Comunicador GT y GT+ – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Trikdis GT y GT+: conexión al bus de datos, al puerto serie o a la salida de línea telefónica de la central de alarma, programación de la central, configuración en TrikdisConfig, transmisión a la CRA y la aplicación Protegus 2.



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

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Versiones: GT y GT+
1.3 Centrales de alarma compatibles
1.4 Partes del comunicador
1.5 Bornes
1.6 Indicaciones LED
1.7 Datos técnicos

2. Puesta en marcha rápida con TrikdisConfig

2.1 Preparativos
2.2 Conexión con la aplicación Protegus 2
2.3 Conexión con la CRA

3. Instalación y conexión

3.1 Pasos de la instalación
3.2 Ubicación y antena
3.3 Conexión a la central de alarma
3.3.1 DSC – bus de datos (Keybus)
3.3.2 DSC – Keybus y TIP/RING (solo GT+)
3.3.3 Paradox – puerto serie
3.3.4 Paradox SP/MG – Keybus y TIP/RING
3.3.5 UTC Interlogix (Caddx) – bus de datos
3.3.6 Texecom – puerto serie
3.3.7 InnerRange Inception
3.3.8 InnerRange Integriti
3.3.9 Honeywell Vista – bus de datos
3.3.10 Cualquier central – TIP/RING
3.4 Conexión de una zona de llave
3.5 Conexión de entradas
3.6 Conexión de una salida con relé
3.7 Conexión del expansor iO-8
3.8 Encendido y primera comprobación
A TRIKDIS átjelző elindítása

4. Programación de la central de alarma

4.1 Conexión al bus de datos o serie
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Conexión por línea telefónica (TIP/RING)
4.2.1 Programación del marcador de la Honeywell Vista
4.2.2 Marcador de la UTC Interlogix (Caddx) NX

5. Control a distancia con la aplicación Protegus 2

5.1 Añadir el equipo

A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armado y desarmado con una salida
5.3 Armado y desarmado desde la aplicación
5.4 Control con mensajes SMS

6. TrikdisConfig – los ajustes en detalle

6.1 La barra de estado
6.2 System settings
6.3 Panel settings
6.4 CMS reporting
6.5 User reporting
6.6 Network settings
6.7 IN/OUT
6.8 RS485 modules
6.9 Event summary
6.10 Restablecer los ajustes de fábrica

7. Programación a distancia

8. Comprobación del funcionamiento del comunicador

9. Actualización del firmware

10. Búsqueda de averías y preguntas frecuentes

11. Instrucciones de seguridad

Ver también

1. Descripción general

El GT y el GT+ son los **comunicadores de red móvil 4G** de Trikdis, que transmiten los eventos de la central de alarma a la CRA y a la aplicación Protegus 2. Se pueden conectar a la central de dos maneras: **directamente**, al bus de datos o al puerto serie de la central (en las centrales DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange y Honeywell), o **al marcador telefónico de cualquier central** (TIP/RING) que envíe los eventos en formato Contact ID con tonos DTMF. El comunicador transmite a la CRA la información completa del evento (código, partición, zona o usuario). Con la aplicación Protegus 2, el usuario controla el sistema a distancia y recibe avisos de los eventos; la aplicación funciona con todas las centrales que admite el comunicador, sea cual sea el fabricante de la central. La transmisión a la CRA y Protegus 2 se pueden usar a la vez. Este manual está hecho para los comunicadores 4G GT y GT+; las diferencias entre las dos versiones se resumen en el apartado 1.2.

1.1 Para qué sirve y cómo funciona

- **Transmite a la CRA.** Envía los eventos por conexión IP al receptor de software o de hardware de Trikdis (protocolo TRK8) –que funcionan con cualquier software de CRA–, a un receptor SIA DC-09 o a un receptor SUR-GARD (TL150). Al receptor SUR-GARD le entrega los códigos Contact ID recibidos de la central convertidos en códigos SIA; la tabla de conversión está en el anexo de la documentación en inglés de Trikdis. Comprueba la conexión con el receptor cada 30 segundos (o con el intervalo configurado) mediante mensajes PING; si el canal principal se corta, pasa al canal de respaldo. Con un canal paralelo, los eventos van a la vez a dos receptores. Si el servicio Protegus también está activado, el evento lo recibe primero la CRA y solo después la aplicación de los usuarios.
- **Avisa al usuario.** La aplicación Protegus 2 avisa de los eventos con notificaciones push y con un sonido propio; desde la aplicación el usuario puede armar y desarmar y accionar los dispositivos conectados (iluminación, puerta, ventilación, calefacción, riego, etc.). En la aplicación, los permisos del administrador, del instalador y del usuario son distintos. Además de Protegus 2, también se pueden pedir avisos por SMS y por llamada telefónica.
- **Controla la central directamente.** Conectado al bus de datos o al puerto serie, el comunicador también ve el estado de las particiones y zonas de la central, y el usuario arma y desarma desde Protegus 2 con su propio código de teclado; para ello no hace falta una zona de llave. El GT+ se puede conectar en las centrales DSC al bus de datos (Keybus) y a los bornes TIP/RING a la vez: el bus sirve para el control y los estados, y los eventos se envían con los códigos Contact ID propios de la central (apartado 3.3.2).
- **Tiene entradas y salidas propias.** Dos bornes de E/S de doble función se pueden usar como entrada (IN) o como salida controlable (OUT). Las salidas se pueden accionar desde la aplicación Protegus 2 y con comandos SMS. Con expansores iO-8 conectados al bus RS485 se pueden añadir más entradas y salidas.
- **Configuración.** La configuración se puede guardar en un archivo y escribir en otros comunicadores. Hay dos niveles de acceso: el del administrador de la CRA y el del instalador. El comunicador también se puede configurar a distancia, y su firmware también se puede actualizar a distancia.

La estructura del sistema se ve en el esquema siguiente: la central de alarma se conecta al comunicador, el comunicador llega a internet a través de la red móvil (LTE), y desde allí al receptor de la CRA (y a su software) y al servidor de Protegus; el usuario ve el sistema en la aplicación Protegus 2 y, a través de la red móvil, también puede recibir SMS y llamadas.

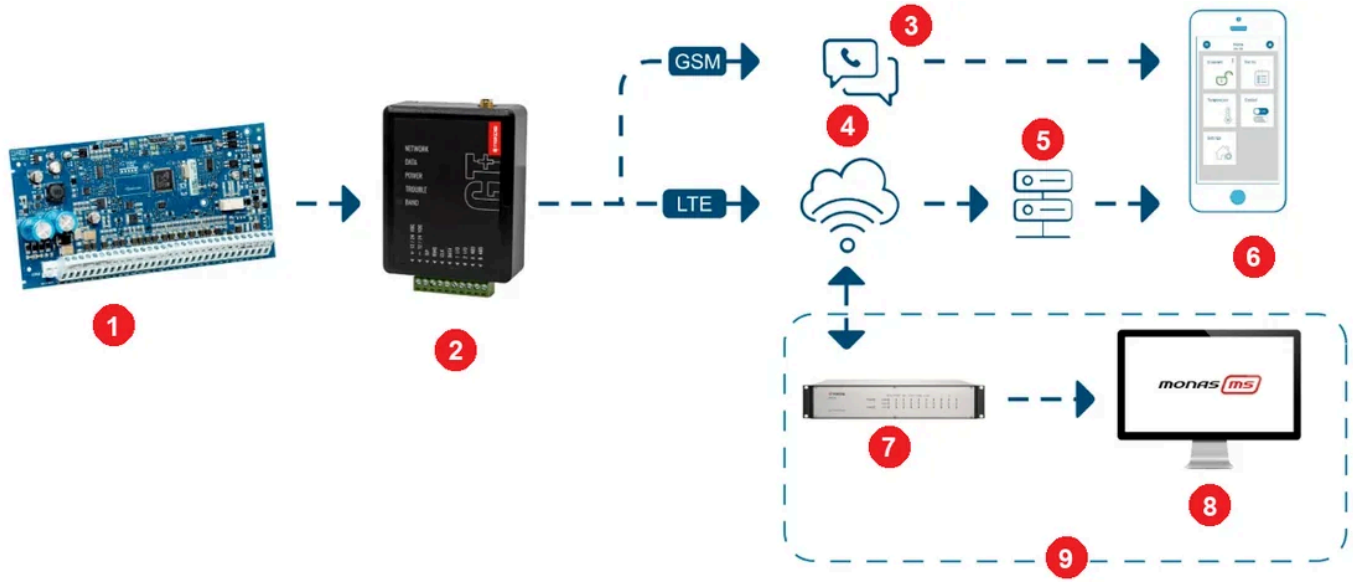


Figura 1. El lugar del comunicador en el sistema: central de alarma → GT / GT+ → red móvil → internet → receptor de la CRA y servidor de Protegus → aplicación Protegus 2; SMS y llamadas directamente por la red móvil.

- 1 central de alarma («Alarm panel»)
- 2 comunicador LTE GT / GT+ («LTE communicator»)
- 3 llamada y SMS («Call/SMS»)
- 4 internet («Internet»)
- 5 servidor de Protegus («Protegus server»)
- 6 teléfono con la aplicación Protegus («Phone with Protegus software»)
- 7 receptor de la CRA («Receiver»)
- 8 software de CRA («Monitoring software»)
- 9 la central receptora de alarmas de la empresa de seguridad («Monitoring station in security company»), en el recuadro discontinuo

1.2 Versiones: GT y GT+

El GT y el GT+ son el mismo dispositivo en dos versiones: su conexión, su configuración y su funcionamiento son casi idénticos, por eso los describimos en un solo manual. Las diferencias se resumen en la tabla siguiente; donde el texto da el dato del GT+, en el GT ten en cuenta este.

