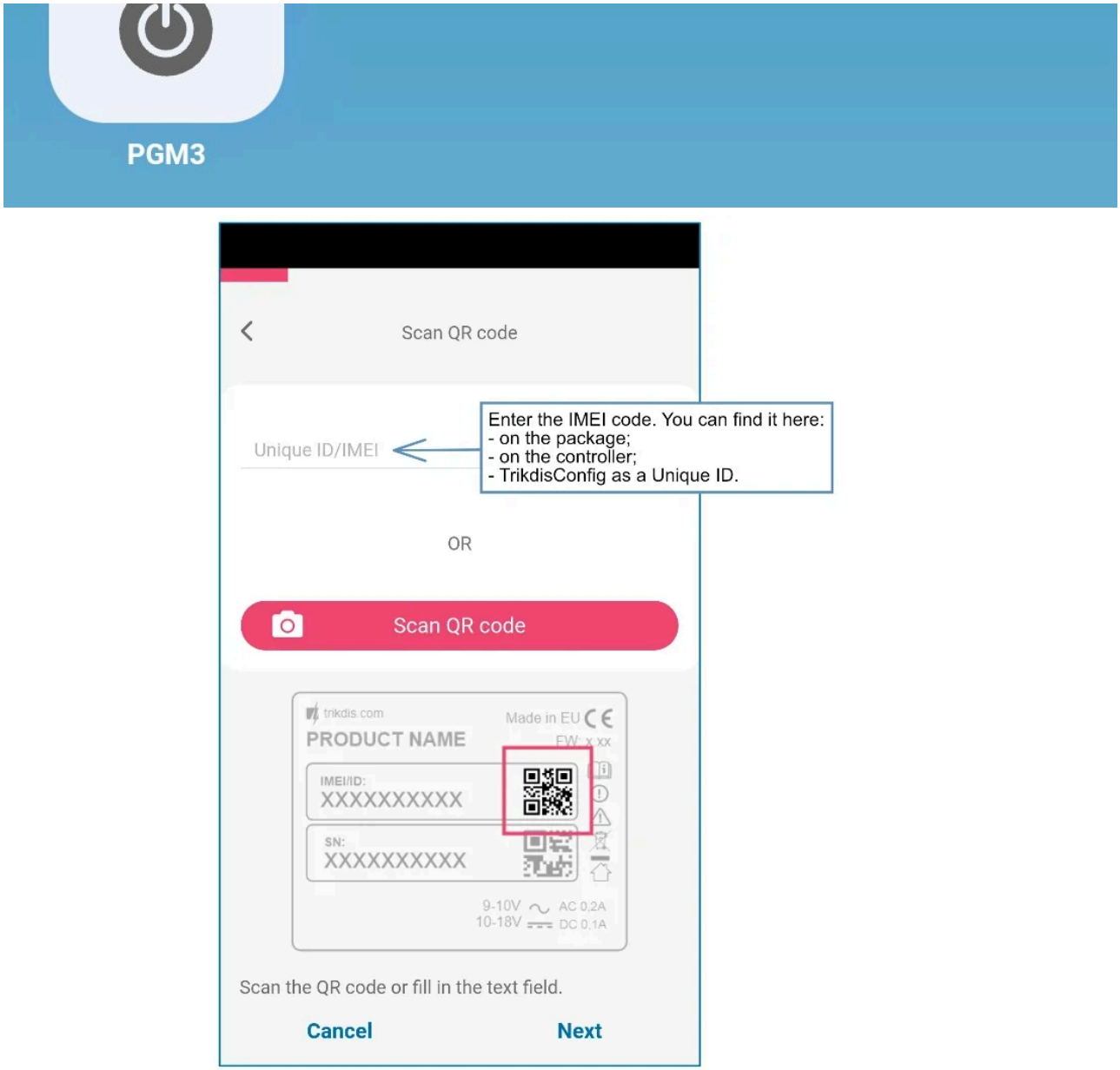


Figura 48. Añadir el sistema en Protegus 2: escribes el número **IMEI/Unique ID** o lees con la cámara el código QR de la etiqueta.

Más usuarios

El propietario puede invitar a más usuarios en Protegus 2. A las direcciones escritas en la columna **Email** de la pestaña **Users & Reporting** → **Users** de TrikdisConfig el sistema también envía una invitación, así el usuario ve el sistema desde su propia cuenta (6.4).

5.2 Armado y desarmado en la aplicación

1. Abre el sistema en la aplicación Protegus 2. En la pantalla de inicio, cada partición tiene su propia tarjeta y su candado: el **candado cerrado y rojo** indica una partición armada; el **candado abierto y verde**, una partición desarmada.
2. Toca el candado de la partición y elige la operación que quieras: armar o desarmar.
3. Si la aplicación lo pide, introduce el código PIN.

El candado adopta el estado real a partir del evento que llega de la central de alarma; la aplicación también confirma en la lista de eventos y con una notificación si la central ha ejecutado la operación.

En la SP3, después de tocar el candado tienes que introducir el **código de usuario** de la central. Es el código que figura en la columna **Code** de la pestaña **Users & Reporting** → **Users** de TrikdisConfig, no la contraseña de la cuenta de Protegus 2. Cada partición aparece en una tarjeta aparte, y solo ves las particiones para las que el usuario tiene permiso en la columna **Areas**. Además del armado total, desde la aplicación también activas los modos parciales: **Stay** (te quedas en casa, las zonas interiores no se arman) y **Sleep** (modo noche). En qué modo vigila una zona lo decide el campo **Definition** de la zona (6.7).

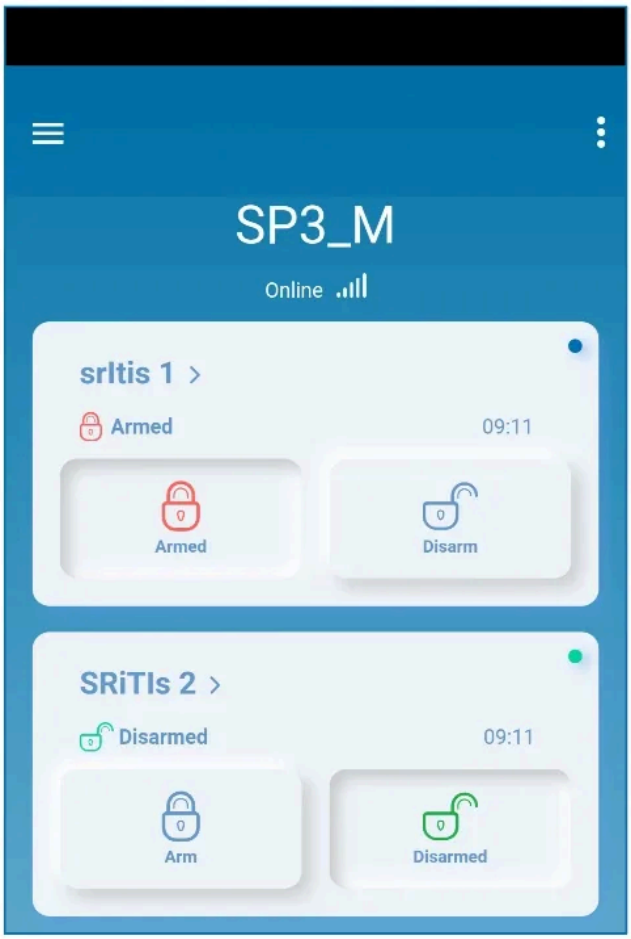


Figura 49. Dos particiones en Protegus 2: la 1 armada (rojo, candado cerrado) y la 2 desarmada (verde, candado abierto).

Si la aplicación no sigue a la central

Si los comandos no hacen nada, o la aplicación muestra algo muy distinto del estado real de la central, abre en Protegus 2 el menú **Settings** → **System configuration** y, en la línea **System out of sync?**, pulsa el botón **Sync**. La aplicación vuelve a leer la configuración de la central.

5.3 Configuración y control por SMS

Solo en las versiones con módem. El SMS lo envías al número de la tarjeta SIM de la central. Todos los mensajes tienen la misma estructura:

Comando espacio **Contraseña** espacio **Datos**

La contraseña es la **SMS password** de seis dígitos (**System Options** → **Access**, 6.2). Su valor de fábrica es **123456**. Por seguridad, al poner en marcha el sistema cámbiala por una contraseña que solo conozcas tú, en TrikdisConfig o con el comando `PSW` (y no la olvides), y no des sin necesidad el número de la tarjeta SIM de la

central. El campo de datos depende del comando; en varios comandos está vacío.

¿Quién puede enviar comandos?

El administrador puede controlar la central por SMS y por llamada. Si quieres autorizar también a otro usuario, añade su número de teléfono en la pestaña **Users & Reporting** → **Users** de TrikdisConfig (6.4) o con el comando `SETN`. La central envía sus respuestas con los textos indicados en la pestaña **SMS answer texts**.

Comando	Datos	Qué hace	Ejemplo
INFO	–	Consulta del estado: nombre del objeto, estado de las particiones, IMEI, nivel de señal, versión de firmware, número de serie.	`INFO 123456`
RESET	–	Reinicio de la central.	`RESET 123456`
OUTPUTx	ON	Activación de la salida x.	`OUTPUT1 123456 ON`
	OFF	Desactivación de la salida x.	`OUTPUT1 123456 OFF`
	PULSE=ttt	Activación de la salida x durante ttt segundos (tres dígitos).	`OUTPUT1 123456 PULSE=002`
PSW	nueva contraseña	Cambio de la contraseña SMS.	`PSW 123456 654123`
TIME	AAAA/MM/DD,hh:mm:ss	Ajuste de la fecha y la hora.	`TIME 123456 2026/10/30,10:02:00`
TXTA	nombre del objeto	Ajuste del nombre del objeto (es el que aparece en los informes).	`TXTA 123456 Casa`
RDR	número de teléfono#texto	La central reenvía por SMS el texto que va tras el # al número indicado. El número empieza por el signo + y el prefijo del país.	`RDR 123456 +34600123456#texto reenviado`
ASKI	–	Estado de las entradas (IN) por SMS.	`ASKI 123456`
ASKO	–	Estado de las salidas (OUT) por SMS.	`ASKO 123456`
ASKA	–	Estado de las particiones por SMS.	`ASKA 123456`
ASKT	–	Valor de todos los sensores de temperatura por SMS.	`ASKT 123456`

Comando	Datos	Qué hace	Ejemplo
ARM	SYS:x	Armado de la partición x (1–8).	`ARM 123456 SYS:1`
DISARM	SYS:x	Desarmado de la partición x (1–8).	`DISARM 123456 SYS:1`
STAY	SYS:x	Armado de la partición x en modo Stay (1–8).	`STAY 123456 SYS:1`
SLEEP	SYS:x	Armado de la partición x en modo Sleep (1–8).	`SLEEP 123456 SYS:1`
FRS	–	Restablecimiento de la alimentación de los detectores de incendio, si la definición de una salida es **Fire Sensor Reset**.	`FRS 123456`
SETN	PhoneX=número#nombre#e-mail	Alta de un usuario en la fila x con número de teléfono, nombre y dirección de e-mail; el número de teléfono y el nombre van separados por el signo #. El número empieza por el signo + y el prefijo del país.	`SETN 123456 PHONE5=+34600123456#JUAN#juan@ejemplo.es`
	PhoneX=DEL	Borrado del número de teléfono y del nombre de la fila x.	`SETN 123456 PHONE5=DEL`
UUSD	*código#	Envío de un código USSD al operador móvil (por ejemplo, consulta de saldo). En la central el nombre del comando figura así, como UUSD.	`UUSD 123456 *245#`
CONNECT	Protegus=ON	Conexión a la nube Protegus.	`CONNECT 123456 PROTEGUS=ON`
	Protegus=OFF	Desconexión de Protegus.	`CONNECT 123456 PROTEGUS=OFF`
	Code=123456	Código de acceso a la nube Protegus (**Cloud access code**).	`CONNECT 123456 CODE=123456`
	IP=dirección:puerto	Dirección IP y puerto del canal principal de la CRA.	`CONNECT 123456 IP=0.0.0.0:8000`
	IP=0	Desactivación del canal principal.	`CONNECT 123456 IP=0`
	ENC=123456	Clave de cifrado TRK.	`CONNECT 123456 ENC=123456`

Comando	Datos	Qué hace	Ejemplo
	APN=nombre	Nombre APN de la tarjeta SIM.	`CONNECT 123456 APN=INTERNET`
	USER=nombre	Nombre de usuario del APN.	`CONNECT 123456 USER=User`
	PSW=contraseña	Contraseña del APN.	`CONNECT 123456 PSW=Password`

Primera comprobación

El comando `INFO` es la forma más rápida de ver en el lugar de la instalación que la SIM funciona, que la central acepta comandos y cuál es la intensidad de la señal. La respuesta llega en pocos segundos.

5.4 Control por llamada telefónica

No en todas las versiones

El control por llamada no funciona en las centrales **SP3_xx7x**. El tipo **SP3_12xx** con firmware 1.14 o posterior no reproduce mensajes de voz, pero los comandos con teclas siguen funcionando.

Condiciones:

1. El número de teléfono de quien llama figura en la pestaña **Users & Reporting** → **Users**, y en ese usuario está marcada la columna **PGM** (control de salidas desde el teléfono), o el sistema está dividido en al menos una partición y el usuario tiene permiso sobre ella.
2. El campo **Output definition** de la salida que quieres controlar es **Remote control** (6.8). Para el control por impulso, también está rellenado el **Pulse time**.

Llama al número de la tarjeta SIM de la central. La central acepta la llamada; después marca el comando en el teclado del teléfono:

Teclas	Función	Ejemplo
[1][partición][#]	Armado de la partición indicada.	`12#` – armado de la partición 2
[2][partición][#]	Desarmado de la partición indicada.	`22#` – desarmado de la partición 2
[3][salida][#][estado]	Control de la salida indicada. Estado: 0 – desactiva, 1 – activa, 2 – desactiva durante el tiempo de impulso, 3 – activa durante el tiempo de impulso.	`31#1` – activación de la salida 1; `32#3` – activación de la salida 2 durante el tiempo de impulso

Solo en las centrales SP3_12xx antiguas (firmware hasta la 1.13), para los mensajes de voz:

Teclas	Función	Ejemplo
[4][#][número de grabación][#]	Iniciar la grabación de un mensaje de voz (1–5).	`4#1#`
[5]	Escuchar el mensaje que acabas de grabar.	`5`
[6]	Guardar la grabación.	`6`

Grabación de mensajes de voz

El inicio y el final de la grabación se indican con un pitido. Un mensaje dura como máximo 15 segundos. El final de la reproducción también se indica con un pitido, y la operación siguiente inicíala solo después del pitido. La central reproduce el mensaje grabado al usuario llamado en caso de alarma: qué mensaje corresponde a cada zona lo indica el campo **Sound** de la zona (6.7). Las llamadas de voz solo están en la versión SP3_12xx, con firmware hasta la 1.13.

6. TrikdisConfig: la configuración en detalle

TrikdisConfig es el programa de configuración gratuito de Trikdis que funciona en Windows. Con él lees y escribes toda la configuración de la central: en el lugar, por USB, o a distancia a través de la nube Protegus. El programa se descarga de trikdis.com (escribe TrikdisConfig en el campo de búsqueda).

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!

Conexión por USB

1. Instala e inicia TrikdisConfig.
2. Conecta la central al ordenador con un cable USB Mini-B. El programa reconoce la central y abre la ventana de configuración de la SP3.
3. Pulsa el botón **Read [F4]**. Si el programa pide un código, introduce el código de administrador o el de instalador (6.2.6). Con el código de administrador de fábrica no lo pide.
4. Ajusta lo que haga falta y pulsa el botón **Write [F5]**. Solo así la configuración se graba en la central.

Modo de programación

Si conectas el cable USB a una central alimentada y en funcionamiento, la central pasa al modo de programación y, hasta que desconectes el cable, no cumple su función de alarma. En un sistema en servicio, avisa al usuario y, al terminar, desconecta el cable.

Los botones de la fila superior: **Read [F4]**: leer de la central; **Write [F5]**: grabar en la central; **Open [F8]**: abrir una configuración guardada antes en un archivo; **Save [F9]**: guardar la configuración actual en un archivo; **Disconnect**: cerrar la conexión. Las ventanas del menú de la izquierda: **System Options**, **Reporting to CMS**, **Users & Reporting**, **Modules**, **Wireless sensors**, **Zones**, **PGM**, **Sensors**, **System events**, **Events Log** y **Firmware** (actualización del firmware, capítulo 9). En la esquina inferior izquierda se ven las casillas **Remember password** y **Show passwords**, el botón **Default settings** → **Restore** (6.12) y el número **IMEI/Unique ID** de la central.

Guárdala en un archivo

El archivo guardado con el botón **Save [F9]** es la documentación del sistema. Después de un cambio de placa o de un restablecimiento de fábrica, con el botón **Open [F8]** y luego **Write [F5]** vuelves a cargarlo todo en unos minutos.

También puedes configurar la central a distancia: en la pantalla de inicio de TrikdisConfig, escribe el número **IMEI/Unique ID** de la central en el campo **Remote access** y pulsa el botón **Configure** (figura en el apartado 6.6.2, el proceso completo en el capítulo 7). Para ello, el servicio en la nube debe estar activado (6.4.3) y la conexión de red debe funcionar.

6.1 La barra de estado

Con la central conectada, la fila inferior del programa y el campo inferior izquierdo muestran los datos del equipo.

Campo	Significado
IMEI/Unique ID	El identificador único de la central. En la versión con módem es el IMEI; en la versión WiFi/Ethernet, un identificador de hardware. Lo piden Protegus 2 y también **Remote access**.
Status	El estado de la operación (por ejemplo, "reading done").
Device	El tipo de central, con la forma SP3_xxxx.
SN	El número de serie de la central.
BL	La versión del cargador de arranque (bootloader).
FW	La versión del firmware.
HW	La versión del hardware.
State	El modo de conexión: **USB** o remoto.
Role	El nivel de acceso después de introducir el código: **Administrator** o **Installer**.



Figura 50. La barra de estado de TrikdisConfig. Los valores de **IMEI/Unique ID** y **SN** se han ocultado en la figura.

El botón **Read [F4]** lee y muestra la configuración guardada en la central. A continuación repasamos los campos ventana por ventana.

6.2 System Options

Tiene seis pestañas: **System general**, **Partitions**, **Scheduler**, **Holidays**, **System troubles** y **Access**.

6.2.1 Pestaña System general

Grupo **General**:

- **Object ID**: identificador del objeto, un número hexadecimal de cuatro cifras (0–9, A–F). Lo da la CRA (CMS); solo hace falta si la central transmite a una CRA. No se pueden usar FFFE ni FFFF.
- **Object name**: el nombre del objeto, como máximo 20 letras y números. Aparece en los informes por SMS.
- **Test period**: si lo marcas, la central envía un informe de prueba con este intervalo, salvo que también esté marcado **Start test at** y hayas indicado una hora.
- **Start test at**: la hora diaria del informe de prueba.
- **Areas in test SMS**: el SMS de prueba incluye también el estado de las particiones indicadas.
- **Clear Events after reset**: al reiniciar, los eventos todavía no enviados se borran del búfer.
- **Text language**: los SMS usan los caracteres propios del idioma elegido.

- **Suspend event reporting when … same events per … s**: suspensión de la transmisión si el mismo evento se repite más veces de las indicadas en el tiempo indicado (por ejemplo, un detector averiado). **Restore event reporting after**: pasados estos minutos (0–999), la central vuelve a transmitir el evento.
- **Call**: cuando hay un evento, la central llama al usuario este número de veces. Si la llamada se acepta o se rechaza, deja de llamar. Una llamada dura 20 segundos.
- **EOL Type**: el valor de las resistencias de fin de línea de las zonas: RT es la resistencia de sabotaje, R1 la del detector 1 y R2 la del detector 2. La conexión se muestra en el capítulo 3.
- **Communication path test**: con este intervalo, la central también envía un mensaje de prueba a la CRA por los canales de respaldo y después vuelve al canal principal.
- **LED out as 2Wire fire**: márcalo si conectas detectores de incendio de dos hilos a la salida LED.

Grupo **SIM**:

- **PIN**: el código PIN de la tarjeta SIM. Si la tarjeta no pide PIN, deja el valor de fábrica.
- **APN**: el nombre del punto de acceso a internet del operador móvil. Es obligatorio si la central transmite a la nube Protegus o a la CRA por internet móvil.
- **Login**, **Password**: usuario y contraseña del APN, solo si el operador los pide.
- **Locked ICCID**: el número ICCID de la tarjeta SIM. Si lo rellenas, la central solo funciona con esta tarjeta.
- **Preferred operator**: el código del operador (MCC + MNC). Si lo rellenas, la central solo se registra en la red de este operador.

Códigos de operador – ejemplo: España

Vodafone 21401, Orange 21403, Yoigo 21404, Movistar 21407. El código de tu operador se forma del mismo modo, con el MCC del país y el MNC del operador. Si lo dejas vacío, la central elige la red automáticamente; escribe el código solo si tiene que quedarse en una red concreta.

Grupo **Time settings**:

- **Set PC time**: graba en la central la hora del ordenador. Si en el campo **Time synchronization** está **Disabled**, se queda esta hora; si está **modem** o **server**, la central se sincroniza desde allí después de encenderse.
- **Time zone (Hours)**: la zona horaria; por ejemplo, +1 en la España peninsular y en Baleares, 0 en Canarias.
- **Time set**: el servidor de hora con el que la central se sincroniza al encenderse.
- **Daylight saving time**: cambio automático entre el horario de verano y el de invierno.
- **AC failure delay**: la central avisa del corte de la alimentación de red con este retardo, y también de su restablecimiento.

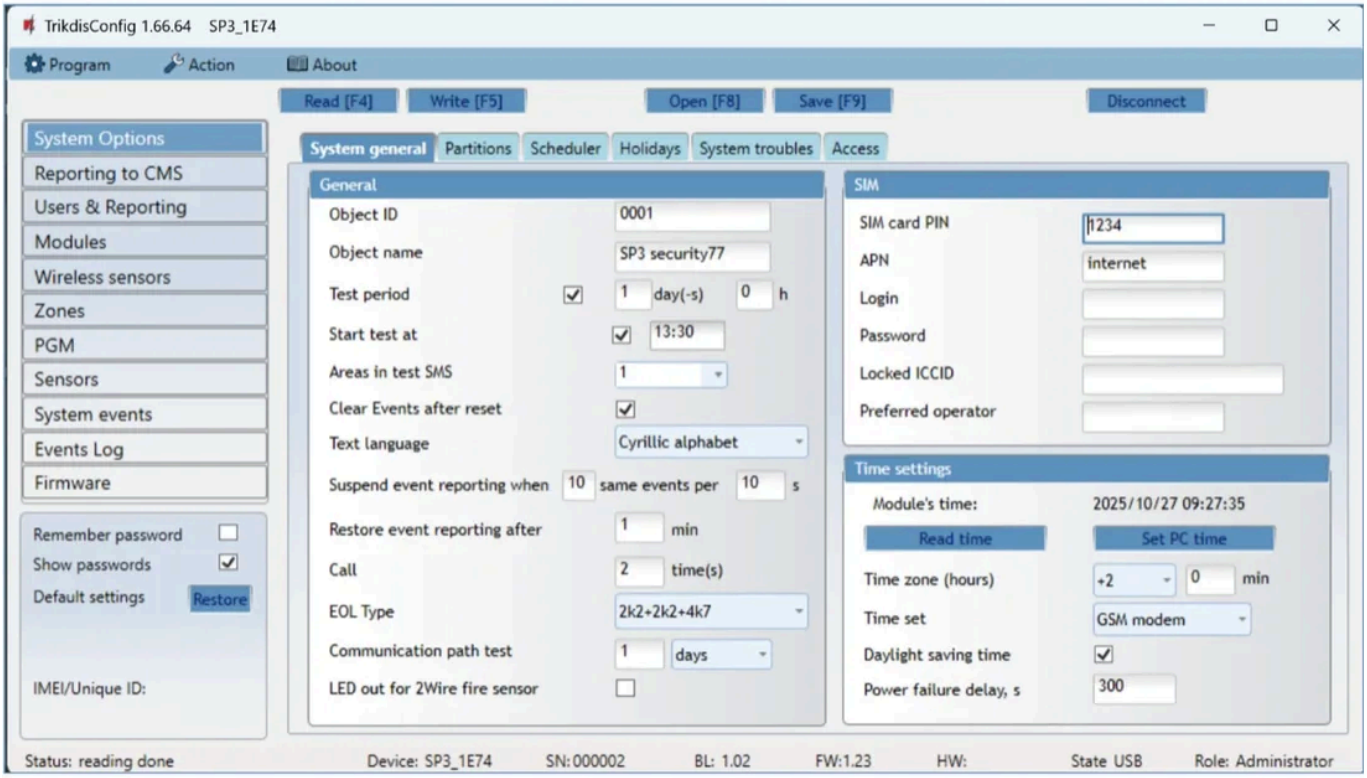


Figura 51. System Options → System general: los grupos General, SIM y Time settings.

6.2.2 Pestaña Partitions

- **Partitions enabled**: en cuántas partes independientes (particiones) divides el sistema.
- **Partition name**: el nombre de la partición.
- **Entry**: retardo de entrada, 0–999 s. Es el tiempo que tienes para ir por la zona Delay hasta el teclado y desarmar el sistema.
- **Exit**: retardo de salida, 0–999 s. Después del armado, contando desde el código de armado introducido en el teclado, es el tiempo que tienes para salir del local por la zona Delay. Con el armado remoto (por ejemplo, desde Protegus 2) el sistema se arma al instante, sin tiempo de salida.
- **Bell**: el tiempo de funcionamiento de la sirena en caso de alarma, 0–999 s.
- **Squawk**: la sirena emite un pitido al armar y dos al desarmar.
- **Re-ARM**: rearmado automático si el sistema se desarmó a distancia, pero nadie violó la zona Delay durante el tiempo de entrada.
- **Force-ARM**: armado forzado. El sistema se puede armar aunque haya zonas Stay abiertas, siempre que la zona de entrada esté cerrada.
- **Keyswitch**: la zona de interruptor de llave arma y desarma por impulso (**Pulse**) o por nivel (**Level**).
- **Tamper**: el tratamiento del evento de sabotaje cuando la central detecta el sabotaje de un detector: **Silent** (solo se envía el aviso a los destinatarios, la sirena no suena), **Audible when armed** (se envía el aviso y la sirena solo suena si el sabotaje se produce con el sistema armado), **Always Audible** (se envía el aviso y la sirena también suena con el sistema desarmado).

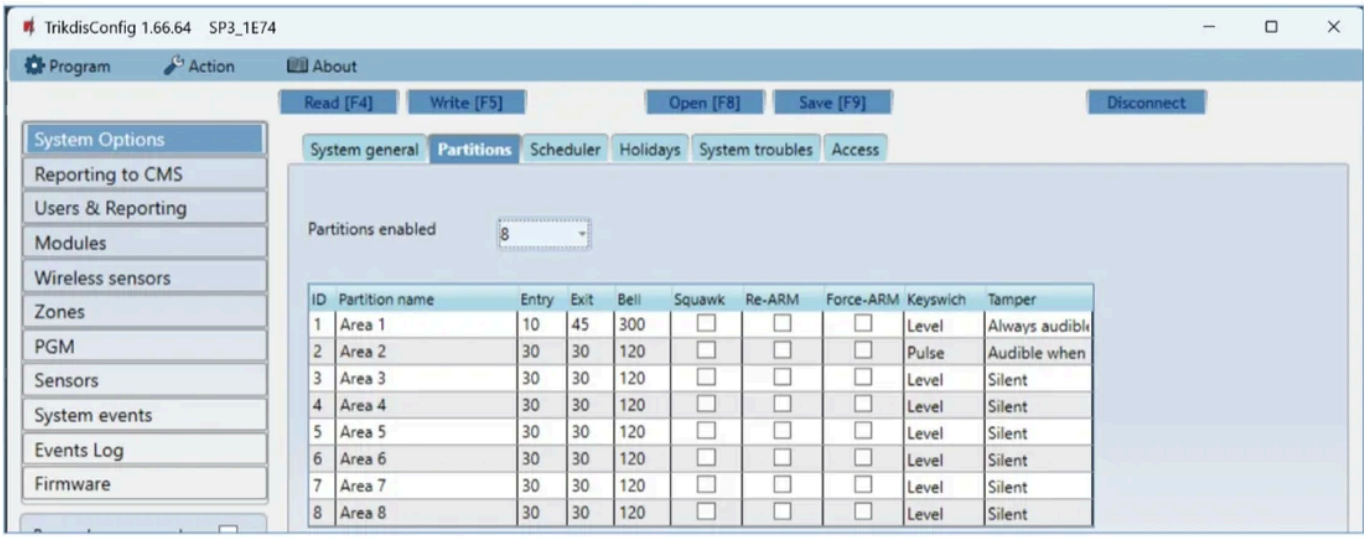


Figura 52. System Options → Partitions: por partición, los tiempos de entrada, de salida y de sirena, y el comportamiento.

6.2.3 Pestaña Scheduler

Armado y desarmado automáticos según los días de la semana, con días festivos.

- **Enable**: activa la programación.
- **Partition**: a qué partición se aplica.
- **Time**: la hora de la operación.
- **Not Armed**: la operación solo se ejecuta si la central no está armada en modo total (Away).
- **Action**: el modo que se ajusta: **Disarm**, **Arm**, **Sleep** o **Stay**.
- **Monday … Sunday**: qué días es válida.
- **Holiday**: el comportamiento en un día festivo: **Disabled** (sin festivos), **Ignore on holidays** (no se ejecuta en festivos), **Additional when holidays** (también se ejecuta en festivos), **Only holidays** (solo se ejecuta en festivos).
- **Holiday group**: qué grupo de festivos (**Any**, 1–4) se considera festivo. Con **Any** cuenta cualquier festivo activo.

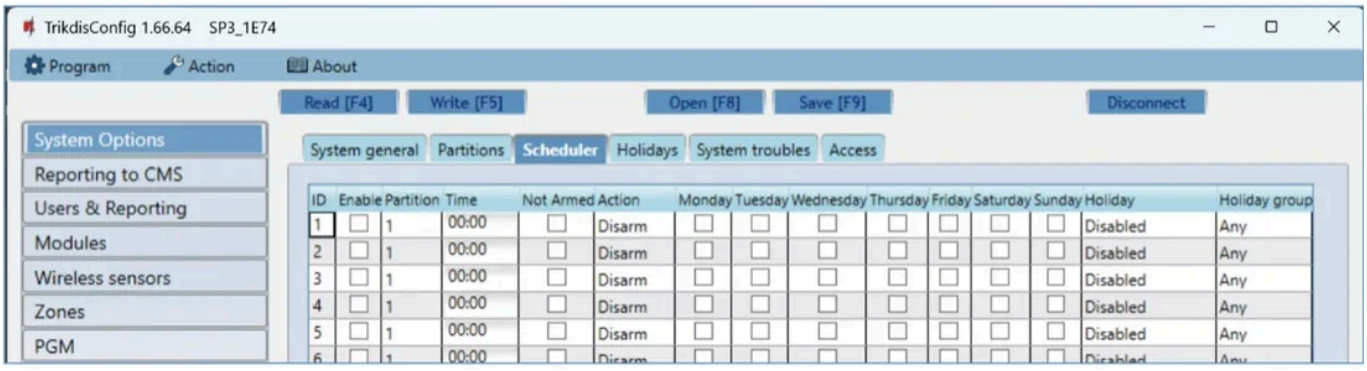


Figura 53. System Options → Scheduler: el horario semanal de armado y desarmado.

6.2.4 Pestaña Holidays

- **Enable**: activa el festivo.
- **Start date**, **Stop date**: el primer y el último día del festivo. En un festivo de un solo día, las dos fechas son iguales.
- **Group 1 … Group 4**: ordenas los festivos en grupos, y la programación (Scheduler) hace referencia a ellos.

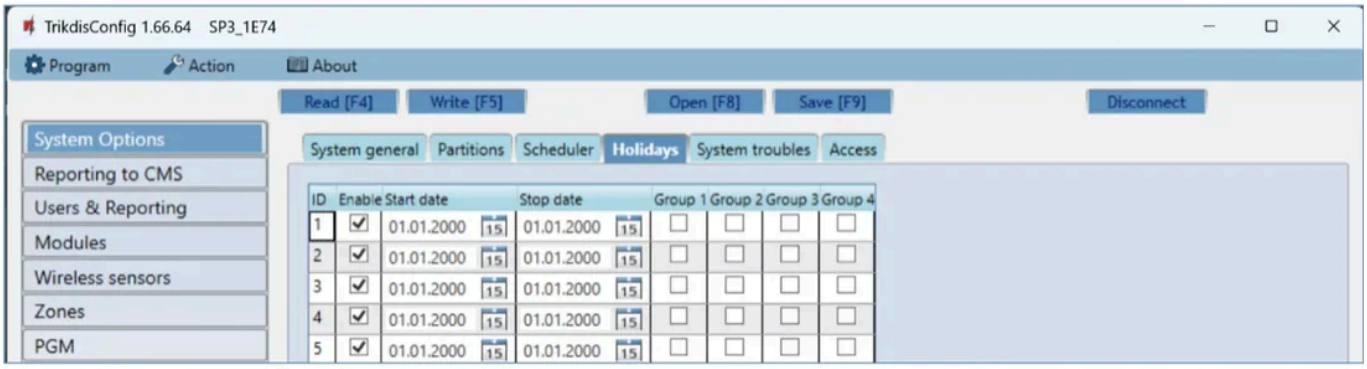


Figura 54. System Options → Holidays: días festivos en cuatro grupos.

6.2.5 Pestaña System troubles

Si aquí marcas un fallo interno, el sistema no se puede armar mientras ese fallo persista. Así puedes impedir, por ejemplo, que se arme con la batería descargada o sin alimentación de red.

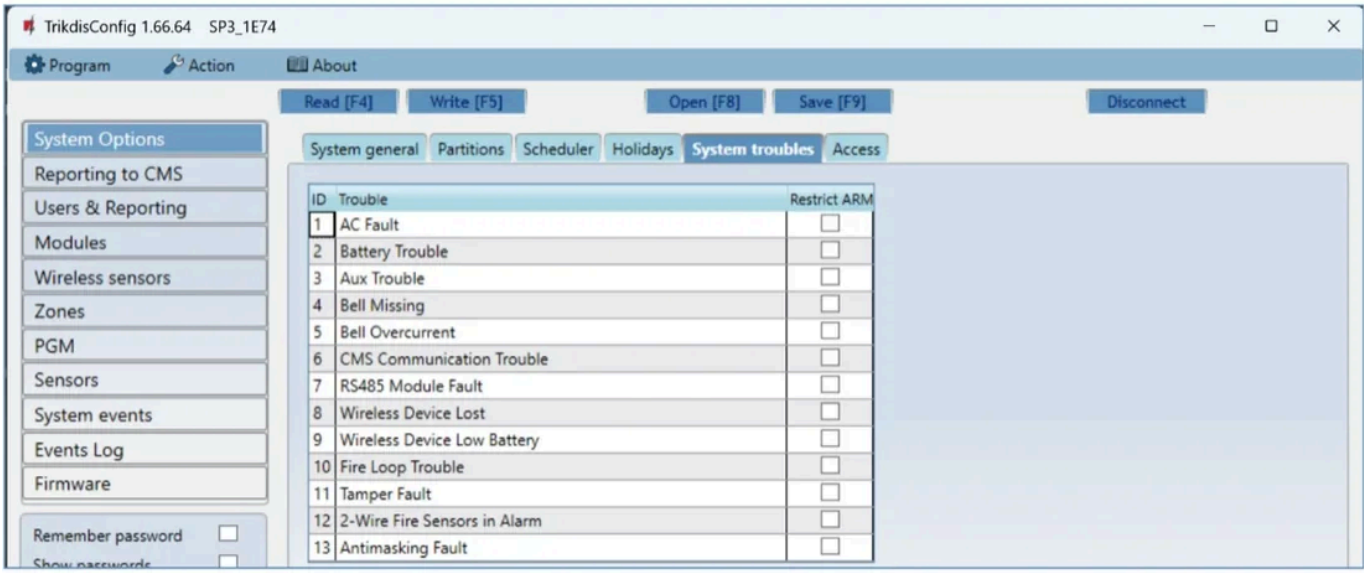


Figura 55. System Options → System troubles: qué fallos impiden el armado.

6.2.6 Pestaña Access

Grupo **Access codes**:

- **Administrator Code**: valor de fábrica 123456. Acceso completo a la configuración. Seis caracteres, letras latinas y/o números.
- **SMS password**: valor de fábrica 123456. La contraseña de los comandos SMS (5.3); con ella se controla el sistema por SMS de forma segura; por seguridad, cámbiala por una contraseña de seis dígitos que solo conozcas tú.
- **Installer Code**: valor de fábrica 654321. El acceso del instalador a la configuración; por seguridad, cámbialo por un código de seis dígitos que solo conozcas tú.

Grupo **Installer permissions**: aquí indicas qué puede ajustar quien entra con el código de instalador.

Código de administrador de fábrica

Mientras el código de administrador sea el 123456 de fábrica, después de **Read [F4]** el programa muestra la configuración sin pedir código.

Antes de la entrega

Antes de entregar el sistema, cambia los tres códigos. El código de administrador es del propietario; el propietario también puede cambiar más adelante el código de instalador y sus permisos.

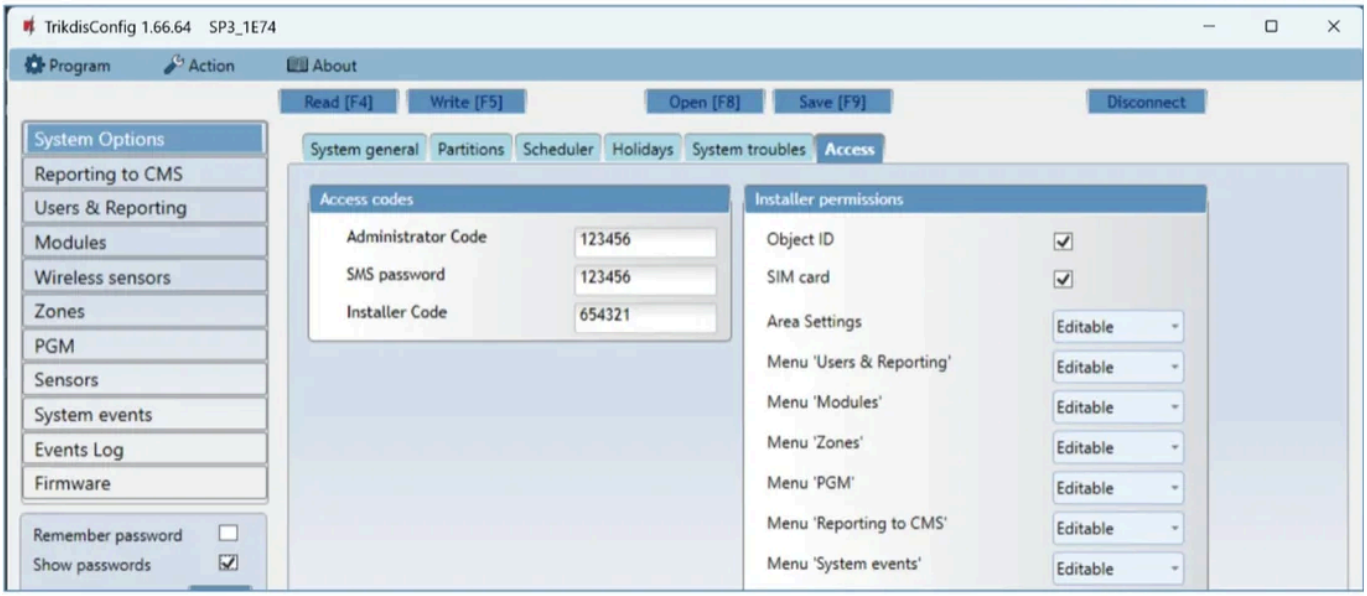


Figura 56. System Options → Access: los tres códigos y los permisos del instalador.