	GT	**GT+**
Tensión de alimentación	10–18 V DC	10–32 V DC
Rótulo de los bornes de alimentación	+12 VDC, −12 VDC	+12 / 24 VDC, −12 / 24 VDC
Conexión de la central DSC	solo al bus de datos (Keybus)	al bus de datos, o al bus de datos y a los bornes TIP/RING a la vez; así los eventos se envían con los códigos Contact ID propios de la central (p. ej., incendio: E110), no como alarma genérica (E130)
Ajuste de la conexión por línea telefónica (TIP/RING) en TrikdisConfig (**Panel settings → Communication protocol**)	**2. Dual tone**	**2. AUTO** (en la lista también se puede elegir **3. MANUAL**)
Comprobación en DSC con conexión bus + TIP/RING (capítulo 8)	–	la alarma de la zona de incendio debe llegar como E110

	GT	GT+
Todo lo demás: entradas/salidas, bus RS485, módem, LED, tamaño, protocolos, Protegus 2, comandos SMS	igual	igual

Las dos versiones se fabrican con tres tipos de módem; para el mercado europeo, también para España, corresponde la versión europea (EU). El tipo de módem y la versión de hardware los encuentras en la barra de estado de TrikdisConfig (**Device**, **HW**) y en la etiqueta del dispositivo.

Módem	Red y bandas de frecuencia
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8
EG915U-LA (Latinoamérica)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Centrales de alarma compatibles

Las centrales siguientes se pueden conectar directamente al comunicador, por bus de datos o por puerto serie. La columna «control directo» indica si el usuario puede armar y desarmar desde Protegus 2 con su propio código de teclado sin conexiones adicionales; donde no es posible, el comunicador lee los eventos del bus y para el control hace falta una zona de llave (apartado 3.4).

Fabricante	Modelo	Conexión	Control directo
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864	bus de datos (Keybus); GT+: también Keybus + TIP/RING	sí
DSC	PC5020	bus de datos (Keybus)	no
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	puerto serie (cable EX-CRP2.4), o Keybus + TIP/RING	sí
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	puerto serie (cable EX-CRP2.4), o Keybus + TIP/RING	sí
Paradox	Digiplex EVO192, EVOHD, EVOHD+	puerto serie (cable EX-CRP2.4)	sí
Paradox	Digiplex EVO48	puerto serie (cable EX-CRP2.4)	no
Paradox	Spectra 1727, 1728, 1738; Esprit E55	puerto serie (cable EX-CRP2.4)	no
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	bus de datos	sí
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	puerto serie (cable EX-CRP4)	sí
InnerRange	Inception, Integriti	puerto serie (con el cable del fabricante de la central)	no
Honeywell	Ademco Vista-15, Vista-20, Vista-48	bus de datos	sí

- El firmware de las centrales **Paradox** de control directo debe ser como mínimo **V.4**. En las centrales Paradox más nuevas (SP+, MG+, EVOHD+) el puerto serie puede venir bloqueado de fábrica; el desbloqueo se explica en el apartado 4.1.2. Las centrales Spectra SP / SP+ y Magellan MG / MG+ también se pueden conectar, en lugar del puerto serie, al bus de datos (Keybus) y a los bornes TIP/RING a la vez; para ello no hace falta el desbloqueo de pago (apartado 3.3.4).
- Las centrales de **cualquier otro fabricante** se conectan a través de su marcador telefónico (TIP/RING), si este envía los eventos en formato Contact ID con marcación DTMF; en ese caso, para el control hace falta una zona de llave.
- Qué comunicador Trikdis y qué conexión corresponde a tu central lo puedes consultar en el buscador de compatibilidad.

1.4 Partes del comunicador

La placa de circuito impreso del comunicador va en una caja de plástico negra; la tapa frontal se quita a presión y la regleta de bornes es extraíble. En la figura siguiente se ve el GT+; el GT es igual, solo que el rótulo de la caja es GT y el de los bornes de alimentación, +12 VDC / −12 VDC.

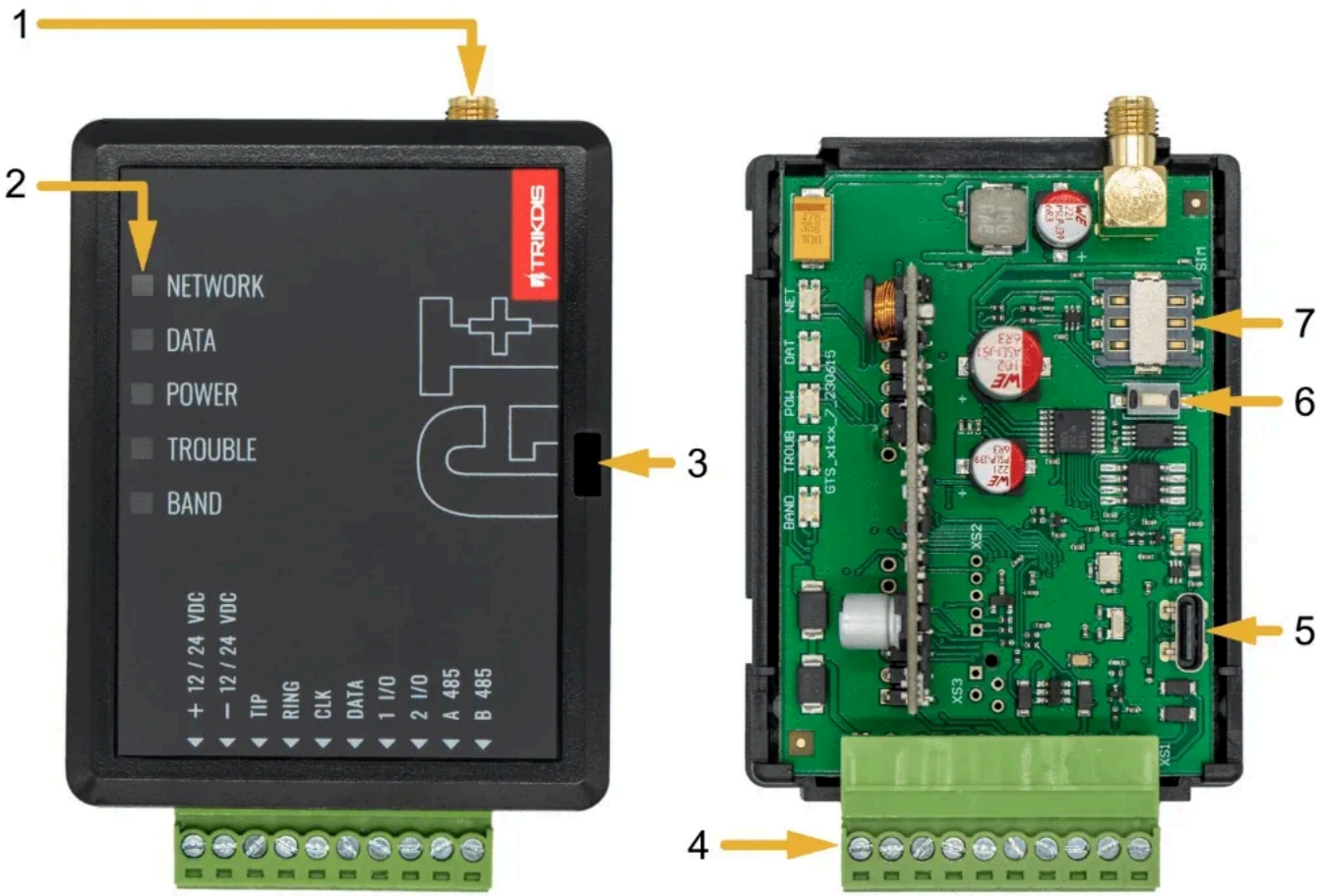


Figura 2. Partes del comunicador por delante (izquierda) y con la caja abierta (derecha).

- 1 Conector SMA de la antena móvil
- 2 Indicadores LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Ranura para ayudar a quitar la tapa frontal
- 4 Regleta de bornes extraíble para las conexiones externas
- 5 Conector USB-C para la programación
- 6 Botón RESET
- 7 Ranura de la tarjeta nano-SIM

La regleta de bornes es extraíble: así el dispositivo se puede dejar sin alimentación o reiniciar con un solo movimiento, es más fácil de manejar durante la conexión y, para programarlo por USB, se puede llevar al ordenador.

1.5 Bornes

Borne (GT)	Borne (GT+)	Función
+12 VDC	**+12 / 24 VDC**	Alimentación, positivo: +10–18 V DC (GT), +10–32 V DC (GT+)
–12 VDC	**–12 / 24 VDC**	Alimentación, 0 V
TIP	**TIP**	Borne TIP del marcador telefónico de la central de alarma
RING	**RING**	Borne RING del marcador telefónico de la central de alarma
CLK	**CLK**	Bus serie o bus de datos (reloj) para la conexión directa de la central
DATA	**DATA**	Bus serie o bus de datos (datos) para la conexión directa de la central
1 I/O	**1 I/O**	Entrada/salida 1 (ajuste de fábrica: entrada, NO)
2 I/O	**2 I/O**	Entrada/salida 2 (ajuste de fábrica: entrada, NO)
A 485	**A 485**	Hilo A del bus RS485
B 485	**B 485**	Hilo B del bus RS485

En los esquemas de conexión, los bornes de alimentación se indican de forma unificada como **+DC** y **–DC** (en el GT son los bornes +12 VDC / −12 VDC; en el GT+, +12 / 24 VDC / −12 / 24 VDC), y los bornes RS485 como **A RS485** / **B RS485** (en el dispositivo, A 485 / B 485). El rótulo de la regleta de bornes también figura en la tapa frontal.

1.6 Indicaciones LED

Los LED de la tapa frontal son la herramienta más importante para la puesta en marcha y la búsqueda de averías. Interprétalos juntos: POWER indica la alimentación; NETWORK, la red; TROUBLE, la avería, y BAND, el tipo de red.

NETWORK – conexión a la red

Indicación	Significado
apagado	No hay conexión con la red móvil
parpadea en amarillo	Conexión a la red móvil en curso
encendido en verde, parpadea en amarillo	Conectado a la red móvil; el número de destellos amarillos es el **nivel de señal**: en 4G, 3 destellos es una señal adecuada

DATA – tráfico de datos

Indicación	Significado
apagado	No hay eventos pendientes de envío
encendido en verde	Hay eventos pendientes de envío en la memoria
parpadea en verde	Transferencia de datos entre el comunicador y el ordenador (durante la programación)

Comprobación rápida

El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del operador; en uno Ethernet, que la conexión hasta el router funciona–, pero no que el dispositivo también salga a Internet. Si el LED NETWORK está en verde, pero el LED DATA sigue encendido de forma continua tras un evento o un informe de prueba, la conexión a Internet no funciona: el mensaje no puede salir. En red móvil lo más habitual es que fallen el APN o el servicio de datos de la tarjeta SIM; en Ethernet, el router, el cortafuegos o el DNS. Si el LED DATA se apaga, el mensaje se ha enviado y la conexión de datos está bien.

POWER – tensión de alimentación

Indicación	Significado
apagado	No hay alimentación, o la alimentación está desconectada
encendido en verde	Encendido, la tensión de alimentación es correcta
encendido en amarillo	Tensión de alimentación inadecuada (11,5 V o menos)
encendido en verde, parpadea en amarillo	Listo para la programación (durante la programación)
encendido en amarillo (durante la programación)	No hay conexión con el ordenador

TROUBLE – avería

Indicación	Significado
apagado	No hay avería
1 destello rojo	No hay tarjeta SIM
2 destellos rojos	Error del PIN de la SIM (código PIN incorrecto)
3 destellos rojos	Error de programación (no hay APN)
4 destellos rojos	No puede registrarse en la red móvil (error de registro)
5 destellos rojos	No puede conectarse a la red de datos (GPRS/UMTS)
6 destellos rojos	No hay conexión con el receptor de la CRA
7 destellos rojos	Se ha perdido la conexión con la central de alarma
8 destellos rojos	El ICCID configurado no coincide con el ICCID de la tarjeta SIM (apartado 6.6)
parpadea en rojo (durante la programación)	Error de memoria
encendido en rojo (durante la programación)	Firmware dañado

BAND – tipo de red

Destellos verdes	Red
1	ninguna
2	GSM
3	GPRS
4	EDGE

Destellos verdes	Red
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.7 Datos técnicos

Parámetro	Valor
Conexión con la central de alarma	bus serie, bus de datos (Keybus) o línea telefónica (TIP/RING, Contact ID, DTMF)
Entradas/salidas	2 E/S de doble función: como entrada NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistencia de fin de línea de 2,2 kΩ); como salida de colector abierto (OC), máx. 0,15 A / 30 V DC. Ampliable con expansores iO-8
Módem	EG915U-EU (Europa), EG915U-LA (Latinoamérica) o BG95-M5 (LTE Cat M1); las bandas de frecuencia se enumeran en la tabla del apartado 1.2
Tensión de alimentación	GT: 10–18 V DC; GT+: 10–32 V DC
Consumo de corriente	como máximo 100 mA en reposo; como máximo 200 mA durante el envío de datos
Protocolos de transmisión	TRK8, DC-09_2007, DC-09_2012, TL150
Cifrado	AES-128
Programación	TrikdisConfig (Windows) con cable USB-C o a distancia
Entorno de funcionamiento	−10 … +50 °C, máx. 80 % de humedad relativa (a +20 °C)
Tamaño	92 × 62 × 26 mm
Peso	80 g

2. Puesta en marcha rápida con TrikdisConfig

Todos los ajustes del comunicador se hacen con el programa **TrikdisConfig**, que funciona en Windows, por cable USB-C o a distancia. En este capítulo describimos el camino más corto: configuras el equipo sobre la mesa, antes de conectarlo, y después en la instalación solo queda conectarlo. Explicamos qué ajustes hacen falta para que el comunicador envíe eventos a la CRA y para que el sistema se pueda controlar desde la aplicación Protegus 2; la explicación detallada de los ajustes está en el capítulo 6.

2.1 Preparativos

Qué necesitas

Cable USB-C para la programación · cable de al menos 4 hilos entre el comunicador y la central · para el puerto serie de Paradox, cable CRP2.4 · destornillador plano de 2,5 mm · antena móvil de ganancia adecuada, si en el lugar la cobertura es débil · tarjeta SIM activa (la petición de PIN se puede desactivar) · el manual de instalación de la central de alarma.

Los accesorios necesarios se piden por separado al distribuidor.

1. Descarga e instala el software TrikdisConfig. En la web de Trikdis (www.trikdis.com), escribe en el campo de búsqueda: «TrikdisConfig».

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Abre la caja del comunicador con un destornillador plano: introduce el destornillador arriba, en la ranura junto a la antena, y haz palanca hacia fuera; después, abajo, en la abertura, hacia abajo. La figura también muestra dónde está el conector USB-C, en el borde de la placa de circuito impreso.

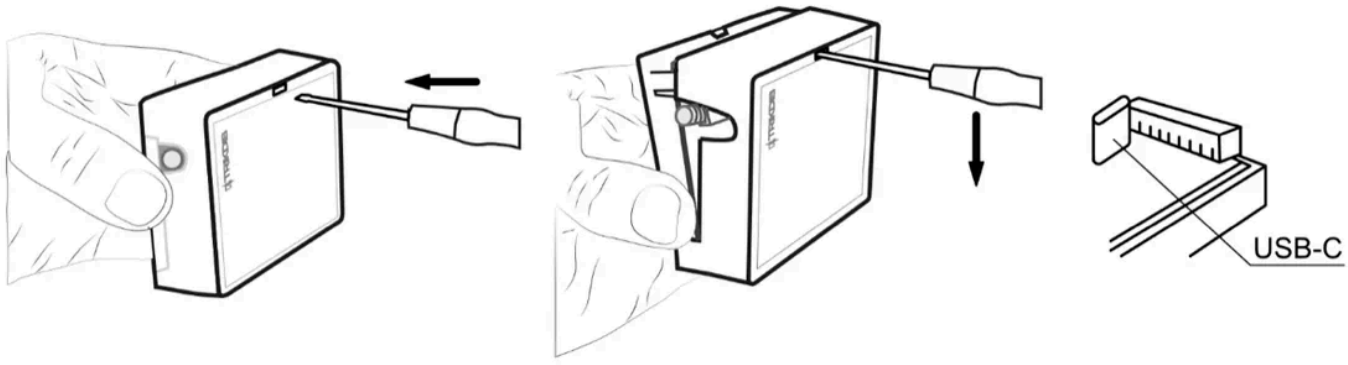


Figura 3. Cómo quitar la tapa frontal con un destornillador plano; el detalle ampliado es el lugar del conector USB-C.

3. Coloca la tarjeta nano-SIM en la ranura, en la orientación que muestra la figura. La tarjeta debe estar activa y tener servicio de datos móviles y, si es posible, desactiva en ella la petición de PIN con un teléfono (así no hace falta escribir el PIN en el equipo).

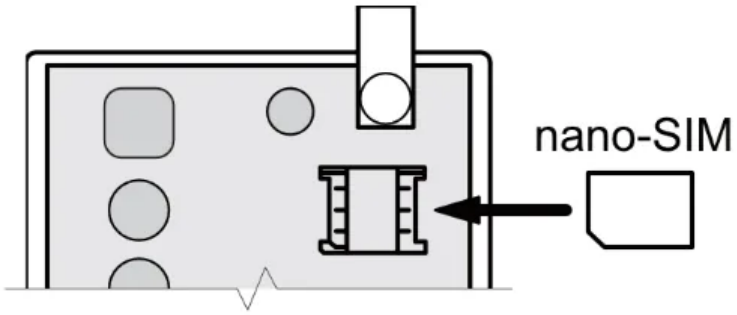


Figura 4. El lugar de la tarjeta nano-SIM en la placa de circuito impreso.

4. Conecta el comunicador al ordenador con un cable USB-C.

Advertencia

Mientras el dispositivo está conectado al ordenador por cable USB, se encuentra en modo de programación: deja de funcionar con normalidad, no vigila, no transmite y no se puede controlar; se alimenta del USB y se reinicia al desconectar el cable. Por eso el dispositivo no debe estar al alcance de cualquiera: debe estar en una caja metálica cerrada, con protección antisabotaje (tamper) o con un detector de movimiento que vigile la caja. Más detalles en las preguntas frecuentes

5. Abre TrikdisConfig. El programa reconoce el equipo y abre la ventana de programación. Haz clic en el botón **Read [F4]** (leer): el programa lee los ajustes actuales del equipo. Si pide contraseña, introduce el código de 6 dígitos del administrador (de fábrica, `123456`) o del instalador (de fábrica, `654321`).

2.2 Conexión con la aplicación Protegus 2

Primero, en la página **Panel settings**, indica cómo se conecta el comunicador a la central.

Si lo conectas a la salida de línea telefónica (TIP/RING) de la central: en el campo **Communication protocol**, elige el valor **AUTO** (en el GT, el segundo elemento de la lista es **Dual tone**; allí, ese).

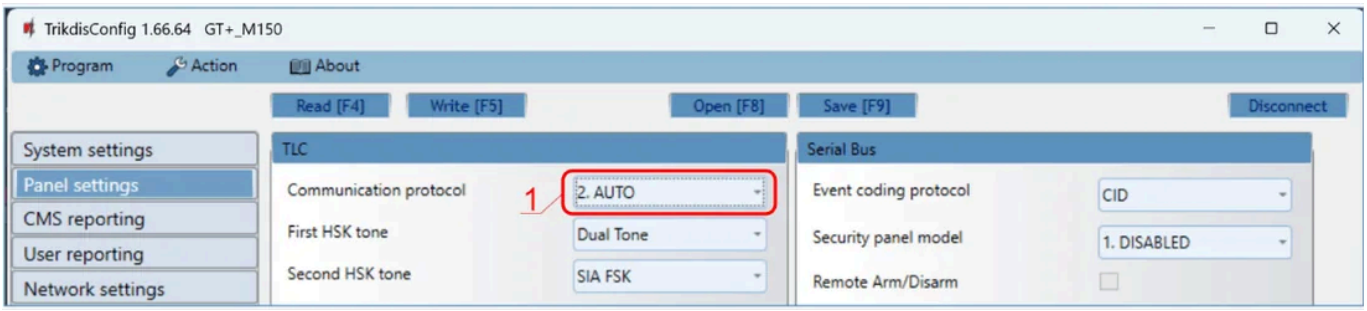


Figura 5. TrikdisConfig – Panel settings, grupo TLC (en la imagen, el ajuste del GT+).