6.3 Reporting to CMS

La central envía los eventos a la CRA (CMS) por internet móvil (IP) o por SMS. Puedes indicar varios canales: el canal principal (**Primary**) y el paralelo (**Parallel**) funcionan a la vez, así que dos receptores pueden recibir los eventos; a cada uno se le puede asignar un canal de respaldo (**Backup**), que entra en funcionamiento si se corta la conexión del canal principal o del paralelo. La conexión está cifrada y protegida con contraseña; para la recepción hace falta un receptor Trikdis: por IP, el receptor de software IPcom o los receptores de hardware RL14 o RM14; para SMS, el RL14, el RM14 o el GM14. El SMS sirve como canal de respaldo porque funciona también sin internet móvil, pero no se recomienda como canal principal.

6.3.1 Pestaña Reporting

Grupos **Primary channel**, **Backup channel**, **Parallel channel** y **Parallel backup channel**:

- **Communication type**: el protocolo usado con el receptor: **TCP/IP**, **UDP/IP**, **SMS** o **Disabled**.
- **Domain or IP**: el nombre de dominio o la dirección IP del receptor.
- **Port**: el puerto del receptor.
- **Protocol**: **TRK** para un receptor Trikdis, **SIA DC-09** para un receptor IP que acepta el formato SIA DC-09.
- **Phone number**: solo con SMS: el número de teléfono del receptor SMS de Trikdis, con el prefijo internacional del país (por ejemplo, 34… para España).
- **Encryption key**: clave de cifrado de seis dígitos; debe coincidir con la clave del receptor.

Si también rellenas el canal paralelo, los eventos van a la vez por los dos canales, así que dos receptores (por ejemplo, una CRA local y una central) los reciben al mismo tiempo. Los dos canales no pueden apuntar al mismo receptor.

Backup channel 2 y **Parallel backup channel 2**: respaldo por SMS: en el campo **Phone number** va el número del receptor SMS de la CRA (con el prefijo del país). La central envía aquí si no lo consigue ni por el canal principal, ni por el paralelo, ni por el de respaldo; es especialmente útil porque funciona también cuando en la red del operador móvil no hay conexión IP. Solo funciona si el primer canal y su respaldo son IP. Se envía un SMS en el primer encendido y cuando se corta la conexión IP en el primer canal y en su respaldo.

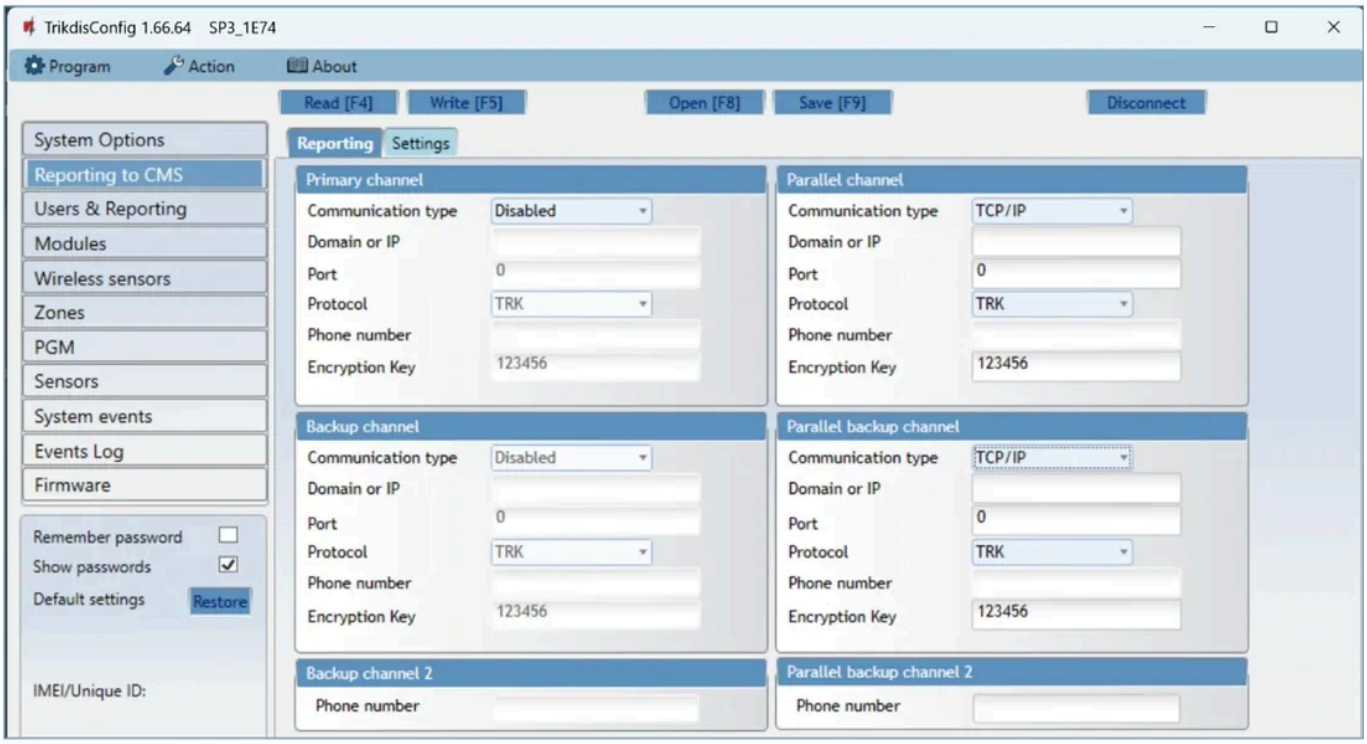


Figura 57. Reporting to CMS → Reporting: canales principal, de respaldo y paralelo.

6.3.2 Pestaña Settings

Grupo **Settings**:

- **Return to primary after**: pasados estos minutos, la central intenta volver al canal principal.
- **IP Ping period**: el intervalo, en segundos, de las señales de control de la conexión IP; la casilla lo activa.
- **SMS Ping period**: el intervalo, en minutos, de las señales de control del canal SMS; la casilla lo activa.
- **Backup reporting after**: después de este número de envíos fallidos, la central pasa al canal de respaldo.
- **DNS1**, **DNS2**: las direcciones de los servidores DNS. Con cualquier configuración IP, indica una dirección DNS que admita el proveedor.
- **Object ID in SIA DC-09**, **SIA DC-09 receiver No.**, **Line No.**: número de objeto, número de receptor y número de línea para el protocolo SIA DC-09.
- **Local time in SIA**: los mensajes enviados a la CRA llevan la hora propia de la central.

Grupo **Reporting mode**: por qué vía se comunica la central con la CRA y con Protegus 2. El orden de los tipos importa: si no se establece la conexión **Main type**, la central pasa a la vía **Backup type** y después a la **Backup type 2**.

- **Main type**, **Backup type**, **Backup type 2**: **SIM**, **WiFi** o **LAN(E485)**, por separado en las columnas CMS y Protegus.

- **Radio T16 (SF485)**: márcalo si también envía un transmisor vía radio T16. El T16 funciona como canal de respaldo si al menos uno de SIM, WiFi o LAN está en uso; si no hay otra conexión, el T16 es el canal principal. El T16 solo envía informes a la CRA.
- **Return to main (both channel)**: pasados estos minutos, la central intenta volver a la vía principal si estaba usando el respaldo.

Grupo **Communicator network settings** (versión WiFi):

- **DHCP mode**: marcado, la central recibe automáticamente la dirección IP, la máscara de subred y la puerta de enlace.
- **Static IP**, **Subnet mask**, **Default gateway**: para la configuración manual.
- **WiFi SSID name**, **WiFi SSID password**: el nombre y la contraseña de la red WiFi.

Grupo **SIM parameters**:

- **Disable indication of the absence of a SIM card**: la central no indica que falta la tarjeta SIM.
- **Use dial and SMS when working over internet module**: marcado, la llamada y el SMS funcionan también cuando la central transmite por WiFi o LAN. Sin marcar, si hay WiFi, la central no usa SMS ni llamadas; si, sin marcar, no hay WiFi, la central se sigue pudiendo controlar por llamada y por SMS, y envía SMS al usuario.
- **Disable the use of SIM card mobile data**: la central no usa los datos móviles de la SIM y solo envía por WiFi. Si el WiFi falla temporalmente, guarda los eventos y los envía más tarde.

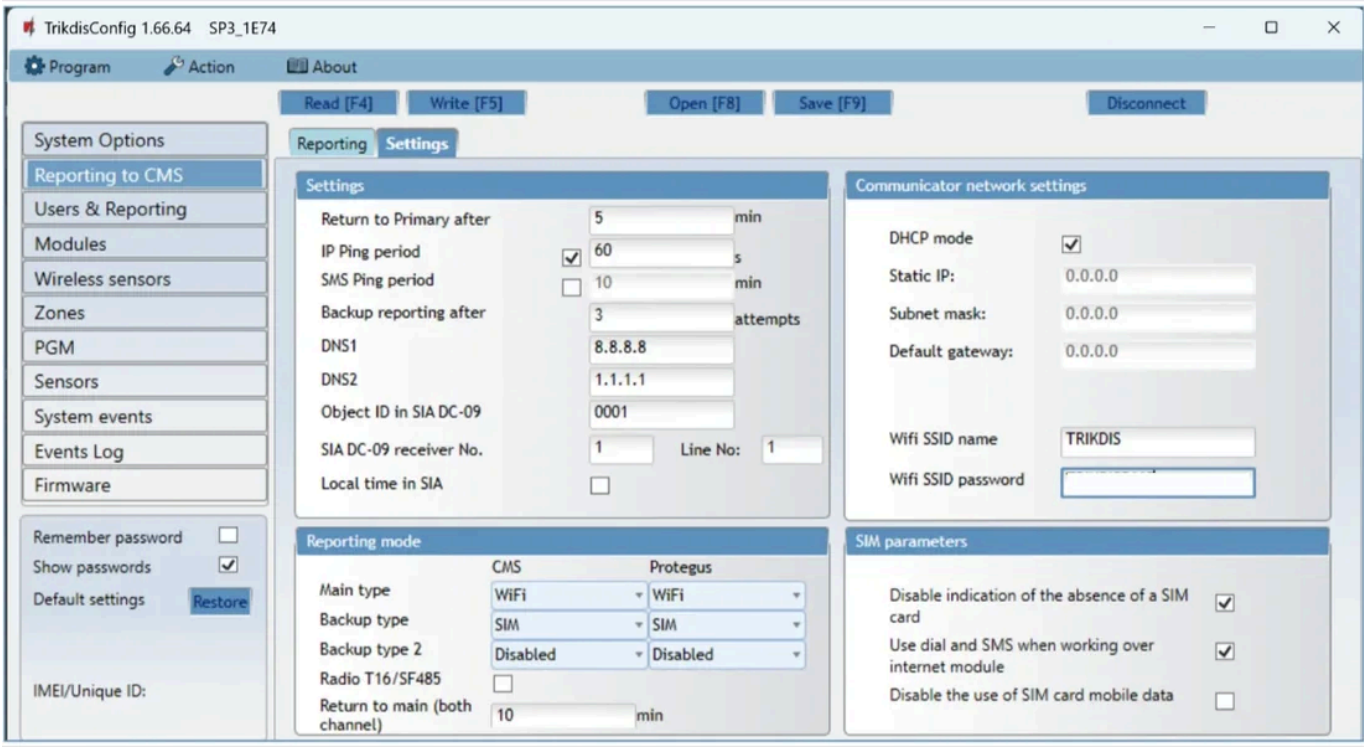


Figura 58. Reporting to CMS → Settings: señales de control, orden de las conexiones, WiFi y parámetros de la SIM.

6.4 Users & Reporting

En las filas de la pestaña **Users** (grupo **Users & Reporting to User**) añades los usuarios:

- **Name**: el nombre del usuario; aparece en los SMS de eventos.
- **Tel number**: número de teléfono con el prefijo internacional del país. Desde él puede controlar el sistema, y a él recibe los SMS. Los ocho primeros números reciben los avisos por SMS y por llamada.

- **Email**: dirección de correo electrónico; el usuario recibe una invitación a Protegus 2.
- **Code**: el código de armado y desarmado del usuario.
- **Tag code**: el número de identificación de una tarjeta o llavero RFID o de una llave iButton.
- **Areas**: qué particiones puede manejar.
- **A**, **D**: puede armar y desarmar, respectivamente.
- **PGM**: puede conmutar las salidas por llamada telefónica, con tonos DTMF (5.4).
- **ACK**: la central confirma por SMS la ejecución de los comandos recibidos.
- **FWD**: los SMS que no llegan de usuarios (información del saldo, publicidad) la central los reenvía a este usuario.

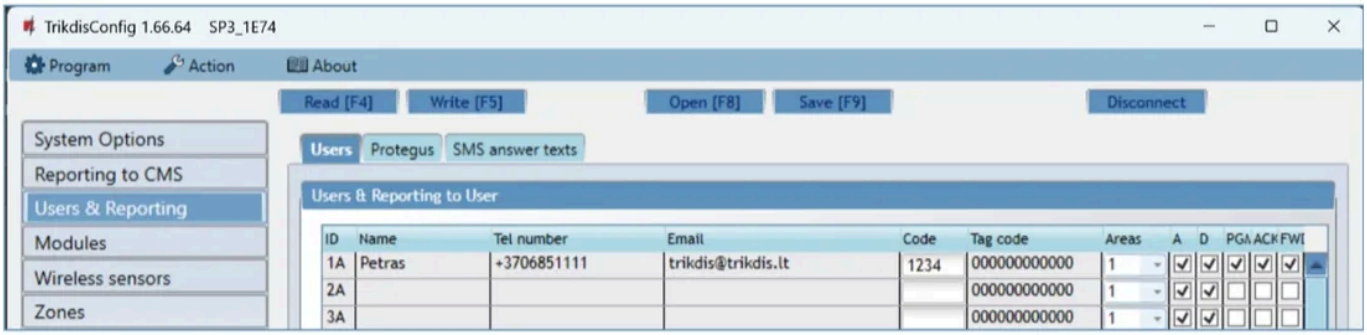


Figura 59. Users & Reporting → Users: usuarios, códigos, identificadores y permisos.

6.4.1 Tarjetas y llaveros RFID

La tarjeta y el llavero RFID no se dan de alta acercándolos al lector: el número de identificación de la tarjeta lo escribes a mano, como número decimal, en el campo **Tag code** y luego pulsas **Write [F5]**. En la mayoría de las tarjetas el número viene impreso.



Figura 60. Números impresos de una tarjeta RFID: el primer grupo de números, enmarcado, es el **Tag code**.

Un lector Wiegand sin teclado, para abrir una puerta

1. Conecta los hilos de datos del lector a los bornes **GRN** y **YEL** de la placa.
2. En la pestaña **Modules → Keypads**, en el grupo **Keypad parameters**, el **Keypad type** debe ser **Wiegand reader**, aunque no haya teclado.
3. En la ventana **PGM**, el campo **Output definition** de la salida controlada debe ser **Remote control**, y el **Pulse time, s**, por ejemplo, 5.
4. En la pestaña **PGM → Control**, en la fila del lector, marca el campo **En**, escribe en el campo **PGM** el número de la salida, y el **PGM mode** debe ser **Pulse**.

6.4.2 Llaves iButton

Alta con el lector **TM17**:

1. Si la lista **Tag code** está vacía, la primera llave que se da de alta va a la primera fila de la lista y se convierte en llave maestra (Master).
2. Para activar el modo de alta, mantén la llave maestra en el "ojo" del lector durante al menos 10 segundos. En el modo de alta, el LED **State** del TM17 parpadea en verde.
3. Acerca las llaves de usuario al lector una por una. Tres pitidos indican que la llave ha entrado en el sistema.
4. Al final, vuelve a acercar la llave maestra al lector; el LED **State** deja de parpadear.
5. Para borrar todas las llaves (incluida la maestra), mantén la llave maestra en el lector durante al menos 20 segundos.

Con el lector **CZ-Dallas**, igual, pero sin indicación LED: la llave maestra durante 10 segundos, las llaves de usuario una por una y al final otra vez la llave maestra; el borrado, con 20 segundos.

La función de la llave maestra

La llave maestra sirve para dar de alta las demás llaves. Si también la usas para armar y desarmar, el comando se ejecuta con retardo.

6.4.3 Pestaña Protegus

Grupo **Cloud application**:

- **Enable cloud service**: activa la nube Protegus. Con ella la central se comunica con Protegus 2, y a través de ella se puede configurar a distancia con TrikdisConfig.
- **Parallel reporting**: los eventos van a la vez por el canal principal a la CRA y a Protegus 2.
- **Cloud access code**: código de seis dígitos para la conexión con Protegus 2; valor de fábrica 123456.

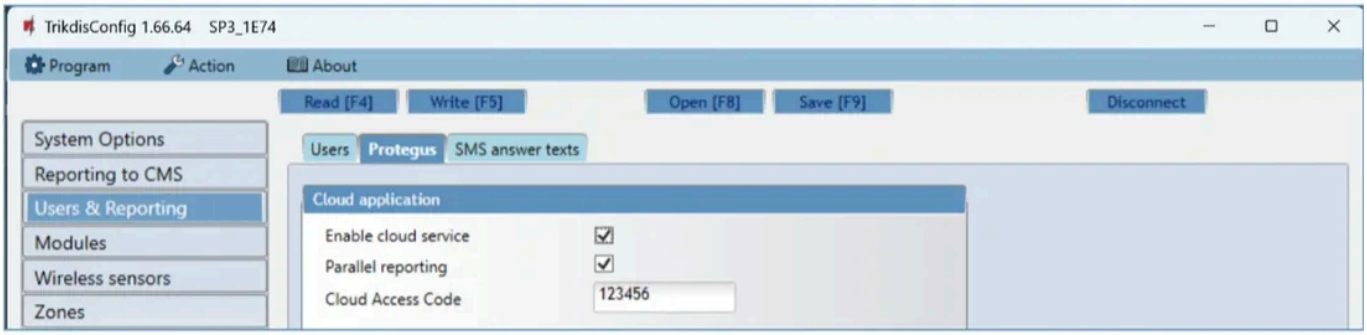


Figura 61. Users & Reporting → Protegus: el interruptor del servicio en la nube y el código de acceso.

6.4.4 Pestaña SMS answer texts

El texto de las respuestas a los comandos SMS lo puedes reescribir en la columna **SMS text**, por ejemplo, en tu idioma.