- 1 **Communication protocol** – con conexión TIP/RING, **2. AUTO** (GT: **2. Dual tone**).

Si lo conectas al bus de datos o al puerto serie de la central: en el grupo **Serial bus**, configura la central.



Figura 6. TrikdisConfig – Panel settings, grupo Serial bus.

- 2 **Security panel model** – el modelo de la central conectada.
- 3 **Remote Arm/Disarm** – márcalo si los usuarios quieren controlar la central desde Protegus 2 con su propio código de teclado. Solo aparece en las centrales de control directo.
- 4 **Security panel PC download password** – para el control directo de centrales Paradox y Texecom, la contraseña de PC o de UDL configurada en la central; las dos deben coincidir.

GT+, central DSC en el bus de datos y en los bornes TIP/RING a la vez: el **Communication protocol** debe ser **AUTO**, el **Security panel model**, el modelo DSC, y marca la opción **Remote Arm/Disarm** si se va a controlar la central desde Protegus 2 (apartado 3.3.2).

Para el control directo también hay que configurar la central de alarma; esto se describe en el capítulo 4, donde también encuentras cómo introducir la contraseña de PC o de UDL.

Después, en la página **User reporting**, en la pestaña **PROTEGUS Cloud**, activa la conexión con la nube.

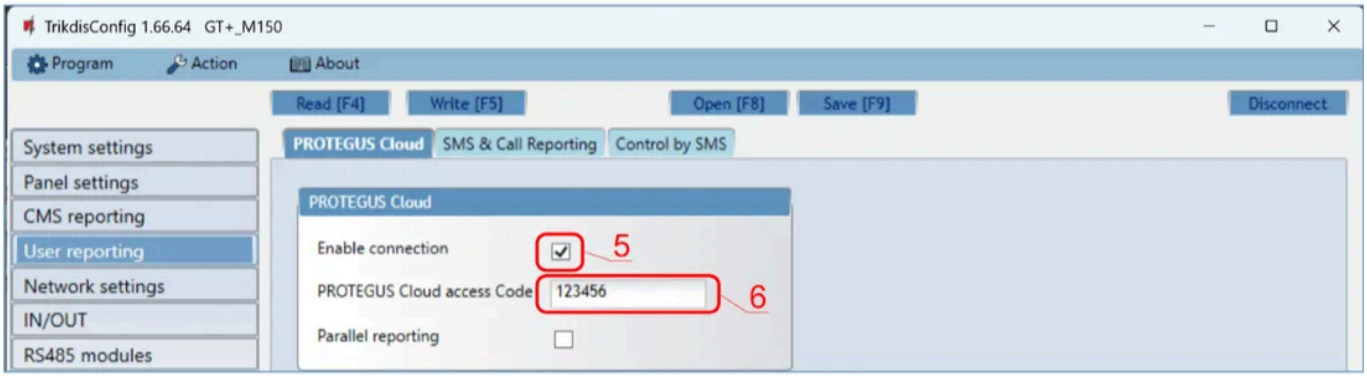


Figura 7. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- 5 **Enable connection** – márcalo: activa la conexión con la nube de Protegus.
- 6 **PROTEGUS Cloud access Code** – el código de acceso a Protegus 2 (de fábrica, `123456`). Cámbialo si quieres que el usuario tenga que introducirlo al añadir el sistema a la aplicación. Importante: si más adelante cambias el código en TrikdisConfig, también hay que cambiarlo en la aplicación Protegus 2.

Por último, en la página **Network settings**, en la pestaña **SIM1**, introduce los datos de la tarjeta.

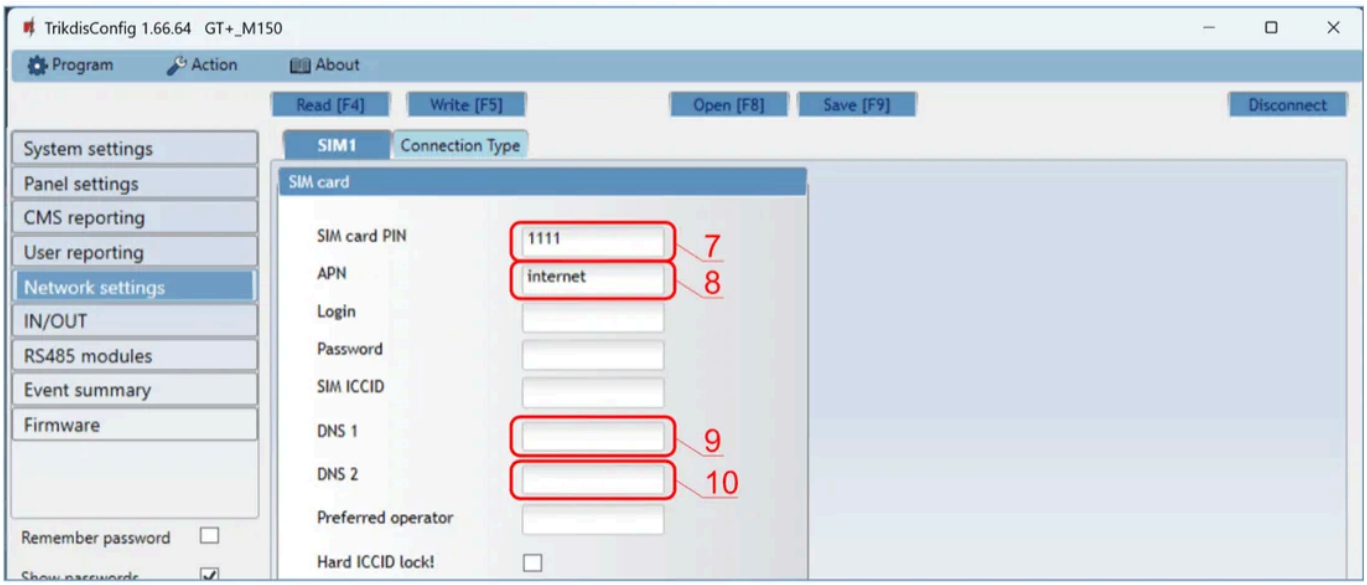


Figura 8. TrikdisConfig – Network settings, pestaña SIM1.

- 7 **SIM card PIN** – el código PIN de la tarjeta (si la petición de PIN está desactivada, se puede dejar el valor de fábrica).
- 8 **APN** – el punto de acceso de datos del operador (ver más abajo).
- 9 **DNS 1** – servidor de nombres principal; de fábrica, el DNS de Google. Independientemente de los ajustes IP, comprueba que las direcciones DNS funcionan con tu operador.
- 10 **DNS 2** – servidor de nombres secundario (de fábrica, también el de Google).

El APN (Access Point Name) es el punto de acceso de datos del operador móvil; sin él, el equipo no puede conectarse a internet. El valor exacto lo encuentras en la web del operador de la tarjeta SIM. Los APN conocidos de los operadores europeos los recogemos en un artículo aparte: Configuración del APN – lista de operadores móviles europeos. Si el operador no te ha dado otro dato, prueba el APN `internet`: es genérico y funciona en las redes de muchos operadores.

Para las tarjetas de datos IoT / M2M (entre máquinas), el operador suele dar **un APN distinto del de las tarjetas para particulares**; con el APN de particulares el equipo no se conecta. Este valor también lo encuentras en el artículo de los APN, o pídeselo al operador; si el operador también te da un nombre de usuario y una contraseña, escríbelos también.

Si el equipo no transmite a una CRA, la configuración ya está lista: pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB.

Con la conexión por línea telefónica (TIP/RING), no olvides activar y configurar el marcador de la central de alarma; si no, la central no envía eventos. Para el control directo, también hay que configurar las centrales Paradox, Texecom, Caddx, InnerRange y Honeywell. La configuración de la central se describe en el capítulo 4.

2.3 Conexión con la CRA

Si el equipo también transmite a un receptor de CRA, primero, en la página **System settings**, introduce el identificador de abonado.

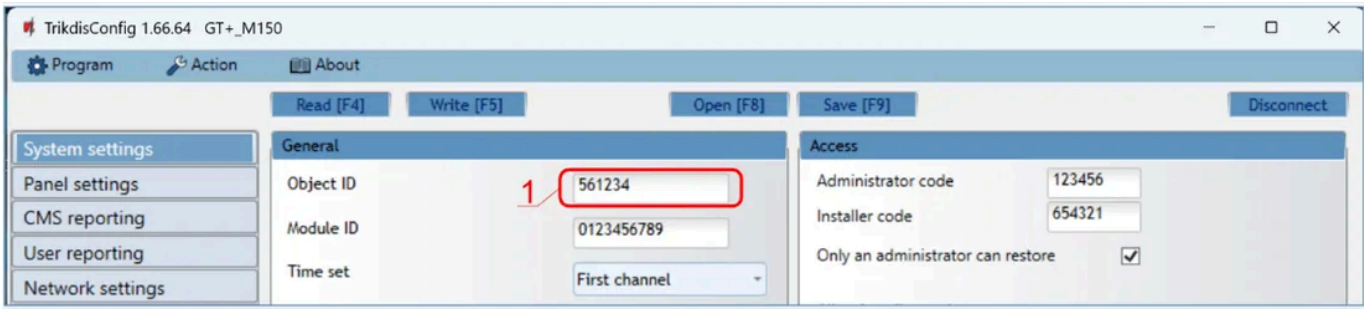


Figura 9. TrikdisConfig – página System settings, grupo General.

- 1 **Object ID** – el identificador de abonado que te da la CRA (6 caracteres hexadecimales, 0–9, A–F). No se pueden usar `FFFE` ni `FFFF`.

En la página **Panel settings**, indica la conexión de la central si no lo has hecho ya en el apartado 2.2: con conexión TIP/RING, el **Communication protocol** debe ser **AUTO** (GT: **Dual tone**); con conexión al bus de datos o serie, elige en el campo **Security panel model** el modelo de la central conectada (las figuras del apartado 2.2).

Después, en la página **CMS reporting**, en la parte **Primary channel** (canal principal), configura los datos del receptor.

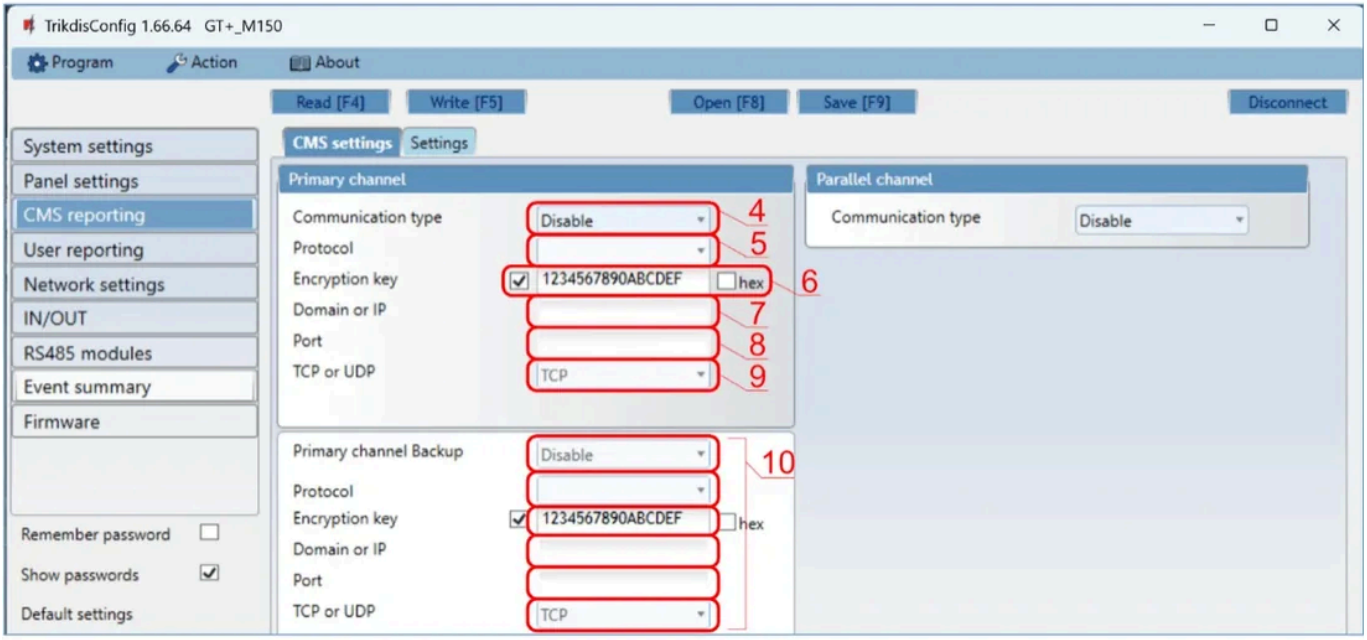


Figura 10. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 4 **Communication type** – elige la conexión **IP**.
- 5 **Protocol** – **TRK8** para un receptor Trikdis, **DC-09_2007** o **DC-09_2012** para un receptor universal, **TL150** para un receptor SUR-GARD.
- 6 **Encryption key** – la clave de cifrado configurada en el receptor.
- 7 **Domain or IP** – el nombre de dominio o la dirección IP del receptor.
- 8 **Port** – el número de puerto del receptor.
- 9 **TCP or UDP** – el protocolo de transmisión; se ajusta según la configuración del receptor.
- 10 **Primary channel Backup** – canal de respaldo para cuando falla el principal; rellénalo de la misma manera, se recomienda configurarlo.

Por último, en la página **Network settings**, en la pestaña **SIM1**, introduce los datos de la tarjeta (**SIM card PIN**, **APN**, **DNS 1, DNS 2**), si no lo has hecho ya en el apartado 2.2.

Con el protocolo **DC-09**, en la pestaña **Settings** introduce también el número de línea y de receptor (**Line No.**, **Receiver No.**, apartado 6.4). El GT y el GT+ solo transmiten a la CRA por conexión IP; no tienen canal de respaldo por SMS.

Al terminar los ajustes, pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB. Con esto el equipo está listo para la conexión. Con la conexión por línea telefónica, también en este caso hay que activar y configurar el marcador de la central de alarma; si no, la central no envía eventos (capítulo 4).

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.

3.1 Pasos de la instalación

1. Quita la tapa frontal (ver el apartado 2.1) y extrae la regleta de bornes.
2. Coloca la tarjeta nano-SIM en la ranura, si no lo has hecho ya en la puesta en marcha.
3. Saca la placa de circuito impreso de la base: abre el pestillo junto al conector de la antena y levanta la placa (ver la figura).

4. Fija la base con tornillos en el lugar elegido (en la figura, los orificios para los tornillos están marcados con un círculo).
5. Vuelve a colocar la placa de circuito impreso en la base y vuelve a enchufar la regleta de bornes.
6. Enrosca la antena móvil.
7. Vuelve a poner la tapa frontal.

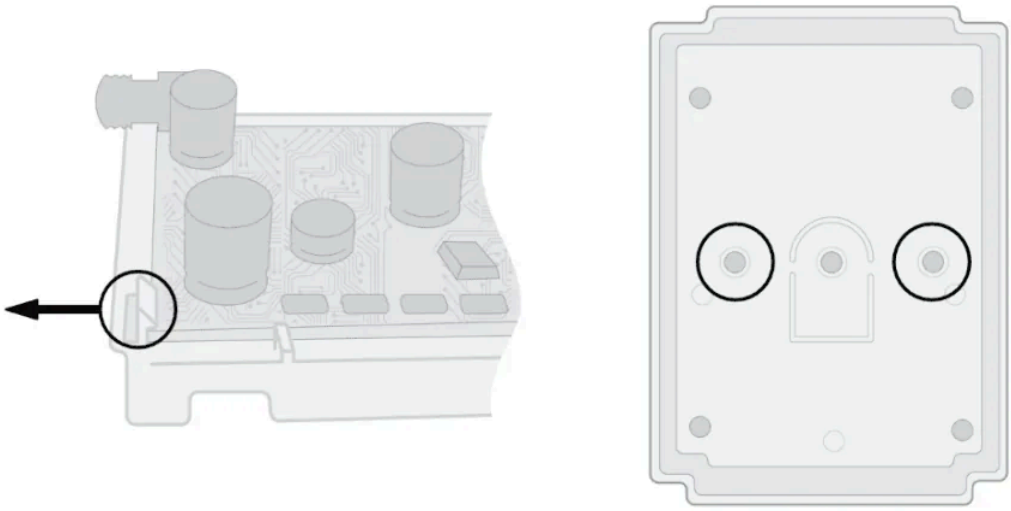


Figura 11. Cómo sacar la placa de circuito impreso de la base (izquierda: el pestillo y la dirección para sacarla) y los orificios para los tornillos de la base (derecha).

La tarjeta SIM debe estar activa y, para el uso por IP, debe tener funcionando la conexión de datos móviles. Si no quieres que TrikdisConfig pida el código PIN, pon la tarjeta en un teléfono móvil y desactiva allí la petición de PIN.

3.2 Ubicación y antena

- Coloca el comunicador en un lugar **seco y en interiores**, preferiblemente cerca de la caja de la central de alarma, para que el cableado sea corto.
- **Dentro de una caja metálica**, la señal móvil se debilita mucho. Si el comunicador va dentro de la caja metálica de la central, saca la antena fuera de la caja o usa una antena con cable más largo.
- Antes de la fijación definitiva, **comprueba el nivel de señal**: el número de destellos amarillos del LED NETWORK debe ser, en 4G, de al menos 3 (apartado 1.6). Si es menor, busca un lugar mejor o cambia a una antena más sensible que se pueda colocar más lejos.
- Mantén la antena y el comunicador alejados del transformador de la central y de los cables de red eléctrica.



A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna használata.

3.3 Conexión a la central de alarma

De los esquemas siguientes, sigue el que corresponda a tu central. En los esquemas, **+DC** y **–DC** son los bornes de alimentación del comunicador (GT: +12 VDC / −12 VDC; GT+: +12 / 24 VDC / −12 / 24 VDC), y **A RS485** / **B RS485**, los bornes A 485 / B 485. El comunicador se alimenta de la salida de alimentación auxiliar (AUX) de la central; así, en un corte de corriente, la batería de la central también alimenta el comunicador. En los esquemas aparece el GT+; la conexión del GT es la misma.

3.3.1 DSC – bus de datos (Keybus)

Conecta el Keybus de la central DSC al comunicador con cuatro hilos: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

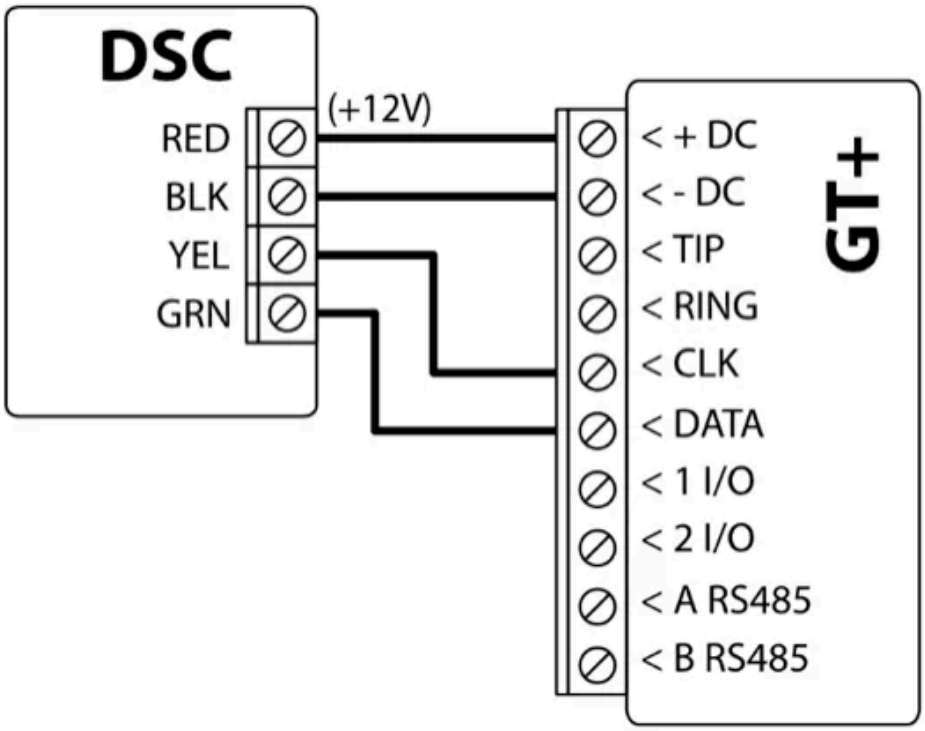


Figura 12. Conexión de la central DSC en el bus de datos (Keybus, «Keypad bus»): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

Conectado solo al Keybus, el comunicador recibe de la central el estado general de las zonas, pero no conoce el tipo de zona (incendio, intrusión, fuga de agua, etc.). Por eso transmite todas las alarmas **como alarma genérica, con el código Contact ID E130**, y algunas CRA lo tratan de otra manera que el tipo de zona que realmente se ha disparado. Si quieres enviar los eventos con los códigos Contact ID propios de la central (por ejemplo, alarma de incendio: E110), en el GT+ conecta también los bornes TIP/RING (apartado 3.3.2).