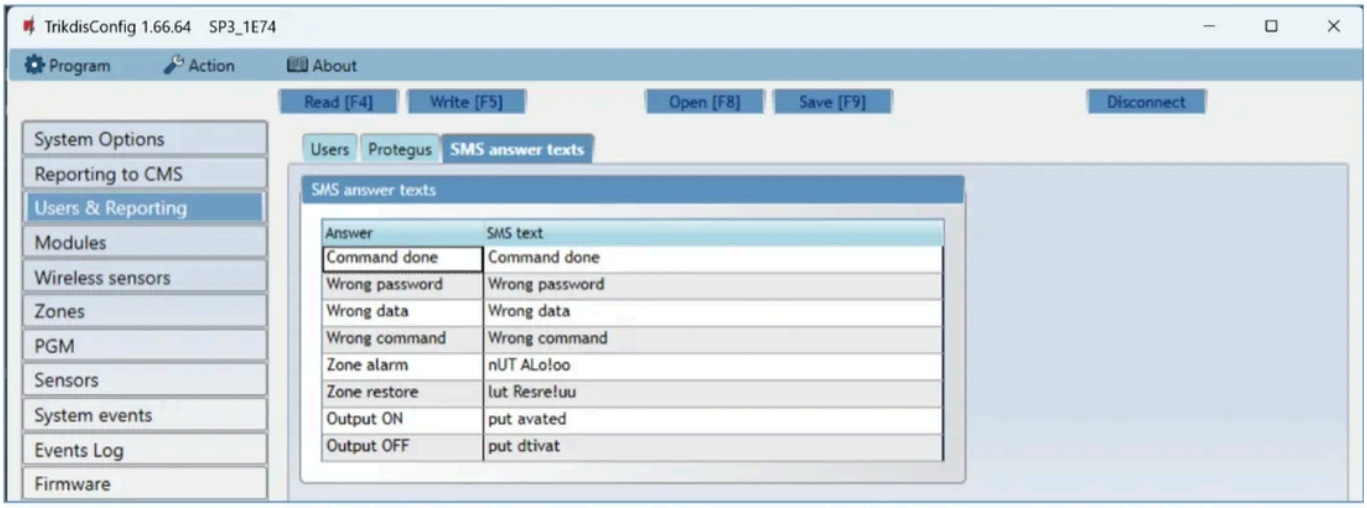


Figura 62. Users & Reporting → SMS answer texts: el texto de los SMS de respuesta.

6.5 Modules

Pestaña **Keypads**:

- **Serial**: el número de serie del teclado; la central lo reconoce automáticamente. Para borrarlo, escribe ceros o pulsa el botón **Remove**.
- **Keypad type**: el tipo de teclado, reconocido automáticamente.
- **Areas**: qué particiones puede manejar el teclado (solo en los teclados FLEXi SK LCD, FLEXi SK LED, SK LCD Button y SK LED Button).
- **Remove**: borra el teclado de la lista.

Grupo **Keypad parameters**:

- **Keypad type**: el tipo de teclado conectado a los bornes **GRN** y **YEL**: **Crow CR16**, **Paradox LED** o **Wiegand reader**.
- **Additional Wiegand on 1IO/2IO**: márcalo si conectas un segundo lector RFID a los bornes **IO1** e **IO2**. En ese caso, estos no se pueden usar como entradas ni como salidas.
- **6 digits user code**: código de usuario de seis dígitos en el teclado. A un código existente de cuatro dígitos, el programa le añade los dos primeros dígitos (1234 pasa a ser 123412); así se transforman todos los códigos de usuario de cuatro dígitos.
- **Duress code type**: el tipo de código de coacción. Bajo coacción armas o desarmas con él: el sistema lo ejecuta y envía una alarma silenciosa a la CRA.
- **Quick ARM**: los botones **ARM**, **STAY** y **SLEEP** del teclado arman sin código.
- **Incorrect codes until lockout**: después de este número de códigos incorrectos, el teclado se bloquea.
- **Lockout timer**: el tiempo de bloqueo, en minutos.
- **Panic alarm type**, **Medical alarm type**, **Fire alarm type**: el efecto de los botones de función de pánico, de emergencia médica y de incendio del teclado cuando se pulsan: **Audible** (suena la sirena, el teclado da una alarma sonora y se envía el aviso a Protegus 2 y a la CRA), **Silent** (solo se envía el aviso a Protegus 2 y a la CRA; la central desactiva la alarma sonora), **Disabled** (no se envía aviso ni a Protegus 2 ni a la CRA).
- **Low voltage reader (1IO/2IO)**: si el lector RFID conectado no funciona, con esto cambias el protocolo entre la central y el lector.
- **Use fingerprint**: para un lector de huellas dactilares con protocolo Wiegand 26/34.

- **Do not change charset**: en el teclado SK-LCD TouchPad se mantiene la codificación de caracteres de los nombres de zonas y particiones.
- **Custom entry beep**: el sonido del retardo de entrada en el teclado es intermitente.

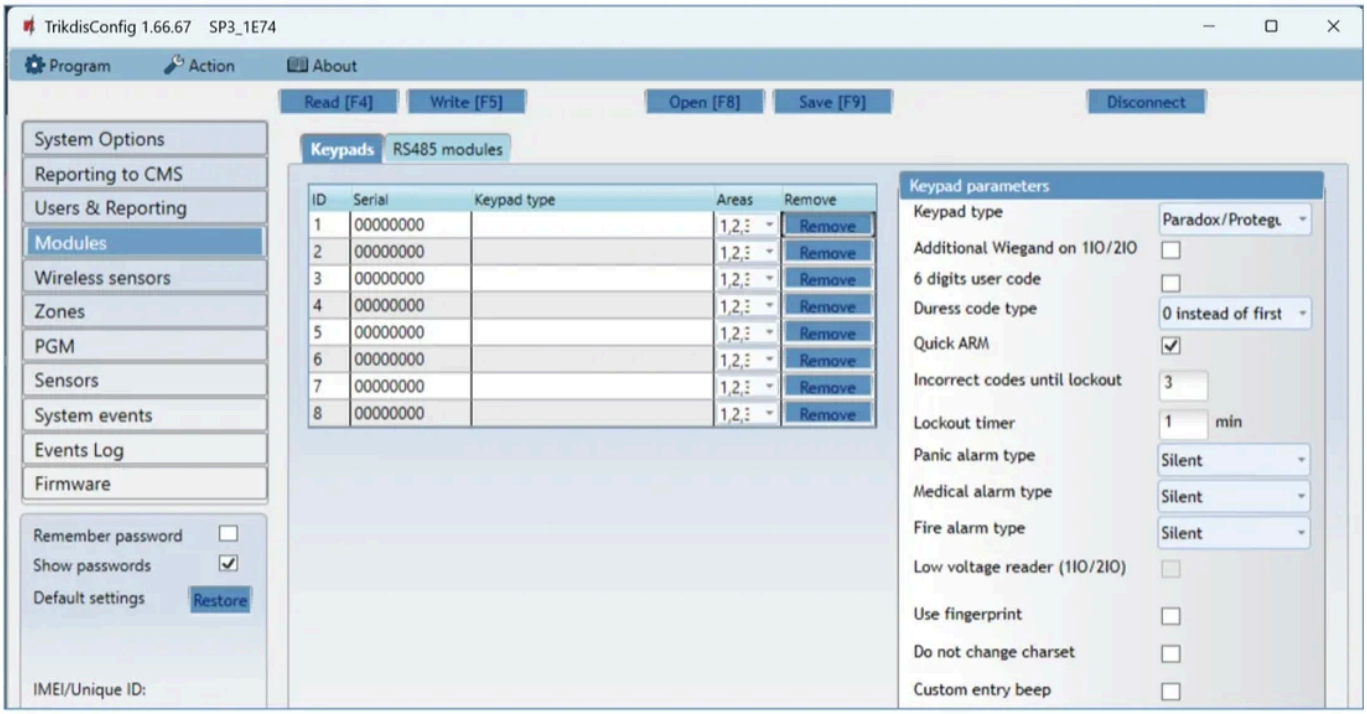


Figura 63. Modules → Keypads: los teclados reconocidos y los parámetros de los teclados.

Pestaña **RS485 modules**:

- **ID**: el número de orden del módulo.
- **Module**: el tipo de expansor, de la lista: 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.**: obligatorio; el número de seis dígitos de la etiqueta de la carcasa y del embalaje del módulo.
- **Area**: la partición del módulo. El TM17 muestra el estado y las zonas de esta partición.
- **Name**: el nombre del módulo.
- **Firmware version**: en cuanto la central encuentra el módulo, aquí aparece su versión de firmware. Es la señal de que el módulo está vivo.

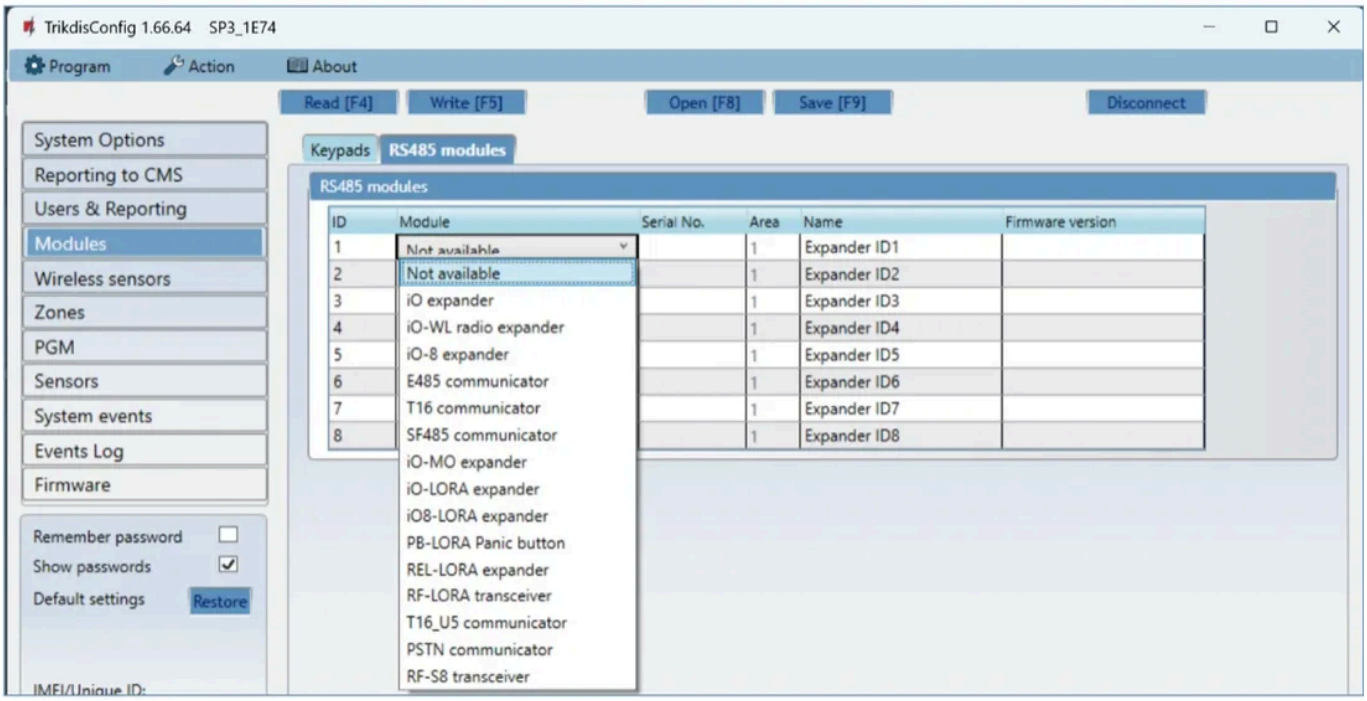


Figura 64. Modules → RS485 modules: la lista de expansores con el desplegable **Module**.

Pestaña **E485 settings**: la configuración de red del comunicador LAN E485: **DHCP mode** (dirección automática: marcado, la central lee automáticamente la configuración de red, máscara de subred y puerta de enlace, y recibe automáticamente la dirección IP) o, para la configuración manual, **Static IP**, **Subnet mask**, **Default gateway**.



Figura 65. Modules → E485 settings: el direccionamiento del módulo LAN E485.

6.6 Wireless sensors

Con el módulo RF-LORA, la "FLEXi" SP3 usa los detectores, sirenas y mandos a distancia inalámbricos del fabricante Maximum. Para ello, la central necesita el firmware con código de receptor 4, como mínimo en la versión 1.21 (SP3_xxx4_0121 o posterior; la 4.ª cifra del nombre del firmware es el tipo de receptor, ver 1.7). El transceptor RF-LORA se conecta al bus RS485 de la central (4.6). Primero registras el módulo RF-LORA en la central (6.6.1) y después das de alta los detectores: a distancia desde TrikdisConfig (6.6.2) o con el botón LEARN del módulo (6.6.3). El emparejamiento de los detectores S8 que funcionan con el receptor RF-S8 se describe en el capítulo 4 del Manual del transceptor RF-S8 y de los detectores S8.



Figura 66. La ventana **Wireless sensors**: la lista de los equipos dados de alta y, encima, los botones **Learn sensors** y **Update**.

6.6.1 Registro del RF-LORA

1. Da alimentación a la central y espera 1 minuto.
2. Inicia TrikdisConfig y conecta la central al ordenador con un cable USB Mini-B.
3. Pulsa el botón **Read [F4]** y abre la pestaña **Modules** → **RS485 modules**. Si en la lista ya figura el **RF-LORA transceiver** con su número de serie y su versión de firmware, has terminado y te saltas los demás pasos.
4. Si no figura, en una fila vacía elige en el campo **Module** el elemento **RF-LORA transceiver**.
5. En el campo **Serial No.**, escribe el número de serie del módulo que figura en la etiqueta de su carcasa o de su embalaje.
6. **Write [F5]** y después desconecta el cable USB.
7. Espera 1 minuto a que la central y el RF-LORA se conecten.
8. Vuelve a conectar el cable USB y pulsa el botón **Read [F4]**. En la ventana **Modules** aparece la versión de firmware del RF-LORA: el módulo está registrado.
9. Desconecta el cable USB, pulsa el botón **Disconnect** y espera 1 minuto.

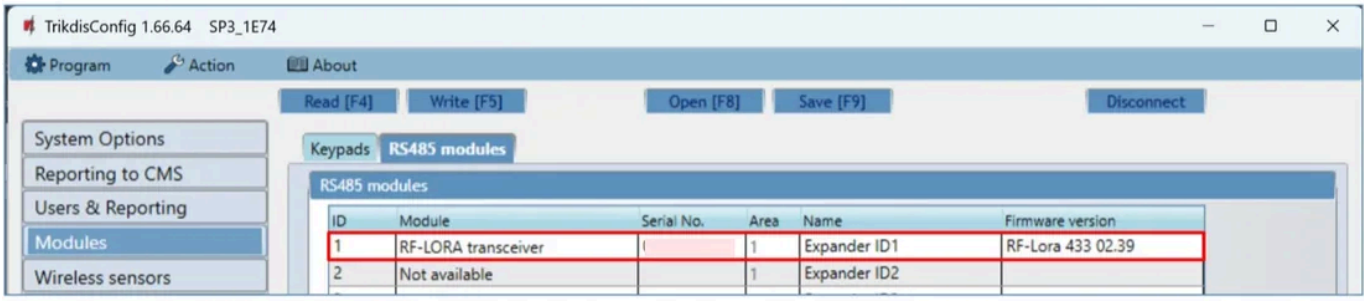


Figura 67. En la pestaña **RS485 modules**, la fila del RF-LORA registrado: tipo, **Area**, nombre y **Firmware version**. El número de serie se ha ocultado en la figura.

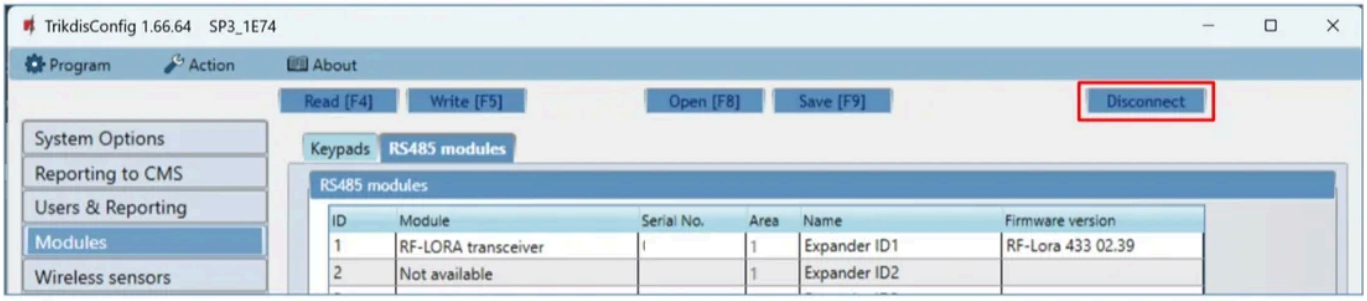


Figura 68. Después de la lectura aparece la versión de firmware del RF-LORA; luego, **Disconnect**.

6.6.2 Emparejamiento de detectores a distancia

Condiciones de la configuración remota: tarjeta SIM activada con el PIN introducido o desactivado y con internet móvil (o conexión WiFi), servicio en la nube activado (6.4.3), alimentación y conexión de red (el LED **NET** verde fijo).

1. En la pantalla de inicio de TrikdisConfig, en el campo **Unique ID** del grupo **Remote access**, escribe el número **IMEI/Unique ID** de la central (en la etiqueta de la placa y del embalaje) y pulsa el botón **Configure**.
2. En la ventana que se abre, **Read [F4]**; si hace falta, introduce el código de administrador o el de instalador.
3. Abre la ventana **Wireless sensors** y pulsa el botón **Learn sensors**. El RF-LORA pasa al modo de aprendizaje, su LED **DATA/TROUBLE** empieza a parpadear en verde y rojo, y TrikdisConfig abre la ventana de aprendizaje.
4. Pon las pilas en los detectores (de movimiento, de apertura, de agua, de humo, sirena). Puedes dar de alta varios detectores a la vez. El RF-LORA debe estar al menos a 1 m de los detectores.
5. Pulsa el botón **TAMPER** (sabotaje) del detector. El LED **DATA/TROUBLE** del RF-LORA parpadea brevemente en verde (el detector ha entrado) y, pasados unos segundos, otra vez en verde y rojo.
6. TrikdisConfig abre una ventana nueva: indica el **Zone number** y la **Zone definition** del detector y pulsa **Save**. El detector entra en la lista.
7. Con el detector siguiente, otra vez el botón **TAMPER**, y así sucesivamente. Al final, pulsa el botón **Stop learning**.
8. A la pregunta, **Yes**: los detectores se graban en la central (**No**, si antes quieres ajustar algo en ellos). Espera unos minutos y luego **Read [F4]**: en la ventana **Wireless sensors** se ven los detectores dados de alta y, en la columna **Serial No.**, su número de serie.
9. Comprueba en la ventana **Zones** que los detectores han quedado en la zona y la partición correctas. Si el campo **Type** de la zona es **EOL_T**, la supervisión de sabotaje del detector también está activa. Después de un cambio, **Write [F5]**.

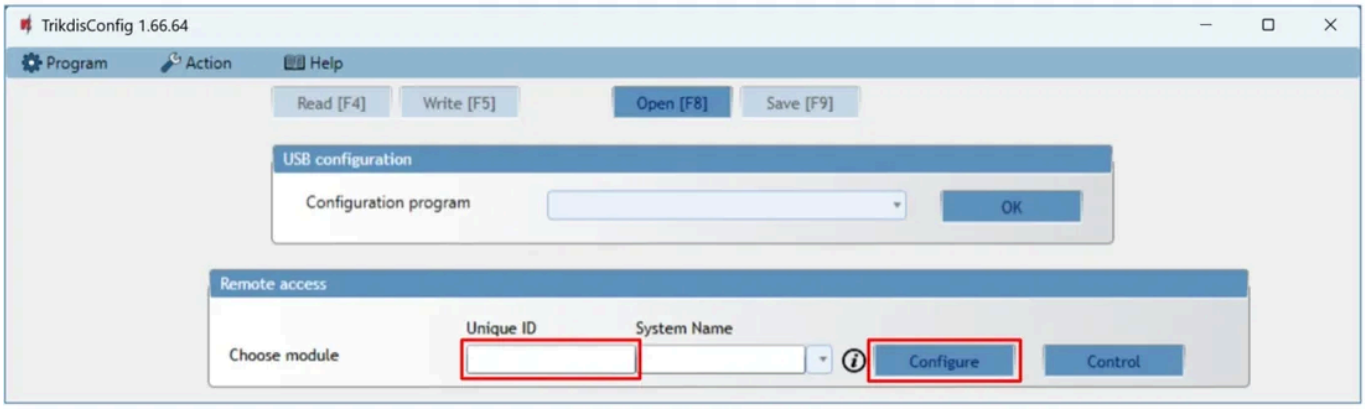


Figura 69. El grupo **Remote access** de la pantalla de inicio: **Unique ID**, **System Name**, **Configure**.

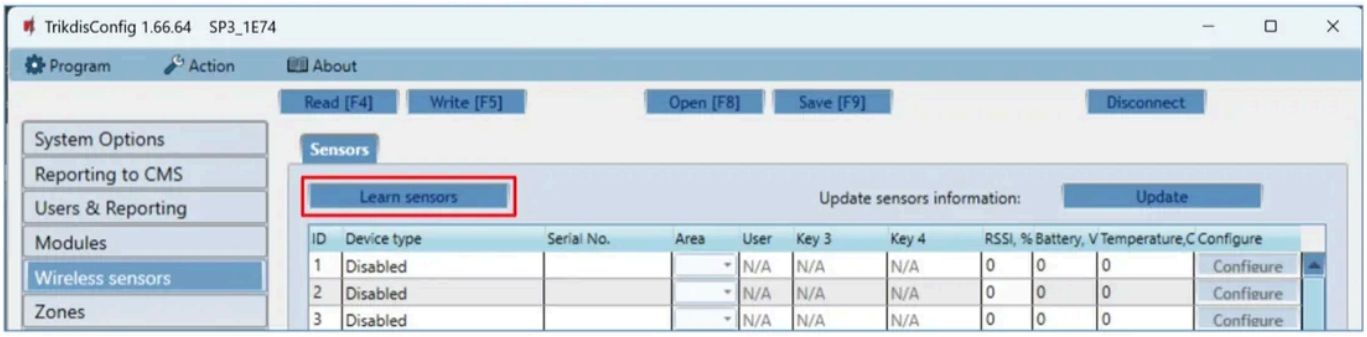


Figura 70. El botón **Learn sensors** de la ventana **Wireless sensors** inicia el modo de aprendizaje.

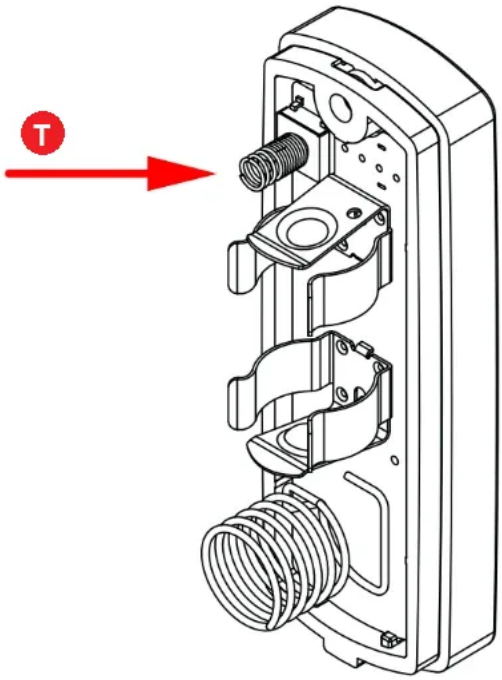


Figura 71. Pulsando el botón **TAMPER**, debajo de la tapa trasera del detector, el detector se da de alta.

- T botón antisabotaje (“Tamper”)

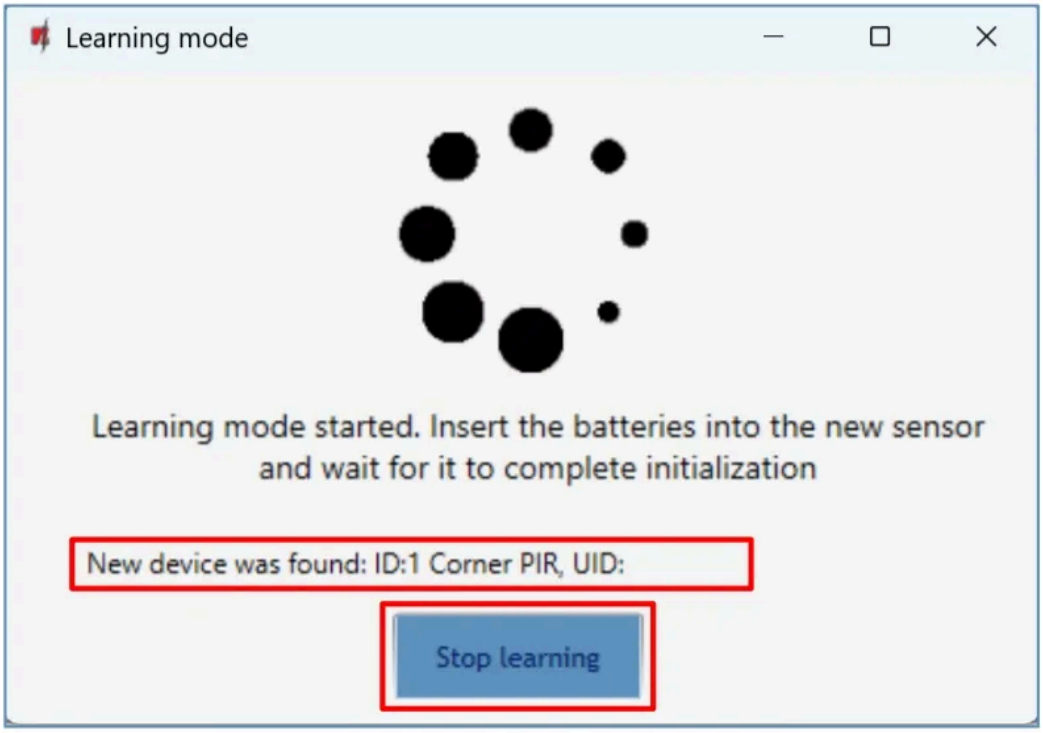


Figura 72. La ventana de aprendizaje: el tipo y el identificador del detector encontrado y, debajo, el botón **Stop learning**. El identificador se ha ocultado en la figura.

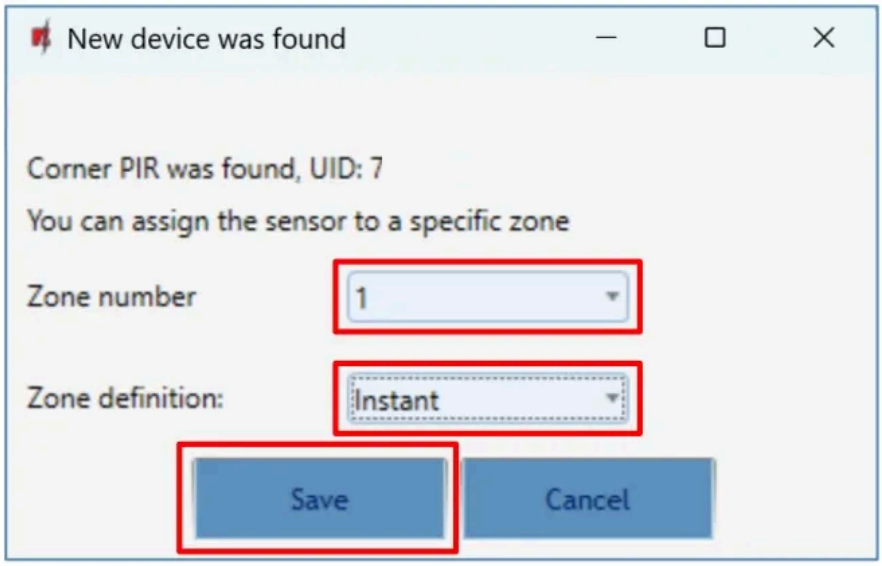


Figura 73. La ventana del equipo nuevo: **Zone number**, **Zone definition**, **Save**.

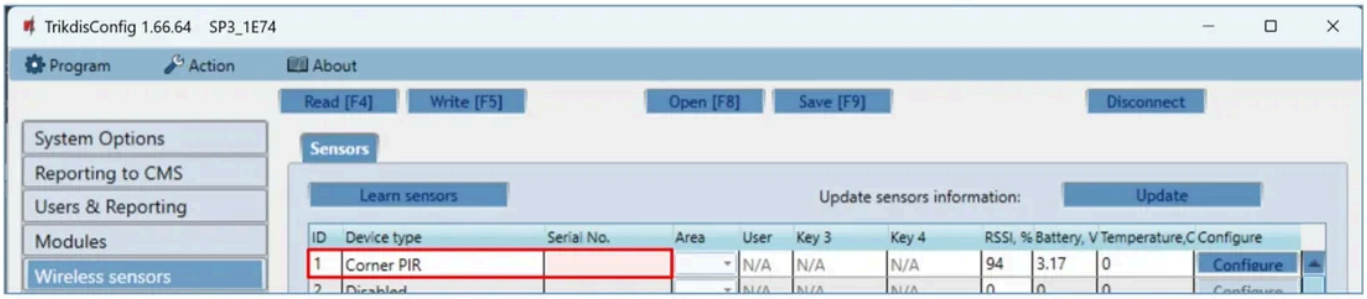


Figura 74. El detector dado de alta en la lista, con la intensidad de la señal (**RSSI**), la tensión de la pila y la temperatura. El número de serie se ha ocultado en la figura.

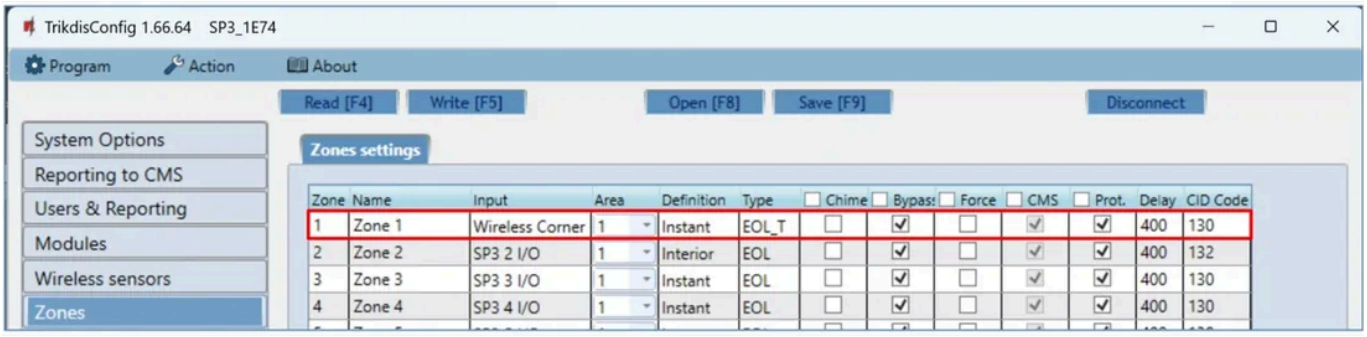


Figura 75. En la ventana **Zones**, la zona del detector inalámbrico con el tipo **EOL_T**: la señal de sabotaje también está supervisada.

Borrar un detector inalámbrico

Conéctate a la central por USB o a distancia, **Read [F4]**, y después, en la columna **Device type** de la ventana **Wireless sensors**, elige **Disabled** en el detector que quieres borrar, y **Write [F5]**.

6.6.3 Emparejamiento con el botón LEARN

1. El RF-LORA debe estar registrado en la central (6.6.1) y la central, encendida.
2. Quita la tapa del RF-LORA. Mantén pulsado el botón **LEARN** hasta que el LED **DATA/TROUBLE** empiece a parpadear en verde y rojo, y suéltalo. El parpadeo indica el modo de aprendizaje.
3. Pon las pilas en los detectores y pulsa el botón **TAMPER** del detector. Un breve parpadeo verde del LED **DATA/TROUBLE** indica que lo ha conseguido; pasados unos segundos vuelve a parpadear en verde y rojo. Con el detector siguiente, otra vez el botón **TAMPER**.
4. Al final, mantén pulsado el botón **LEARN** hasta que se detenga el parpadeo verde y rojo, y suéltalo. El RF-LORA ha salido del modo de aprendizaje.
5. Conecta la central al ordenador por USB, inicia TrikdisConfig, **Read [F4]**. En la ventana **Wireless sensors** se ven los equipos dados de alta con su número de serie de siete dígitos.
6. En la ventana **Zones**, comprueba las zonas y las particiones; después de un cambio, **Write [F5]**.

6.6.4 RF-SH y equipos Crow

Los sistemas más antiguos, con el módulo RF-SH, usan los equipos inalámbricos de las series Crow FW2 y Shepherd (SH). El RF-SH ya no está a la venta; la descripción se mantiene aquí, en resumen, para el mantenimiento de los sistemas existentes; la conexión del módulo se muestra en el apartado 4.2.

- **Registro del RF-SH**: como con el RF-LORA (6.6.1): en la pestaña **Modules → RS485 modules**, **RF-SH**, **Serial No.**, **Write [F5]**, desconectar el USB, esperar 1 minuto, volver a conectar el USB, **Read [F4]**; la aparición de la versión de firmware indica que se ha conseguido.
- **Detectores FW2**: pulsa el botón **LEARN** del módulo hasta que el LED **LEARN** parpadee en verde. Pon la pila del detector y espera a que se apaguen sus LED. Sal con el botón **LEARN**, USB, **Read [F4]**: el número de serie de siete dígitos debe coincidir con el de la carcasa. Indica la zona y la partición, **Write [F5]**. Borrado: **Device type → Disabled**.
- **Mando a distancia FW2**: mantén pulsados a la vez los botones 3 y 4 hasta que el LED destelle en amarillo y después en verde. En la lista, indica su partición y su usuario; la función de los botones 3 y 4 (armado, desarmado, pánico silencioso o sonoro) se elige en la tabla. Restablecer el mando a distancia: botones 2 y 3 a la vez, hasta que veas un parpadeo verde y rojo.
- **Sirena FW2**: da alimentación a la sirena; el flash parpadea lentamente durante 30 segundos. Mientras tanto, mantén pulsado el botón **LEARN** de la placa de la sirena hasta que el flash destelle rápido, y suéltalo. Restablecimiento: con el botón **LEARN** pulsado, da la alimentación, hasta tres destellos.

- **Detectores y teclado SH**: pon la pila; el LED verde encendido durante 3 segundos indica que el alta se ha hecho bien. Si no, quita la pila durante 10 segundos y vuelve a intentarlo.

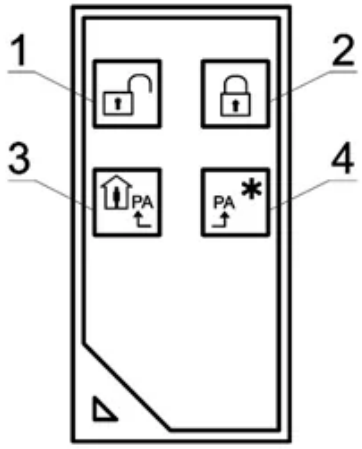


Figura 76. Mando a distancia Crow FW2: para darlo de alta, mantienes pulsados a la vez los botones 3 y 4.

6.7 Zones

Pestaña **Zones settings**:

- **Zone No**: el número de orden de la zona.
- **Name**: el nombre de la zona.
- **Input**: qué entrada **IN** de la central o del expansor corresponde a la zona.
- **Area**: la partición de la zona.
- **Definition**: el funcionamiento de la zona:
    - **Delay**: zona retardada, para el detector magnético de apertura de la puerta de entrada. Para este tipo de zona puedes ajustar un tiempo de entrada y uno de salida. Después del armado, durante el tiempo de salida, la zona Delay se puede violar libremente (se puede abrir la puerta); si al acabar el tiempo de salida sigue violada, se activan las salidas **Siren** y **Flash** y se envía el aviso de alarma. Con el sistema armado, la violación de la zona Delay inicia el tiempo de entrada, durante el que hay que desarmar el sistema; si no lo desarmas antes de que acabe el tiempo de entrada, se activan las salidas **Siren** y **Flash** y se envía el aviso de alarma.
    - **Interior**: zona seguidora, para el detector de movimiento junto a la puerta de entrada. Con el sistema armado, al violarse se activan las salidas **Siren** y **Flash** y se envía el aviso de alarma. Si con el sistema armado se viola primero la zona Delay, la zona Interior se puede violar libremente durante el tiempo de entrada ajustado; si no desarmas el sistema durante el tiempo de entrada, se activan las salidas **Siren** y **Flash** y se envía el aviso de alarma.
    - **Interior Stay**: zona seguidora, para el detector de movimiento junto a la puerta de entrada; funciona igual que la Interior: con el sistema armado, al violarse se activan las salidas **Siren** y **Flash** y se envía el aviso de alarma, pero si antes se violó la zona Delay, se puede violar libremente durante el tiempo de entrada. Con el sistema armado en modo STAY, las zonas Interior Stay no están protegidas (la central no las vigila).
    - **Instant**: zona instantánea, para detectores de movimiento. Si con el sistema armado se viola la zona Instant, se activan al instante, sin tiempo de entrada, las salidas **Siren** y **Flash** y se envía el aviso de alarma.

    - **Instant Stay**: zona instantánea, para detectores de movimiento. Si con el sistema armado se viola la zona Instant Stay, se activan al instante las salidas **Siren** y **Flash** y se envía el aviso de alarma. Con el sistema armado en modo STAY, las zonas Instant Stay no están protegidas.
    - **Fire**: para detectores de incendio. Al violarse, se activan al instante las salidas **Siren** y **Flash** y se envía el aviso.
    - **Keyswitch**: para un interruptor de llave u otro interruptor: la zona arma y desarma. El armado se produce cuando acaba el tiempo de salida.
    - **24_hour**: para detectores de rotura de cristal y antisabotaje. Siempre vigilada; al violarse, da la alarma al instante: se activan las salidas **Siren** y **Flash** y se envía el aviso del evento.
    - **Silent**: con el sistema armado, al violarse se envía el aviso al instante, pero las salidas **Siren** y **Flash** no se activan.
    - **Silent 24h**: para un pulsador de pánico. Sea cual sea el estado del sistema, se envía al instante el aviso del evento, sin sirena: las salidas **Siren** y **Flash** no se activan.
- **Type**: el tipo de lazo conectado a la entrada, de la lista: **NC** (normalmente cerrado), **NO** (normalmente abierto), **EOL** (con resistencia de fin de línea), **EOL_T** (con resistencia de fin de línea y supervisión de sabotaje), **ATZ** (dos zonas en una entrada: dos circuitos de zona normalmente cerrados con resistencias de fin de línea, sin supervisión de sabotaje; para este tipo, elige también la segunda zona ATZ en la lista **Input**), **ATZ_T** (dos zonas con supervisión de sabotaje: dos circuitos de zona normalmente cerrados con resistencias de fin de línea y supervisión de sabotaje; también para este, elige la segunda zona ATZ en la lista **Input**), **3EOL** (con resistencia de fin de línea y supervisión de sabotaje, para detectores de movimiento con función antienmascaramiento, anti-masking). Los valores de las resistencias se indican en el campo **System Options** → **EOL Type** (6.2.1).
- **Chime**: timbre: al abrirse la zona, el teclado emite un pitido.
- **Bypass**: la zona se puede anular.
- **Force**: armado forzado: el sistema se puede armar también con la zona abierta; la zona abierta en el momento del armado queda excluida temporalmente, tras cerrarse (restablecerse) vuelve a estar vigilada, y a partir de entonces su violación provoca una alarma.
- **CMS**: los eventos de la zona van a la CRA.
- **Prot.**: los eventos de la zona van a la nube Protegus.
- **Delay**: el tiempo de reacción de la entrada, en milisegundos.
- **CID code**: el código Contact ID del evento; se rellena automáticamente al elegir la definición.
- **Sound**: el número del mensaje de voz que la central reproduce al usuario llamado en caso de alarma (solo SP3_12xx, firmware hasta la 1.13).