3.3.2 DSC – Keybus y TIP/RING (solo GT+)

El GT+ se puede conectar a la central DSC al bus de datos y a la salida de línea telefónica a la vez: además de los hilos del Keybus, conecta también los bornes **TIP** → **TIP** y **RING** → **RING** de la central con los del comunicador.

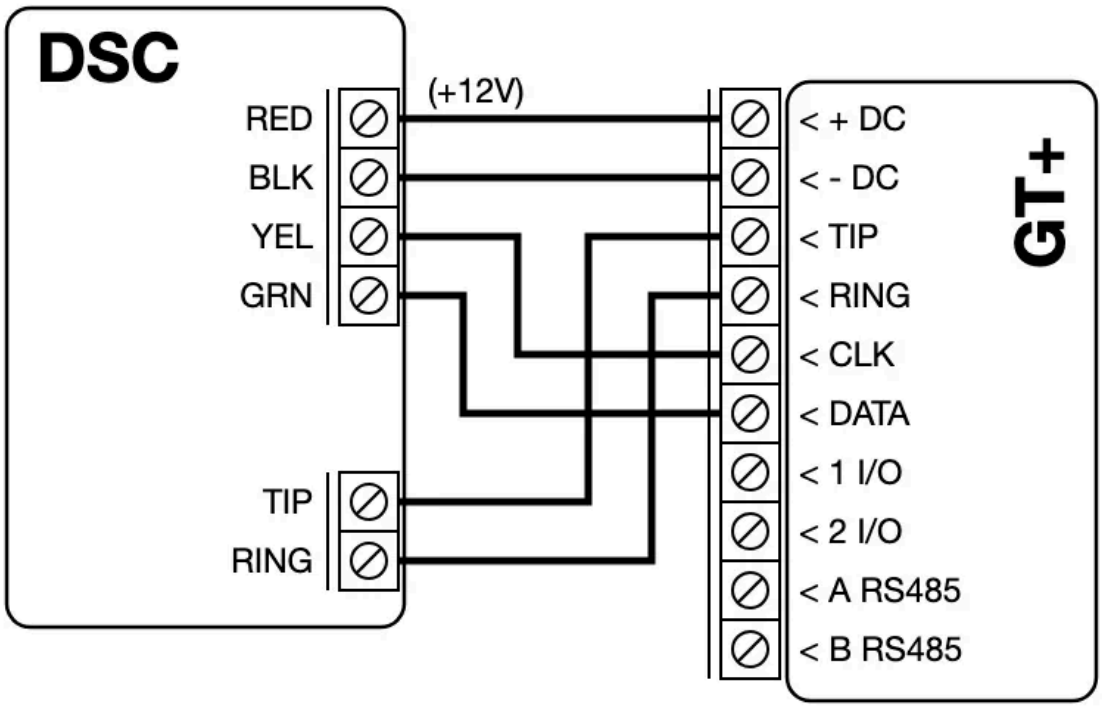


Figura 13. Conexión de la central DSC en el bus de datos («Keypad bus») y en los bornes TIP/RING a la vez (GT+): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA, y TIP → TIP, RING → RING.

En este caso, el Keybus sirve para el control y los estados (armado y desarmado a distancia, estado de particiones y zonas), y los eventos los envía el marcador telefónico de la central por los bornes TIP/RING, es decir, se envían con los códigos Contact ID propios de la central. Mientras la conexión TIP/RING funciona, el comunicador no vuelve a enviar los eventos que llegan del Keybus.

Para esta conexión, en la página **Panel settings** de TrikdisConfig configura lo siguiente:

1. **Communication protocol**: **AUTO**.
2. **Security panel model**: el modelo de la central DSC.
3. **Remote Arm/Disarm**: márcalo si los usuarios quieren controlar la central desde la aplicación Protegus 2.

También hay que programar el marcador telefónico de la central DSC para que envíe los eventos; esto se describe en el apartado 4.1.1.

3.3.3 Paradox – puerto serie

El comunicador se conecta al puerto serie de la central Paradox con el cable **EX-CRP2.4**, que se pide por separado: **rojo → +DC**, **negro → −DC**, **amarillo → CLK**, **verde → DATA**.

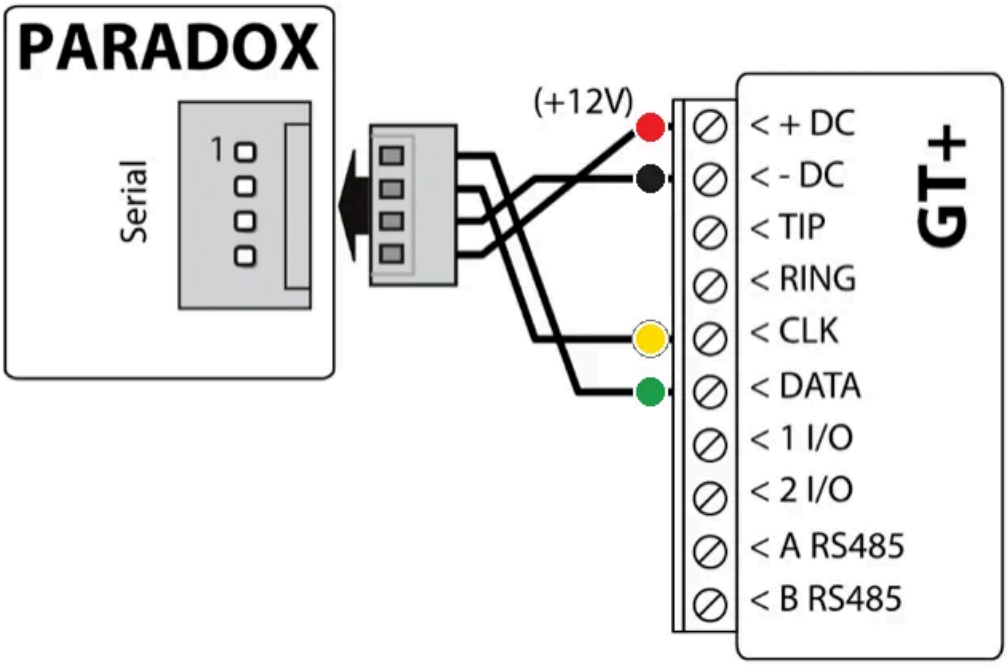


Figura 14. Conexión de la central Paradox en el puerto serie con el cable EX-CRP2.4 (se pide por separado; «Use the EX-CRP2.4 cable (ordered separately)»): rojo → +DC, negro → −DC, amarillo → CLK, verde → DATA.

- hilo rojo («R - red»)
- hilo negro («B - black»)
- hilo amarillo («Y - yellow»)
- hilo verde («G - green»)

En las centrales Paradox más nuevas (SP+, MG+, EVOHD+) el puerto serie puede venir bloqueado de fábrica; el desbloqueo se explica en el apartado 4.1.2. En las centrales Spectra SP / SP+ y Magellan MG / MG+, en lugar del puerto serie también se puede usar la conexión del apartado siguiente.

3.3.4 Paradox SP/MG – Keybus y TIP/RING

Las centrales Paradox Spectra SP, SP+ y Magellan MG, MG+ también se pueden conectar, en lugar del puerto serie, a su bus de datos (Keybus) y a sus bornes TIP/RING a la vez: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK**, y **TIP** → **TIP**, **RING** → **RING**. Esta conexión usa el Keybus de la central en lugar del puerto serie, por eso no necesita el desbloqueo de pago del puerto serie de Paradox.