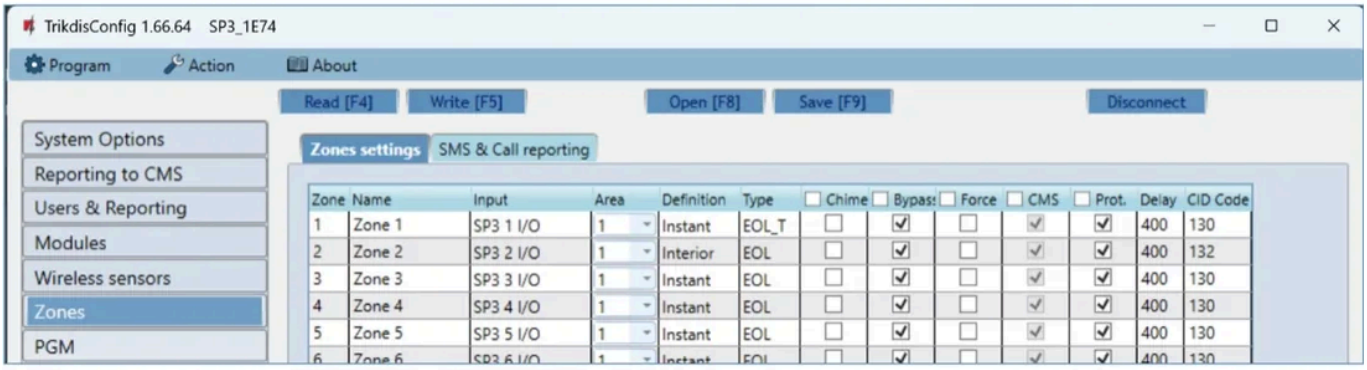


Figura 77. Zones → Zones settings: la definición, el tipo de lazo y las casillas de las zonas.

Pestaña **SMS & Call reporting**: solo se ve si en la ventana **Users & Reporting** hay al menos un número de teléfono.

- **Zn**: el número de la zona y el tipo de evento: **Event** (alarma) o **Restore** (restablecimiento).

- **User / SMS and Call**: por usuario, marcas si recibe un SMS y/o una llamada por el evento de la zona.

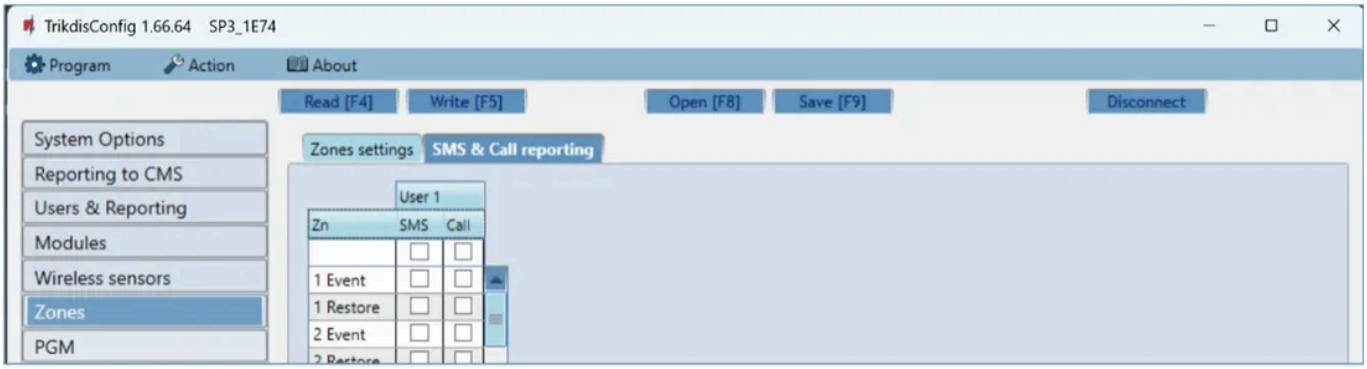


Figura 78. Zones → SMS & Call reporting: quién recibe SMS o llamada por los eventos de cada zona.

6.8 PGM

Pestaña **Outputs**:

- **PGM No**: el número de orden de la salida PGM.
- **Name**: el nombre de la salida.
- **PGM output**: qué salida **OUT** de la central o de un expansor corresponde a la PGM.
- **Area**: la partición de la salida.
- **Output definition**: el funcionamiento de la salida:
  - **Siren**: para una sirena.
  - **Remote control**: para conmutar un equipo externo (desde la aplicación, por SMS, por llamada, con un lector).
  - **Fire Sensor Reset**: para reiniciar los detectores de incendio después de una alarma.
  - **System State**: para un indicador de estado; por ejemplo, un LED muestra si el sistema está armado.
  - **Flash**: para un flash: con el sistema armado, señal continua; en alarma, señal por impulsos; al desarmar, se apaga.
  - **Thermostat**: modo termostato. Hace falta un sensor de temperatura en la central; la temperatura que hay que mantener se indica en la pestaña **Thermostat**.
  - **Buzzer**: repite las señales acústicas del teclado.
- **Pulse time, s**: el tiempo de activación en el funcionamiento por impulso, 0–9999 s.
- **CMS**, **Prot.**: la activación y la desactivación de la salida se notifican a la CRA y a la nube Protegus, respectivamente.

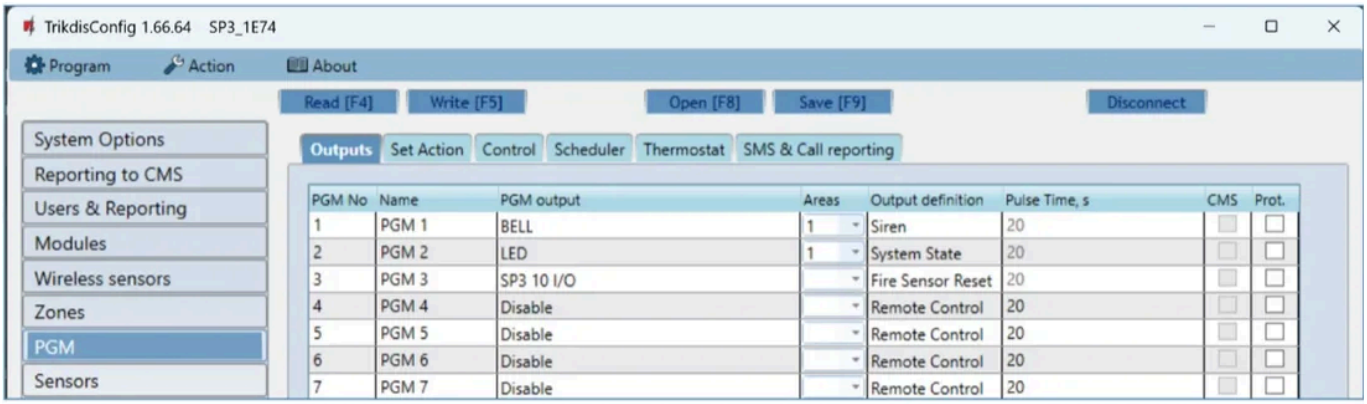


Figura 79. PGM → Outputs: la definición y el tiempo de impulso de las salidas.

Pestaña **Set Action**: qué conmuta la salida:

- **ID**: el número de la fila.
- **Enable**: activa la regla.
- **PGM No.**: la salida controlada, que conmuta el evento descrito en las columnas **Factor**, **Factor No.**, **Start when** y **Set value**.
- **Action**: **PGM OFF** (se apaga), **PGM ON** (se enciende), **Pulse OFF** (normalmente encendida, apagada durante el **Pulse time**), **Pulse ON** (normalmente apagada, encendida durante el **Pulse time**).
- **Pulse time, s**: 0–9999 s.
- **Factor**, **Factor No.**: el evento que la activa y su número: **Zone**, **Sensor**, **Jamming**, **Sensor lost**, **iButton**, **Arm**, **Disarm**, **SMS received**, **Zone(follow)**, **Stay**, **Sleep**, **AC lost**, **Low battery**, **Zone tamper**. También se puede asignar una programación horaria a la salida (la programación indica cuándo debe estar encendida la salida); en la pestaña **Scheduler** se pueden crear como máximo diez distintas.
- **Start when**: una condición adicional para el evento que la activa.
- **Set value**: el valor que depende de la condición: el texto de un SMS recibido, una tensión o una temperatura. Si la central reconoce este valor, ejecuta la operación elegida en la columna **Action**. Con SMS, la palabra clave que conmuta la salida la separas del resto del mensaje recibido con signos `%`: `%texto%`: el mensaje contiene el texto (por ejemplo, `%hoUSe%`: el mensaje contiene "hoUSe", como en el mensaje `VacationhoUSe25864`); `texto%`: el mensaje empieza por él (por ejemplo, `hoUSe%`: el mensaje empieza por "hoUSe", como `hoUSeddss`); `%texto`: el mensaje termina en él (por ejemplo, `%hoUSe`: el mensaje termina en "hoUSe", como `1144hoUSe`). El texto distingue entre mayúsculas y minúsculas.

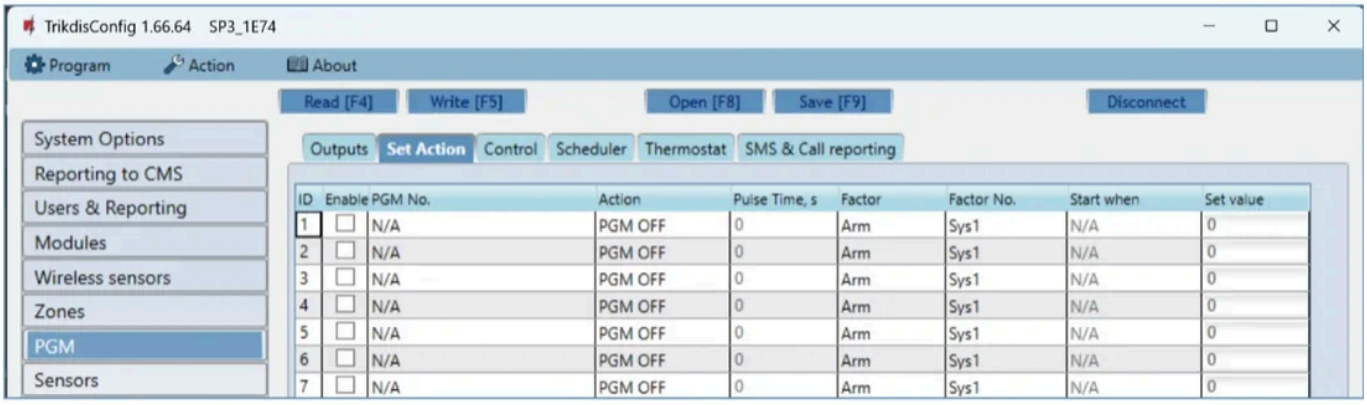


Figura 80. PGM → Set Action: salidas que conmutan por un evento, un SMS o un valor.

Pestaña **Control**:

- Grupo **Entry/Exit control**: **Reader**: los lectores que se pueden conectar (iButton, Wiegand 1 en el borne **G/Y**, Wiegand 2 en el borne **IO**); **En**: el lector puede controlar una salida; **Code**: la operación también se puede ejecutar con un código de usuario (conmutar la salida PGM o controlar la central); **PGM**: la salida controlada (debe estar en modo **Remote control**); **PGM mode**: **Pulse** o **Level**; **Area action**: qué debe pasar con el estado de armado del sistema cuando se acerca una llave o una tarjeta al lector.
- Grupo **Paradox keypad control**: **Utility key**: manteniendo pulsada 3 segundos la tecla auxiliar del teclado, la salida conmuta: durante el tiempo de impulso (**Pulse**) o cambia de estado (**Level**).

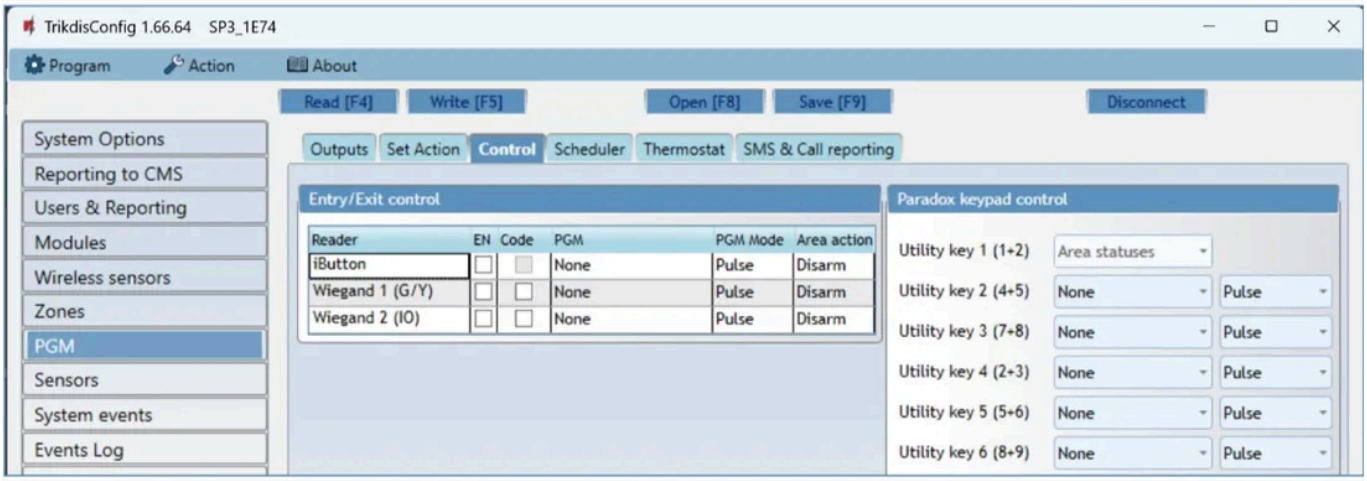


Figura 81. PGM → Control: control de salidas desde los lectores y las teclas de los teclados Paradox.

Pestaña **Scheduler**: **ID**, **Enable**, **Start time** (encendido), **Stop time** (apagado), **Mon – Sun** (días).

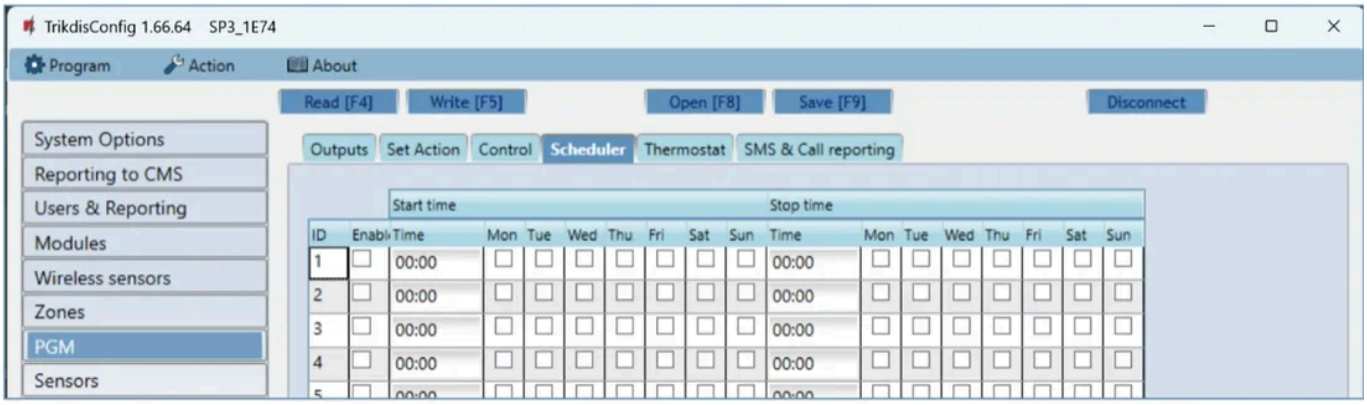


Figura 82. PGM → Scheduler: la programación horaria de las salidas, como máximo diez programaciones.

Pestaña **Thermostat**: **ID**; **PGM No.** (la salida controlada); **Action** (calefacción o refrigeración); **Active** (el termostato funciona con el sensor elegido); **Sensor No** (el sensor de temperatura); **Temperature** (la temperatura que hay que mantener).

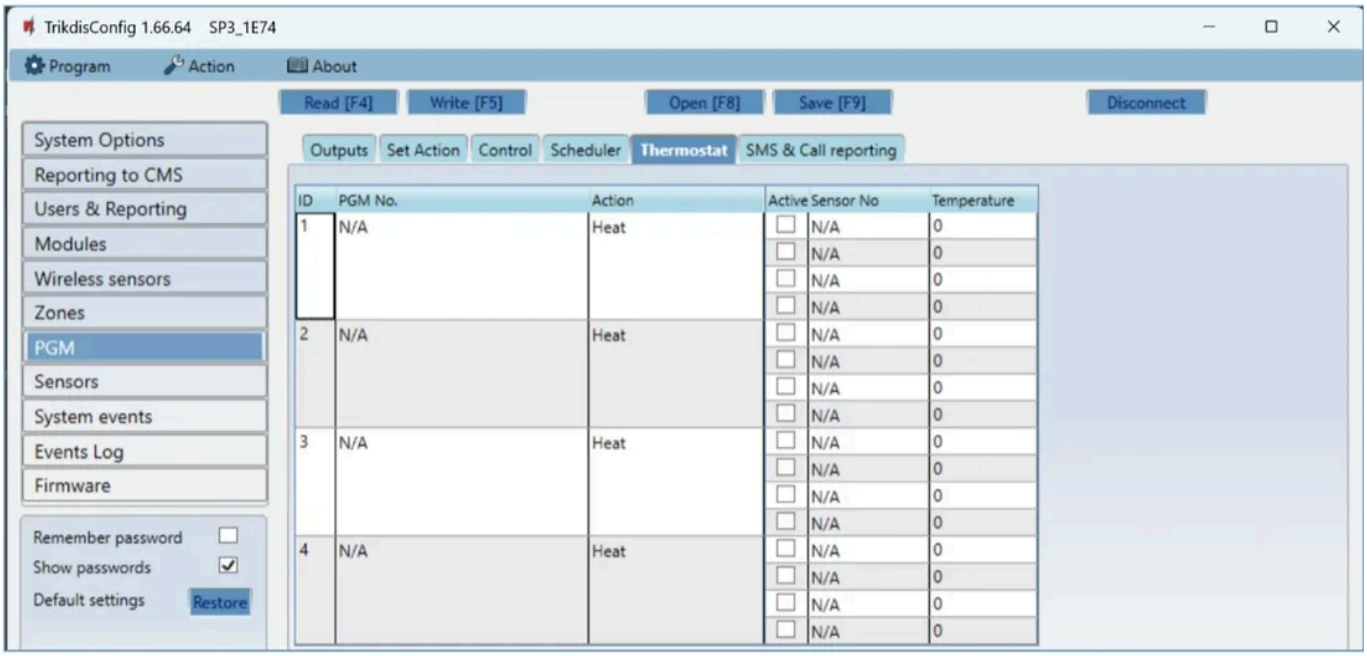


Figura 83. PGM → Thermostat: salida para regular la temperatura.

Pestaña **SMS & Call reporting**: solo se ve si hay algún número de teléfono de usuario, y solo se puede ajustar para los ocho primeros usuarios. **PGM**: el número de la salida y el tipo de evento (**Event**: activación, **Restore**: desactivación); **User / SMS and Call**: quién recibe un SMS y/o una llamada.

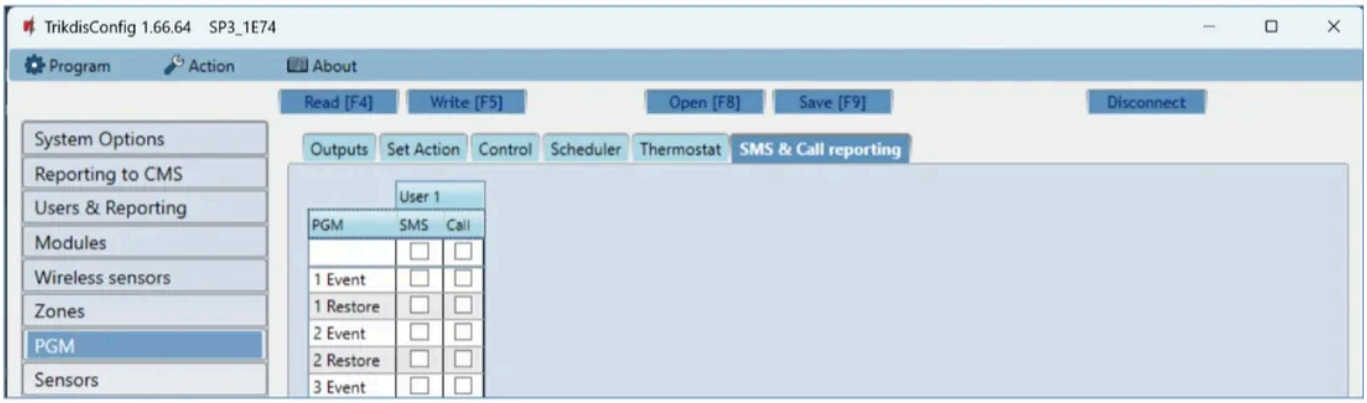


Figura 84. PGM → SMS & Call reporting: aviso de la conmutación de las salidas.

6.9 Sensors

- **ID**: el número de orden del sensor de temperatura.
- **Module type**: el sensor asignado al identificador.
- **Serial No.**: el número de serie del sensor conectado a la central.
- **Sensor name**: el nombre del sensor.
- **Max**: con una temperatura superior a esta se genera un evento, si **High** está marcada.
- **Min**: con una temperatura inferior a esta se genera un evento, si **Low** está marcada.
- **Delay, min**: el evento solo se envía si el valor límite se supera durante estos minutos.
- **Sensor type**: **Dallas 1-Wire**: como máximo ocho sensores, reconocidos automáticamente; **Humidity & Temperature (AM23xx series)**: un sensor de humedad y temperatura AM2301, que hay que elegir a mano en la columna **Module type**.

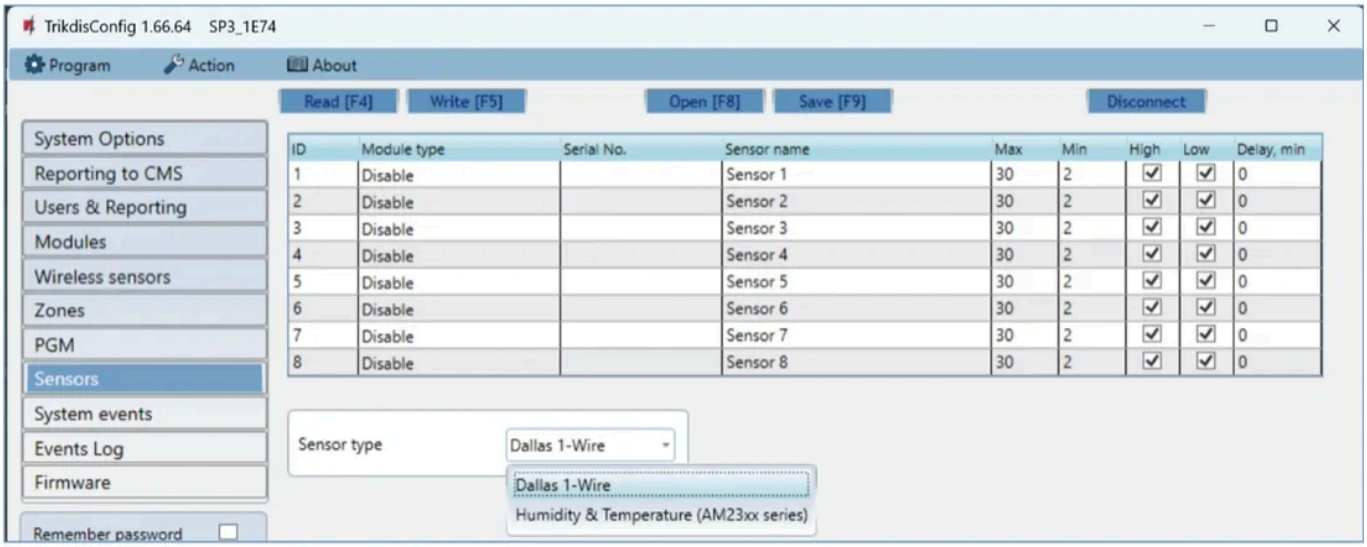


Figura 85. La ventana **Sensors**: valores límite de los sensores de temperatura. La columna del número de serie se ha dejado vacía en la figura.

6.10 System events

Pestaña **Events**:

- **ID**: el número de orden del evento.

- **Event name**: el nombre del evento.
- **Enable**: la vigilancia y la transmisión del evento.
- **CMS**, **Prot.**: aviso a la CRA y a la nube Protegus, respectivamente.
- **CID Code**: el código Contact ID del evento.
- **SMS event text**, **SMS restore text**: el texto SMS del evento y del restablecimiento.

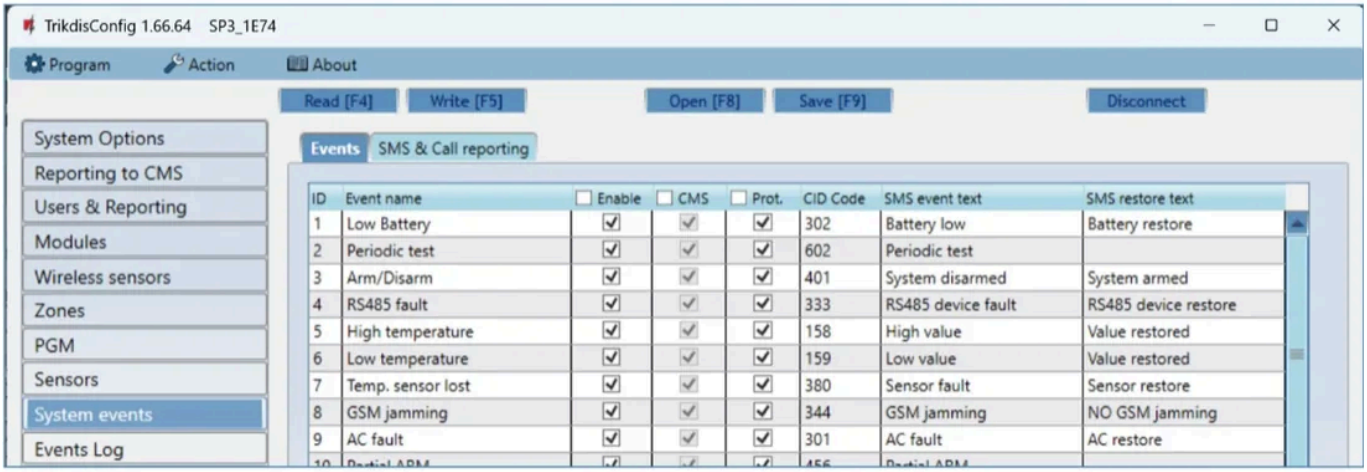


Figura 86. System events → Events: el código, el destino y el texto SMS de los eventos del sistema.

Pestaña **SMS & Call reporting**: solo se ve con un número de teléfono de usuario. **ID**: el número y el tipo de evento (**Event**, **Restore**); **Event SMS text**: el texto del SMS; **User / SMS and Call**: quién recibe un SMS y/o una llamada.

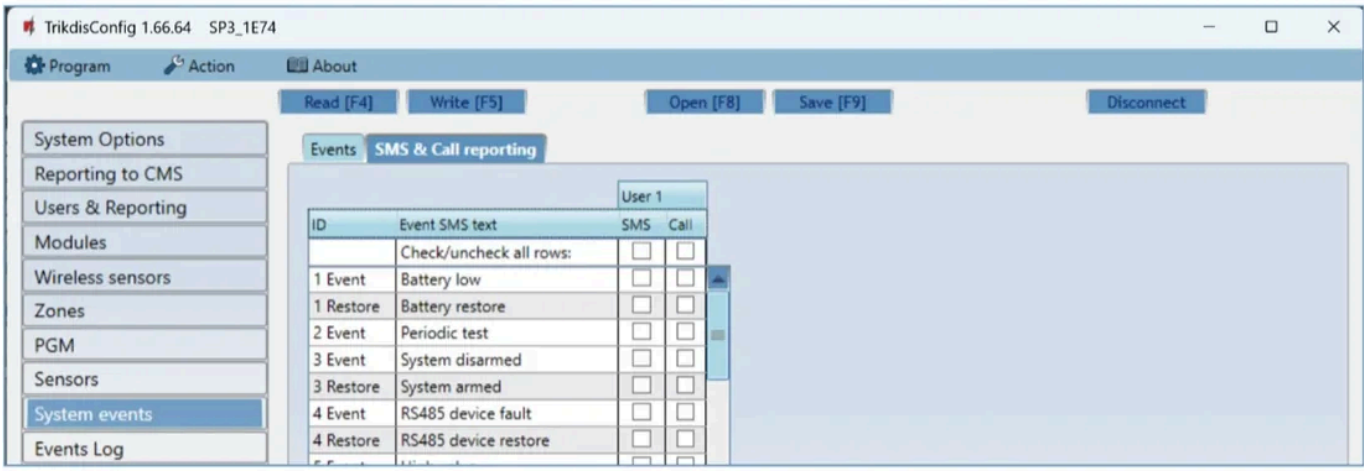


Figura 87. System events → SMS & Call reporting: aviso de los eventos del sistema.

6.11 Events log

- **Read Log**: lee el registro de eventos de la memoria de la central.
- **Clear Log**: borra el registro.
- Las columnas de la tabla: **Event No.**, **Time**, código **CID**, **Event definition**. El registro muestra como máximo 1000 eventos.

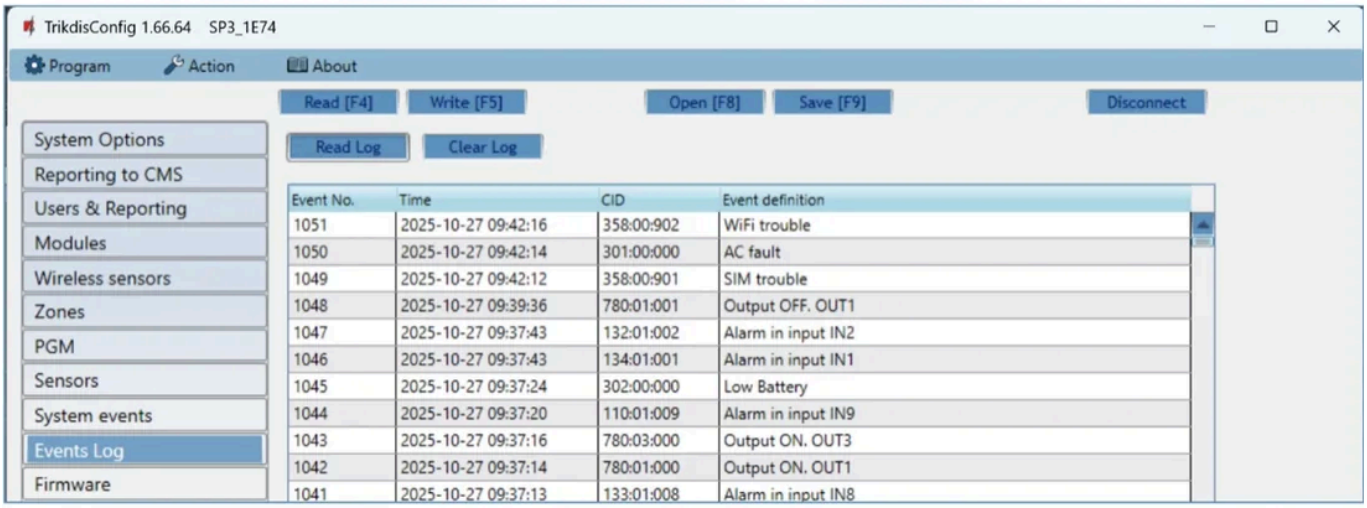


Figura 88. La ventana **Events log**: los últimos 1000 eventos de la central.

Buscar fallos en el registro

Ante una alarma dudosa, lee primero el registro: se ve qué zona dio la señal, cuándo y con qué código, y si el aviso se envió.

6.12 Restablecer la configuración de fábrica

Para restablecer la configuración de fábrica, haz clic en el botón **Restore** del grupo **Default settings**, en la parte inferior izquierda de la ventana de TrikdisConfig. El restablecimiento borra toda la configuración, también los códigos y las contraseñas, así que antes guarda la configuración en un archivo (**Save [F9]**).

Con el código de instalador solo es posible si el administrador no lo ha bloqueado en la pestaña **System Options** → **Access** (6.2.6).

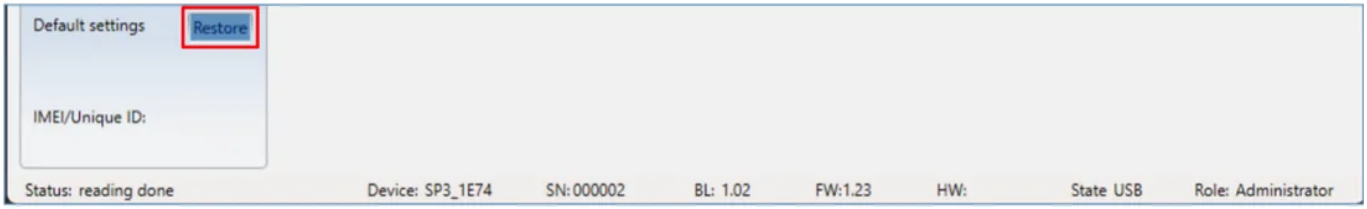


Figura 89. El botón **Restore** del grupo **Default settings**, abajo a la izquierda, restablece la configuración de fábrica.

Después del restablecimiento

Los códigos vuelven a los valores de fábrica (6.2.6); el PIN de la SIM, el APN, los datos WiFi, los usuarios y las zonas se borran. Si antes guardaste la configuración en un archivo (**Save [F9]**), puedes volver a cargarla con los botones **Open [F8]** y **Write [F5]**.

7. Programación remota

TrikdisConfig llega a la "FLEXi" SP3 no solo por cable USB, sino también **a distancia, a través de la nube Protegus**: puedes cambiar la configuración de una central ya instalada, leer el registro de eventos e incluso actualizar el firmware sin ir al lugar de la instalación.

Para el acceso remoto hace falta:

1. La central debe estar encendida y tener conexión de red: el LED **PWR** parpadea en verde; con red móvil, el LED **NET** está verde fijo; con Wi-Fi, el LED **MOD**, y con Ethernet, el LED **ETH** están verde fijo (apartado 1.6). En la versión con módem, la tarjeta SIM está activa y la petición del PIN está desactivada o el PIN está introducido.
2. La **nube Protegus** debe estar activada: ajústala en la ventana **Users & Reporting**, en la primera puesta en marcha por USB (apartado 6.4).
3. Debes conocer el **identificador único** de la central (**IMEI / Unique ID**: figura en la etiqueta de la placa y de la caja, y en la barra de estado de TrikdisConfig) y el código de administrador o de instalador.

Pasos:

1. Inicia el software TrikdisConfig.
2. En la sección **Remote access**, escribe el identificador único de la central en el campo **Unique ID**.
3. Si quieres, ponle un nombre al sistema en el campo **System name**: el programa lo recuerda, y la próxima vez puedes elegirlo de la lista desplegable.
4. Pulsa el botón **Configure**.
5. En la ventana que se abre, haz clic en el botón **Read [F4]** e introduce el código de administrador o de instalador. Con la casilla **Remember password**, el programa lo recuerda.
6. Haz los cambios y envíalos a la central con el botón **Write [F5]**.

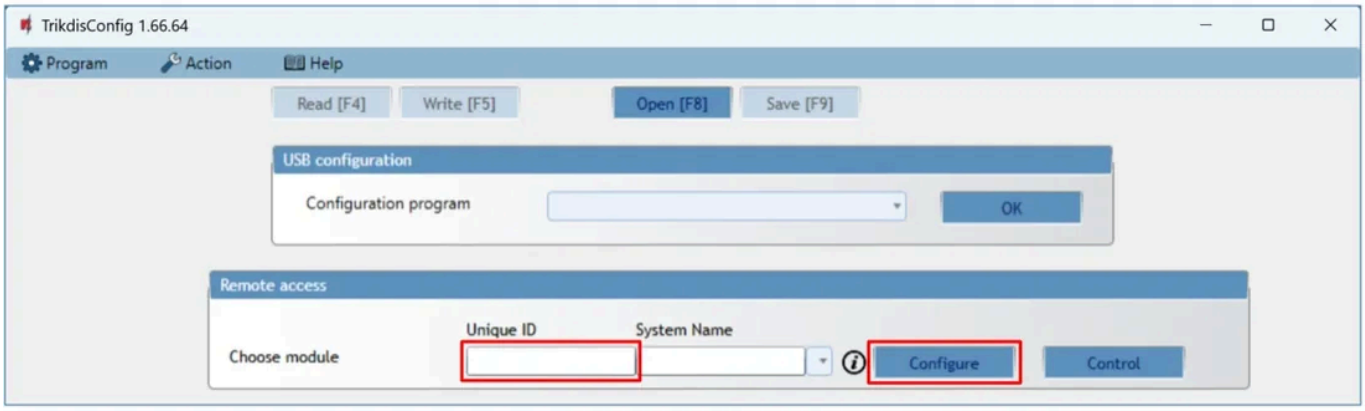


Figura 90. TrikdisConfig – Remote access: el campo Unique ID, System name y el botón Configure.

La programación remota también se puede iniciar desde la aplicación Protegus 2 con la contraseña de instalador; pero para la configuración detallada hace falta TrikdisConfig. Por la red móvil, la conexión remota consume datos: al actualizar el firmware, incluso varios megabytes.

8. Comprobación del funcionamiento del sistema

Después de la conexión y de la programación, comprueba siempre la cadena completa: detector → central → CRA y/o Protegus 2.

1. **Mira los LED.** El LED **PWR** debe parpadear en verde sin destellos rojos, el LED de red (**NET**, **MOD** o **ETH**) debe estar verde fijo, y el LED **DAT** debe apagarse después de que se hayan enviado los eventos (apartado 1.6). Si el PWR destella en rojo, busca el fallo según el capítulo 10.
2. **Provoca un evento.** Arma y desarma el sistema desde el teclado o, con el sistema armado, viola una zona para que se produzca una alarma.
3. **Comprueba la recepción.** El evento debe aparecer en el software de la CRA y/o en la lista de eventos de la aplicación Protegus 2, con el número de partición, de zona y de usuario correcto. En el registro propio de la central (**Events log**, apartado 6.11) también puedes ver si el evento se produjo y si se

envió.

4. **Las zonas, una por una.** Viola por orden todas las zonas (apertura, movimiento, botón de prueba del detector de humo, sabotaje) y comprueba que en el teclado y en Protegus 2 señala la zona correcta.
5. **Salidas.** Conmuta a distancia las salidas PGM desde Protegus 2 y comprueba que el equipo conectado (sirena, piloto, relé) se activa de verdad.
6. **Armado remoto.** Si el sistema también se controla a distancia, ármalo y desármalo también desde la aplicación Protegus 2, y comprueba que el estado del teclado lo sigue.
7. **Corte de alimentación.** Desconecta la alimentación de red: la central debe seguir funcionando con la batería, y debe llegar el evento **AC Fault** y, después de volver a conectarla, el evento **AC Restore** (apartado 2.2).