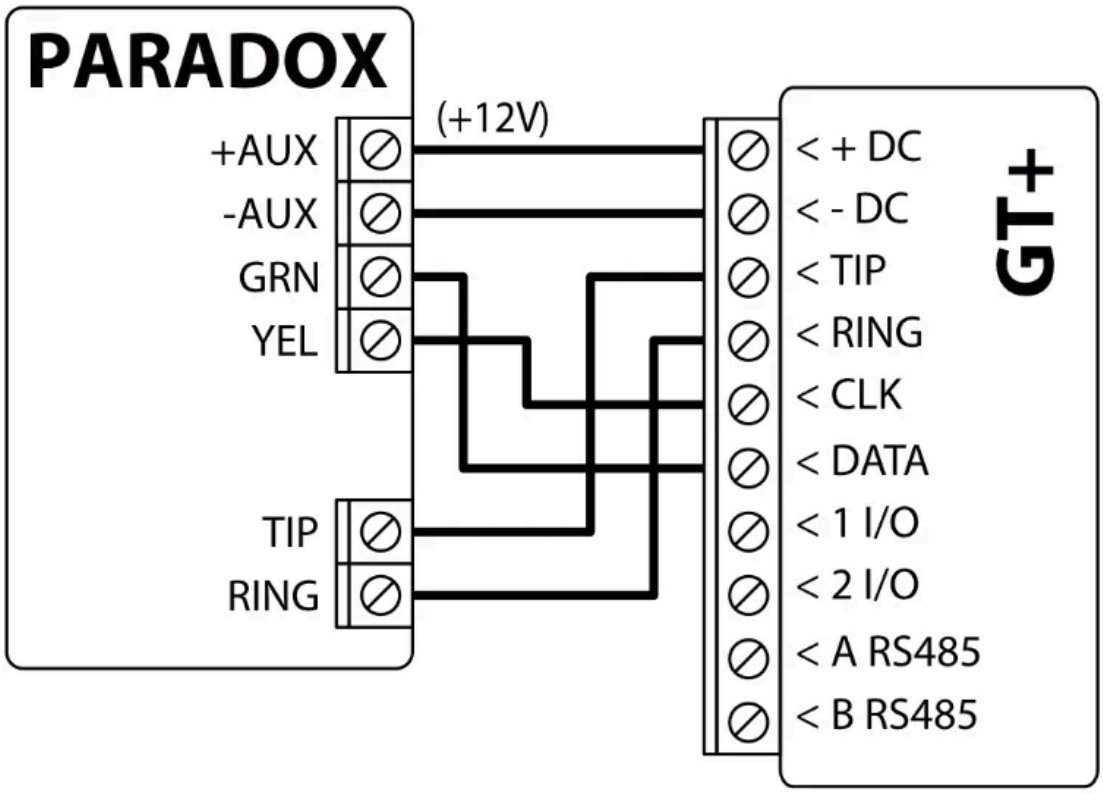


Figura 15. Conexión de la central Paradox SP / SP+ / MG / MG+ en el Keybus (bus de datos, «Keypad bus») y en los bornes TIP/RING a la vez: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

Para esta conexión, el firmware del comunicador debe ser como mínimo el **1.21** (la actualización se describe en el capítulo 9).

Para esta conexión, en la página **Panel settings** de TrikdisConfig configura lo siguiente:

1. **Communication protocol**: **AUTO** (GT: **Dual tone**).
2. **Security panel model**: **7. Paradox SP+/MG+ series KeyBus**.
3. **Remote Arm/Disarm**: márcalo si los usuarios quieren controlar la central desde la aplicación Protegus 2 con su propio código de teclado.
4. **Security panel PC download password**: para el control directo, introduce la contraseña de PC configurada en la central; las dos deben coincidir.



Figura 16. TrikdisConfig – Panel settings para la conexión Keybus + TIP/RING: Communication protocol AUTO, Security panel model 7. Paradox SP+/MG+ series KeyBus, Remote Arm/Disarm marcado, PC download password introducida.

También hay que programar la central Paradox para que envíe los eventos a la CRA y se pueda controlar desde Protegus 2; esto se describe en el apartado 4.1.2.

3.3.5 UTC Interlogix (Caddx) – bus de datos

Conecta el bus de datos de la central Caddx NetworX al comunicador con tres hilos: **POS** → **+DC**, **COM** → **−DC**, **DATA** → **DATA**. Los bornes TIP, RING y CLK no hacen falta.

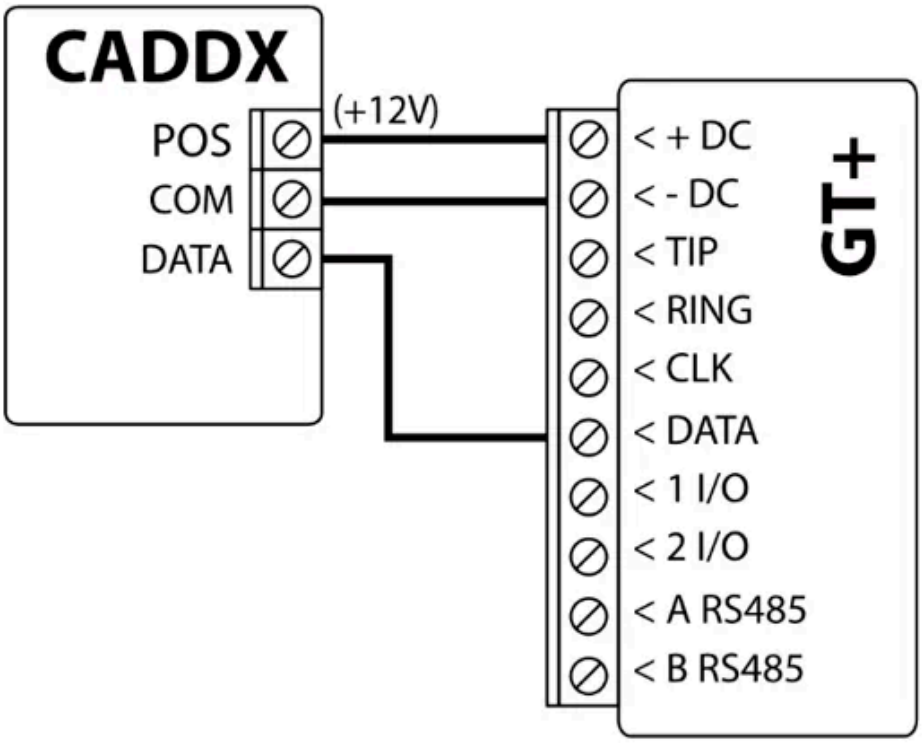


Figura 17. Conexión de la central UTC Interlogix (Caddx) NetworX en el bus de datos («Keypad bus»): POS → +DC, COM → −DC, DATA → DATA.

3.3.6 Texecom – puerto serie

El comunicador se conecta al puerto serie de la central Texecom Premier / Premier Elite con el cable **EX-CRP4**, que se pide por separado: **rojo** → **+DC**, **negro** → **−DC**, **azul** → **CLK**, **blanco** → **DATA**.

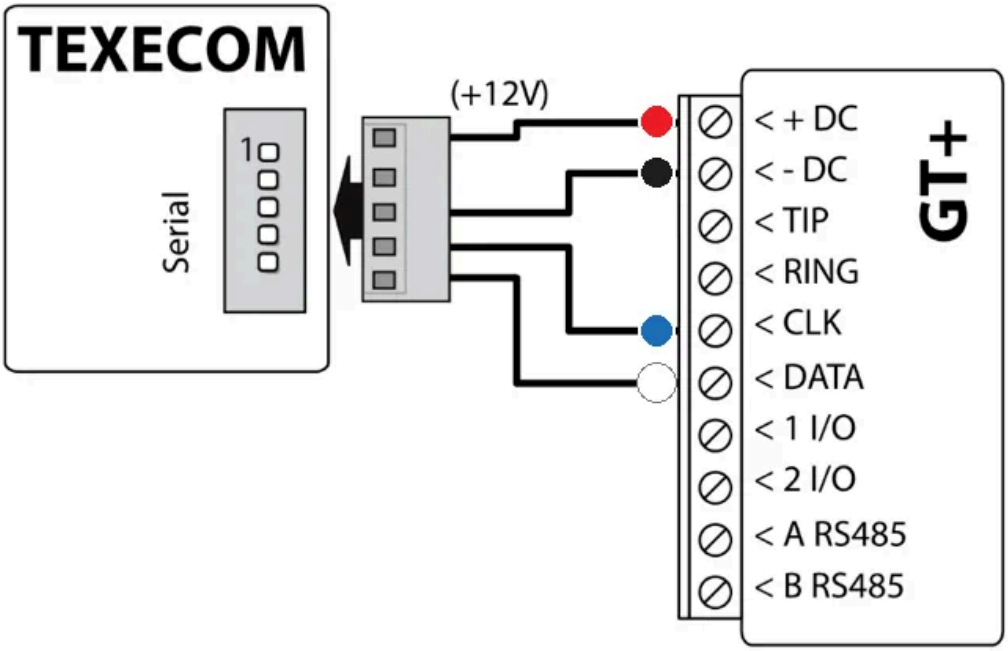


Figura 18. Conexión de la central Texecom en el puerto serie con el cable EX-CRP4 (se pide por separado; «Use the EX-CRP4 cable (ordered separately)»): rojo → +DC, negro → −DC, azul → CLK, blanco → DATA.

- hilo rojo («R - red»)
- hilo negro («B - black»)
- hilo azul («BL - blue»)
- hilo blanco («W - white»)

3.3.7 InnerRange Inception

El comunicador se alimenta de la salida de alimentación de la central Inception (**VOUT + → +DC**, **VOUT 0V → −DC**), y la conexión de datos llega del puerto USB de la central, con el cable **993030USB** de Inner Range: **negro → 0V / −DC**, **verde → CLK**, **blanco → DATA**.

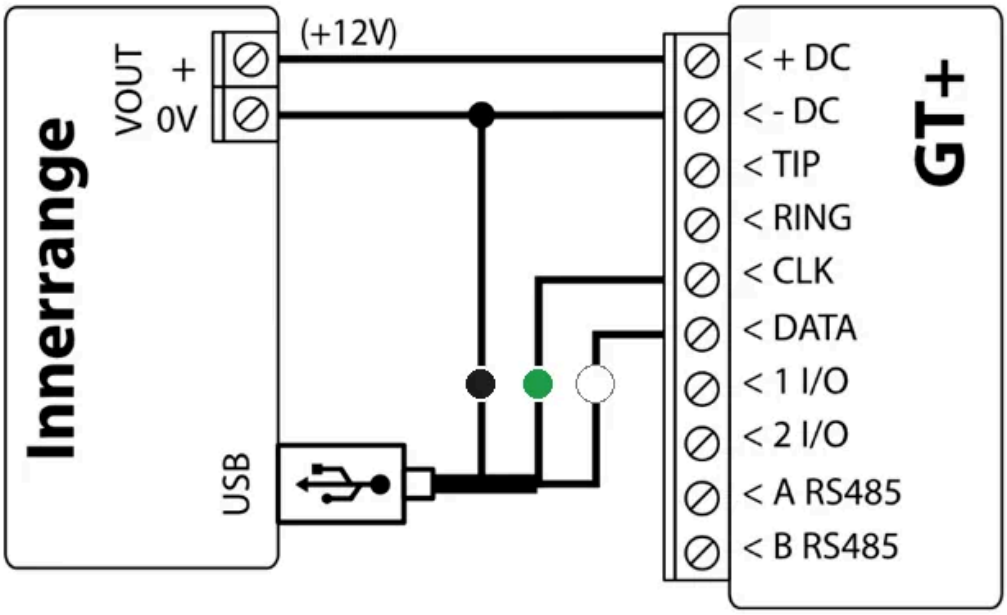


Figura 19. Conexión de la InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; desde el puerto USB, con el cable 993030USB («Cable, Inner Range part number 993030USB»), negro → −DC, verde → CLK, blanco → DATA.