De fábrica, la central no envía a la CRA (apartado 6.3), pero la nube Protegus está activada de fábrica. Si la CRA no recibe eventos, mira primero la configuración de **Reporting to CMS** y si el LED PWR da 4 o 5 destellos.

9. Actualización 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!

¿Qué archivo elegir?

El nombre del archivo de firmware es **SP3_yxxz_NNNN.fw** (apartado 1.7). La cifra **y** es la versión de hardware: solo se puede cargar el archivo que corresponde a la versión propia de la central; con otra versión, el programa da un error. La cifra **z** es el tipo de detectores inalámbricos (**4** para los detectores MAXIMUM (RF-LORA) y S8 (RF-S8), **1** para el Paradox RTX3); elígela según la instalación; de ella depende también el número de zonas que se pueden gestionar (32 o 64). Las reglas para elegir se describen en el artículo Firmware de la FLEXi SP3: ¿cómo elegir el adecuado?.

Puedes actualizar el firmware tú mismo, a una versión más nueva y, si hace falta, también a una anterior. Tras la actualización, todos los ajustes del dispositivo se mantienen sin cambios.

1. Inicia el software TrikdisConfig y conecta el dispositivo con un cable USB, o entra en su programación de forma remota.
2. Si hay un firmware más reciente, el programa te ofrece descargarlo: acéptalo.
3. Elige la página **Firmware** y haz clic en el botón **Open firmware**. Selecciona el archivo de firmware.
4. Pulsa el botón **Update [F12]**, espera a que termine la actualización y luego haz clic en **OK** en la ventana emergente. Mientras tanto, no desconectes el cable ni interrumpas la conexión.

Los archivos de firmware están en la carpeta de instalación de TrikdisConfig, dentro de la subcarpeta **Firmwares**, en la carpeta con el nombre del dispositivo. Si no existe esa carpeta, o no hay actualización para el dispositivo, o hay que actualizar el propio software TrikdisConfig. Los archivos más recientes también se pueden descargar, como usuario registrado, desde la web del fabricante, en la página del dispositivo.

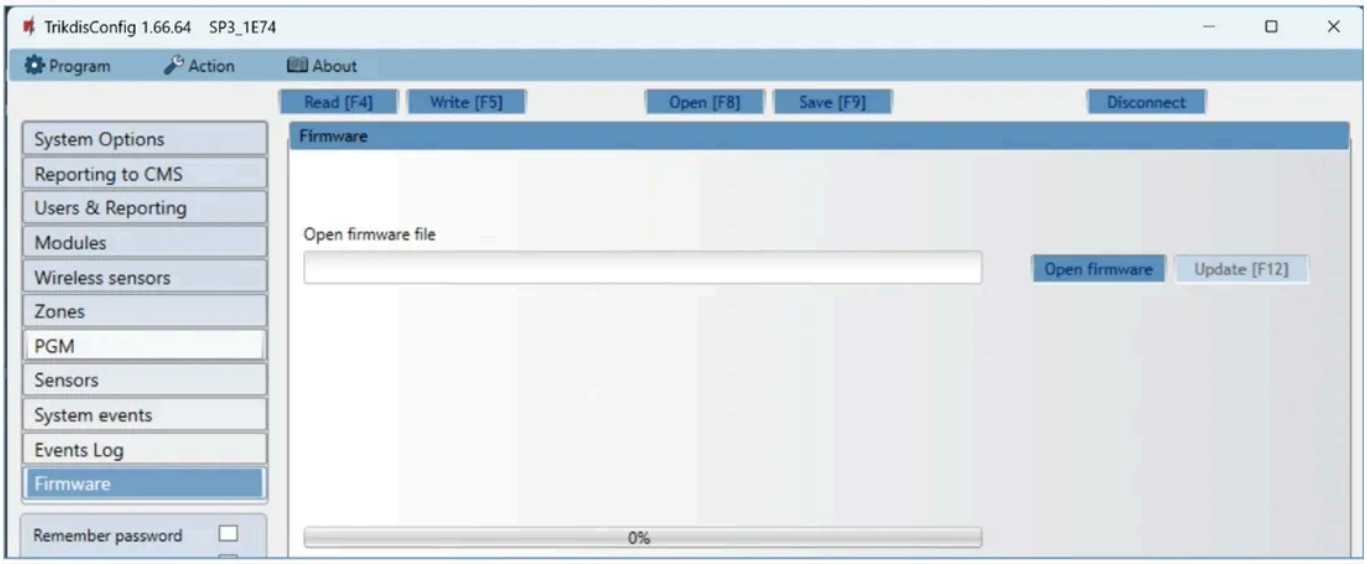


Figura 91. TrikdisConfig – página Firmware: Open firmware y Update [F12].

Después de conectarse, TrikdisConfig ofrece automáticamente actualizar el firmware si hay una versión más reciente; para ello hace falta conexión a internet. Un antivirus o un cortafuegos pueden impedir la descarga automática del firmware; en ese caso, permite TrikdisConfig o descarga el archivo a mano (después de registrarte, en la web de Trikdis) y ábrelo en la página Firmware. Al final de la actualización, haz clic en el botón **Write [F5]** y solo después desconecta el cable USB.

10. Solución de problemas y preguntas frecuentes

Las preguntas y los fallos más frecuentes, partiendo de los LED de la placa (el significado de los LED está en el apartado 1.6). Si la respuesta remite al capítulo detallado, allí encontrarás el lugar exacto del ajuste.

El LED PWR destella en rojo: ¿qué significa el número de destellos?

En funcionamiento normal, el LED **PWR** parpadea en verde. Si hay un fallo, destella en rojo, y el número de destellos indica cuál es el problema:

Destellos	Fallo	Dónde buscar
1	no hay tarjeta SIM	la nano-SIM en la ranura, el contacto (2.4, 6.2)
2	el código PIN de la tarjeta SIM es incorrecto	el PIN en la página **System Options**, o desactiva la petición del PIN en un teléfono (6.2)
3	no puede conectarse a la red móvil	antena, intensidad de la señal (los destellos amarillos del LED **NET**: 0–5; 3 ya es suficiente), si la SIM está activa
4	no hay conexión con el receptor de la CRA por el canal 1	**Reporting to CMS**: dirección, puerto, TCP/UDP, clave de cifrado, identificador del objeto (6.3)
5	no hay conexión con el receptor de la CRA por el canal 2	lo mismo con el receptor de respaldo (6.3)
6	el reloj interno no está en hora	ajuste de la hora en la página **System Options** (6.2)
7	la tensión de la alimentación de respaldo no es suficiente	la batería y sus terminales, la antigüedad de la batería, la corriente de carga (2.2)

Destellos	Fallo	Dónde buscar
8	no hay alimentación de red (AC)	fuente de alimentación, magnetotérmico, bornes de la alimentación principal (2.1)
9	no puede conectarse a la red Wi-Fi	nombre de la red y contraseña, red de 2,4 GHz (ver la pregunta siguiente)

La central no encuentra la red Wi-Fi

1. El módulo Wi-Fi de la "FLEXi" SP3 **solo se conecta a redes de 2,4 GHz** (802.11 b/g/n, WPA / WPA2). No ve las redes de 5 GHz; si el router usa un nombre común para las dos bandas, la banda de 2,4 GHz debe estar activada.
2. Comprueba el nombre y la contraseña de la red en la página **System Options** (6.2), y que el router no filtre los equipos por dirección MAC.
3. El LED **MOD** parpadea en verde mientras se conecta, y queda verde fijo cuando la conexión se ha establecido.
4. Dentro de una caja metálica la señal Wi-Fi puede ser débil: la central funciona de forma fiable con la antena fuera de la caja, con el router cerca de la caja o con una señal más fuerte.

Hay red, pero no llegan eventos a Protegus 2

1. El LED **DAT** está amarillo fijo si hay mensajes sin enviar en la memoria: en ese caso el fallo es la conexión, no la configuración. Mira el LED **NET** / **MOD** y los destellos del PWR.
2. La conexión con la nube Protegus está activada de fábrica; si se ha desactivado, vuelve a activarla con la casilla **Enable cloud service** de la pestaña **Users & Reporting** → **Protegus** (6.4.3). En la pestaña **Reporting to CMS** → **Settings** solo se ajusta por qué vía (SIM, Wi-Fi, LAN) va el tráfico de Protegus.
3. En la página **System events**, el envío del evento en cuestión debe estar activado (6.10): lo que está desactivado aquí, la central no lo envía por ningún canal.
4. ¿Está el equipo vinculado a la cuenta de Protegus 2 (5.1)? Para añadir un sistema nuevo hace falta el identificador único del equipo.

La CRA no recibe eventos

1. La transmisión a la CRA está **desactivada de fábrica**; hay que activarla en la página **Reporting to CMS** e introducir los datos del receptor (6.3).
2. Los 4 o 5 destellos rojos del LED PWR indican que no hay conexión con el receptor por el canal 1 o por el canal 2, respectivamente: dirección, puerto, protocolo (TCP/UDP), clave de cifrado, identificador del objeto.
3. Si están configuradas tanto la CRA como Protegus 2, el evento va primero al receptor y después al usuario; por lo tanto, que el evento aparezca en Protegus 2 no significa que también lo haya recibido el receptor.

¿Qué firmware cargo? ¿Qué significan los números del nombre del archivo?

El nombre del archivo de firmware es `SP3_yxxz_NNNN.fw`. El **primer** número (y) es la versión de hardware (1: Wi-Fi + 4G, 2: Wi-Fi, 3: LAN / LAN + Wi-Fi, 5: Wi-Fi + 2G, 6: LAN + 4G); no se puede cambiar al actualizar, y TrikdisConfig avisa si has elegido un archivo que no corresponde al hardware. El **último** número (z) indica el tipo de receptor inalámbrico y, con ello, el número de zonas: 0 RF-SH (32 zonas), 1 Paradox RTX3 (32), 2 Honeywell (64, no se usa en Europa), 4 detectores MAXIMUM (RF-LORA) o S8 (RF-S8) (64; para los expansores LORA no hace falta). Este sí se puede cambiar: para otro receptor hace falta un firmware con otro número z (1.7 y capítulo 9). El número de cuatro cifras del final es la versión; la regla general es usar la más alta.

¿Cuántas zonas puedo tener y de qué depende?

La placa tiene **10** bornes IO, y cada uno puede ser una zona (entrada) o una salida PGM. Con la duplicación de zonas (ATZ) se pueden conectar dos detectores a un borne, así que son **20** zonas. Con teclados, expansores de la serie iO y LORA, y con un receptor inalámbrico, el número de zonas se puede ampliar **a 32 o a 64**; a cuál de los dos lo decide el último número del firmware (pregunta anterior). El número de particiones es 8.

Sustituyo una central antigua: ¿tengo que cambiar las resistencias de los detectores?

No. En la "FLEXi" SP3 el valor de las resistencias de fin de línea es ajustable, así que los detectores existentes pueden quedarse con las resistencias usadas con la central antigua. El tipo de zona (NC, NO, EOL, 3EOL, ATZ) y los valores de las resistencias se ajustan en la página **Zones** (3.2 y 6.7).

Quiero conectar a una salida un consumo mayor (sirena, cerradura, puerta)

Como salida, el borne IO es de colector abierto y admite **como máximo 100 mA**: directamente solo se le puede conectar un piloto o la bobina de un relé pequeño. Para un consumo mayor, usa un relé según el apartado 3.8. La salida **BELL** admite 1 A, y la salida **AUX** da a los equipos externos como máximo 1 A a 12 V DC: suma el consumo de los teclados, expansores y detectores con la tabla 1.4, y no lo superes.

¿Qué teclado puedo usar y cuántos?

La central admite los teclados Trikdis FLEXi / SK y los teclados Paradox y Crow indicados (la lista y los consumos están en el apartado 1.4). En un bus, **como máximo 8 teclados**, y deben ser **del mismo tipo**. Los teclados LED solo gestionan las dos primeras particiones; para más particiones hace falta un teclado LCD. El teclado FLEXi LCD guarda cuatro idiomas a la vez; si el que necesitas no está entre ellos, hay que actualizar el firmware del teclado: https://trikdis.es/proceso-de-actualizacion-de-firmware-del-teclado-flexi-lcd .

Quiero usar un receptor Paradox RTX3

Para el RTX3, el último número del firmware debe ser **1** (`SP3_xxx1_NNNN.fw`); el archivo lo encontrarás en la carpeta de instalación de TrikdisConfig, en la subcarpeta `Firmwares\SP3\RTX3`, y el proceso de actualización, en el capítulo 9. Después del cambio, la página **Wireless** indica si todavía no hay ningún RTX3 registrado. La frecuencia del RTX3 y la de los equipos inalámbricos deben coincidir (433 u 868 MHz): compruébalo antes de comprar. Detalles: https://trikdis.es/flexi-sp3-modulo-de-expansion-inalambrico-paradox-rtx3 .

La central no responde a los comandos SMS

1. Por SMS y por llamada telefónica solo se pueden controlar las versiones **con módem** (2G / 4G); las centrales solo Wi-Fi o solo Ethernet, no.
2. La estructura del mensaje y la lista de comandos están en el apartado 5.3; la contraseña SMS de fábrica es `123456`, y conviene cambiarla enseguida en el grupo **System Options** → **Access** (6.2).
3. Por llamada y por SMS solo puede controlar el sistema el usuario cuyo número de teléfono figura en la lista de usuarios de la página **Users & Reporting** (6.4).

¿Qué debo configurar sin falta en la primera puesta en marcha?

Con la configuración de fábrica funcionan la mayoría de los sistemas pequeños y medianos, pero no te saltes esto: el cambio del **código maestro** y de los códigos de acceso de instalador / administrador (6.2, 6.4), el ajuste de la **hora** (6.2), el tipo y las resistencias de las zonas (6.7), los usuarios y sus números de teléfono (6.4), los datos del receptor de la CRA, si lo hay (6.3), y la vinculación del sistema con la cuenta de Protegus 2 (5.1). Al final, haz la comprobación del capítulo 8.

11. Garantía e instrucciones de seguridad

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 Garantía y limitación de responsabilidad

La central de alarma tiene una garantía de **24 meses** desde la compra; durante este tiempo, el fabricante repara gratuitamente los defectos de los que sea responsable. La garantía exige que la central la instale una persona cualificada de acuerdo con este manual y con la normativa sobre equipos eléctricos, y que también el uso se ajuste a ellos. Para la reparación, la central se envía en el embalaje original, con la descripción del fallo; una vez terminada la garantía, el mantenimiento y la reparación se pueden solicitar con coste.

La garantía se extingue antes de tiempo si

- la central la ha reparado, o ha intentado repararla, una persona no autorizada;
- se ha usado para un fin distinto del previsto;
- se ha almacenado o instalado en un lugar inadecuado (condiciones climáticas inadecuadas, entorno químico agresivo);
- ha sufrido daños mecánicos o se ha dañado intencionadamente;
- la ha dañado un caso de fuerza mayor (por ejemplo, un rayo).

El fabricante no responde

- del mal funcionamiento de la central si no se ha instalado o usado según el manual;
- del mal funcionamiento de la central si su causa es un fallo o un corte de la conexión de red móvil o de internet, o un fallo de la red del proveedor;
- de la limitación, la suspensión o el corte del servicio de red móvil o de internet, o del suministro eléctrico, ni de los daños materiales o morales que se deriven de ello;
- de los daños materiales o morales sufridos por el comprador o el usuario por robo, intrusión, hurto, incendio u otro siniestro.

11.2 Instrucciones de seguridad

- Antes de usar la central, lee este manual. La “FLEXi” SP3 es un equipo eléctrico: solo puede instalarla y mantenerla una persona cualificada, respetando el manual y la normativa sobre la instalación de equipos eléctricos.
- **Durante la instalación, la central debe estar sin tensión**; antes de cada conexión y de cada intervención de mantenimiento, desconéctala de la alimentación: de la red con el magnetotérmico, y de la batería quitando los terminales.
- Monta la central en un lugar cerrado al que no tengan acceso personas no autorizadas, a una distancia segura de los equipos electrónicos sensibles. La placa no resiste las vibraciones, los golpes mecánicos, la humedad ni los entornos químicos agresivos; cumple la clase ambiental II de la norma EN 50131.

- La caja, el transformador, la batería y el equipo de programación deben cumplir los requisitos de seguridad de la EN 60950.
- La central funciona desde la red de 230 V, 50 Hz a través de un transformador reductor de Clase II (16–18 V AC) o desde una fuente de alimentación de 16–24 V DC; como alimentación de respaldo hace falta una batería de 12 V con una capacidad de al menos 7 Ah. El consumo depende de los equipos externos conectados (apartado 2.1).
- En el circuito de alimentación hay que instalar un interruptor automático magnetotérmico bipolar con una separación de al menos 3 mm entre sus contactos abiertos; el interruptor debe estar en un lugar conocido y accesible para el técnico que hace el mantenimiento de la central.
- Los fallos derivados de una instalación o un uso inadecuados, así como los cambios y las reparaciones no autorizados por el fabricante, anulan la garantía.
- Respeta la normativa local sobre residuos: no tires el equipo averiado, la batería ni los componentes con la basura doméstica.

Ver también

- Firmware de la FLEXi SP3: ¿cómo elegir el adecuado?: el significado del código de hardware y del código de receptor, qué firmware corresponde a cada sistema.
- FLEXi SP3 + módulo de expansión inalámbrico Paradox RTX3: detectores inalámbricos Paradox con la SP3.
- Transceptor RF-S8 y detectores S8: manual de instalación y emparejamiento: los equipos inalámbricos S8 con la SP3: conexión, firmware, emparejamiento.
- Control de accesos inalámbrico y flexible con el sistema GATOR RF-LoRa: los módulos RF-LORA e iO-LORA en un sistema.
- La Trikdis FLEXi SP3 ha obtenido la certificación GRADE 3: qué significa la certificación.
- Trikdis FLEXi SP3: presentación de la central de alarma inteligente: presentación de la central, sustitución de una central antigua.
- Proceso de actualización del firmware del teclado FLEXi LCD: los idiomas del teclado y su actualización.
- Teclado Trikdis FLEXi Keypad SK-LED button: guía rápida de usuario y teclado SK-LCD button: guía rápida de usuario: para el usuario.
- Armado remoto con un interruptor de llave desde la aplicación Protegus 2: si la salida PGM de la SP3 arma otra central.
- Añadir una cámara IP a Protegus 2: imagen en directo en la pantalla de inicio de Protegus 2.
- Documentación en inglés: docs.trikdis.com – Security control panel “FLEXi” SP3.

Los manuales de docs.trikdis.com están en inglés.

Productos relacionados

Trikdis FLEXi SP3 Ethernet central de alarma inteligente

Trikdis FLEXi SP3 WiFi central de alarma inteligente

Trikdis FLEXi SP3 WiFi + 4G central de alarma inteligente

Trikdis FLEXi SP3 WiFi + 2G central de alarma inteligente

Trikdis FLEXi SP3 Ethernet + 4G central de alarma inteligente

Trikdis FLEXi SP3 Ethernet + 2 SIM 4G central de alarma inteligente

Caja metálica mediana con fuente de alimentación para FLEXi SP3

Caja metálica pequeña con fuente de alimentación para FLEXi SP3 **Trikdis FLEXi teclado LCD**

Trikdis FLEXi teclado LED

Derechos de autor

Este manual ha sido elaborado por trikdis.hu y mobilamb.eu. Su texto, su estructura, nuestras propias ilustraciones y sus añadidos son propiedad intelectual nuestra y están protegidos por derechos de autor. Sin nuestro permiso no se puede copiar, distribuir ni publicar en otro sitio web, ni total ni parcialmente. Puedes descargarlo e imprimirlo libremente para instalar y usar el producto.

Los nombres y logotipos Trikdis y Protegus son marcas registradas de UAB Trikdis.

Versión siempre actualizada de este manual: https://trikdis.es/manual-flexi-sp3