- hilo negro («Black wire»)
- hilo verde («Green wire»)
- hilo blanco («White wire»)

3.3.8 InnerRange Integriti

El comunicador se conecta al puerto serie **Port 0** de la central Integriti con el cable **INTG-996795** de Inner Range: **+DET (+13 V) → +DC**, **GND (5) → −DC**, **Rx (3) → CLK**, **Tx (2) → DATA**.

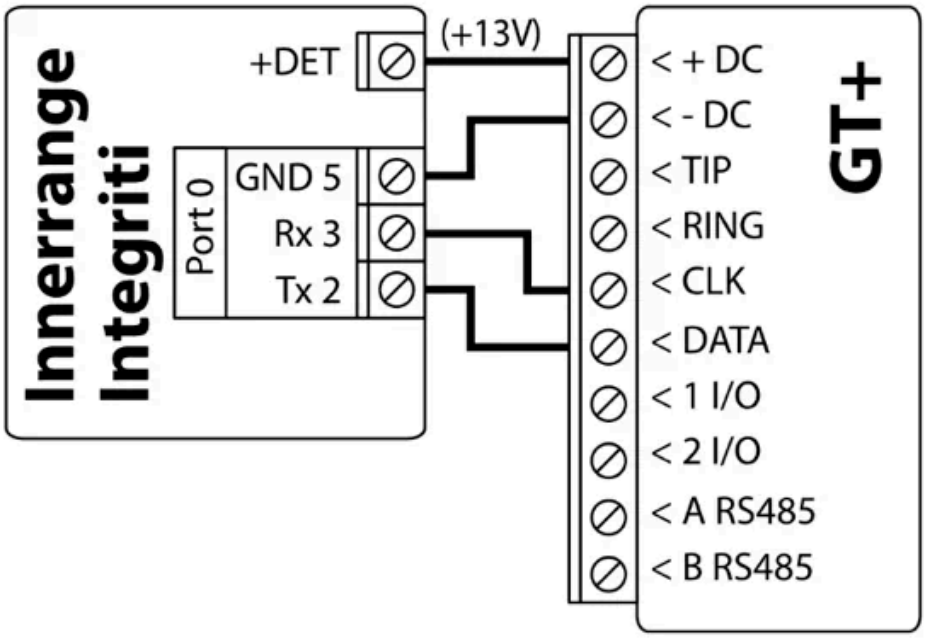


Figura 20. Conexión de la InnerRange Integriti al Port 0 con el cable INTG-996795 («Cable, Inner Range part number INTG-996795»): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.9 Honeywell Vista – bus de datos

Conecta el bus de teclados de la central Honeywell Ademco Vista-15, Vista-20 y Vista-48 desde los bornes de la central al comunicador: **5** → **+DC** (+12 V), **4** → **–DC**, **7** → **CLK**, **6** → **DATA**.

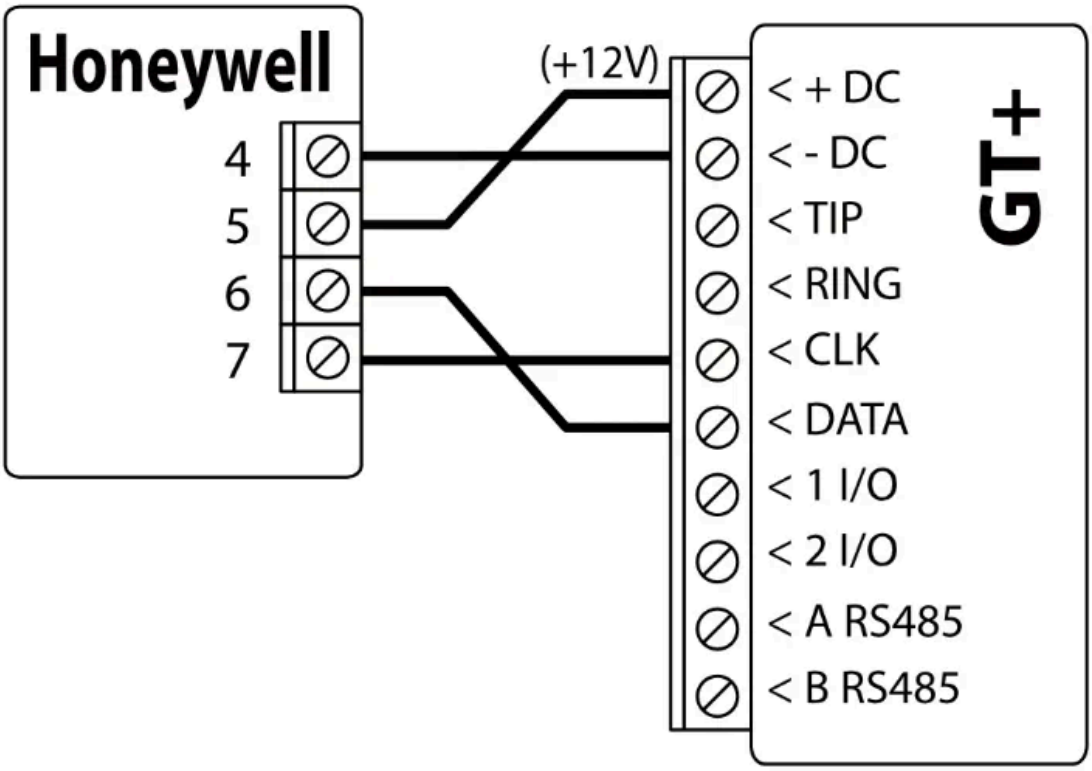


Figura 21. Conexión de la central Honeywell Vista-15 / -20 / -48 en el bus de datos («Keypad bus»): borne 5 → +DC, 4 → –DC, 7 → CLK, 6 → DATA.

3.3.10 Cualquier central – TIP/RING

Cualquier otra central se puede conectar a través de su marcador telefónico: la alimentación, desde la salida de alimentación auxiliar de la central (**+AUX** → **+DC**, **–AUX** → **–DC**), y la salida de línea telefónica, a los bornes **TIP** y **RING** del comunicador (**TIP** → **TIP**, **RING** → **RING**). Hay que configurar el marcador de la central (apartado 4.2).

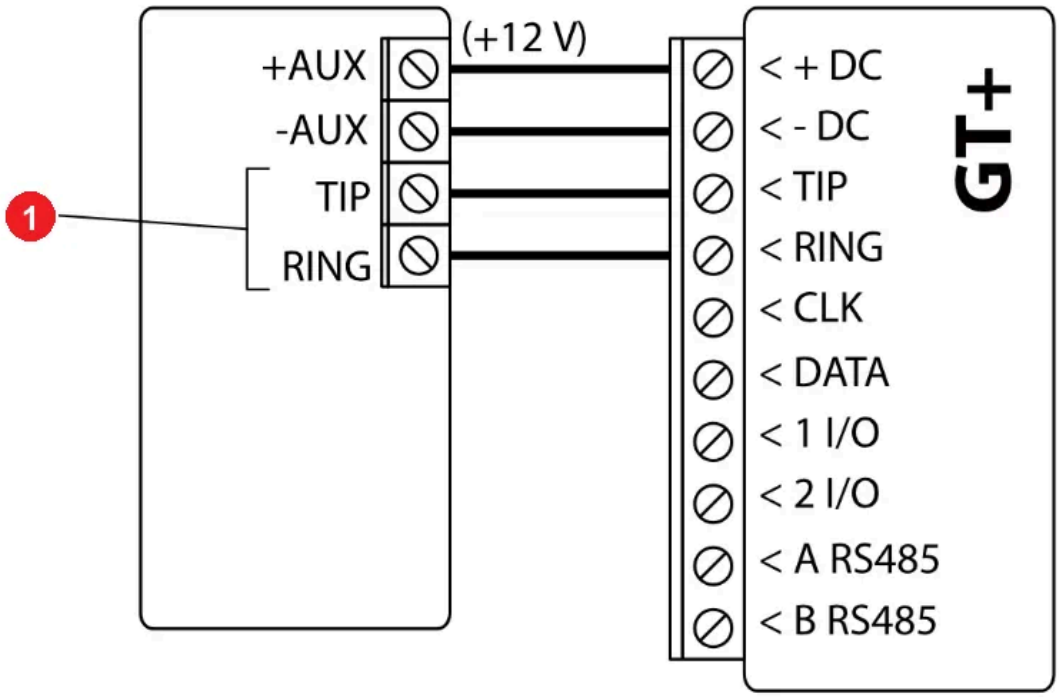


Figura 22. Conexión al marcador telefónico de la central («Control panel»): +AUX → +DC, −AUX → −DC, TIP → TIP, RING → RING.

- 1 bornes del marcador telefónico de la central («Telephone line communicator terminals»)

3.4 Conexión de una zona de llave

Si quieres armar y desarmar la central desde la aplicación Protegus 2 de manera que la salida (PGM) del comunicador accione la **zona de llave** de la central, sigue esta conexión. Los dos bornes de E/S de doble función del comunicador se pueden configurar como salida (OUT, PGM), así que las dos salidas pueden controlar dos particiones del sistema: conecta la zona de llave de la partición 1 al borne **1 I/O**, y la de la partición 2, al borne **2 I/O**. Con esta conexión, en la página **Panel settings** de TrikdisConfig desmarca **Remote Arm/Disarm**, configura los bornes en la página **IN/OUT** con la función **OUT** (apartado 6.7) y, en la aplicación Protegus 2, asigna las salidas a las particiones según el apartado 5.2.

Con la conexión al bus de datos o serie, la conexión de datos entre la central y el comunicador se mantiene (el comunicador lee los eventos del bus), y el armado y desarmado se hacen a través de la zona de llave:

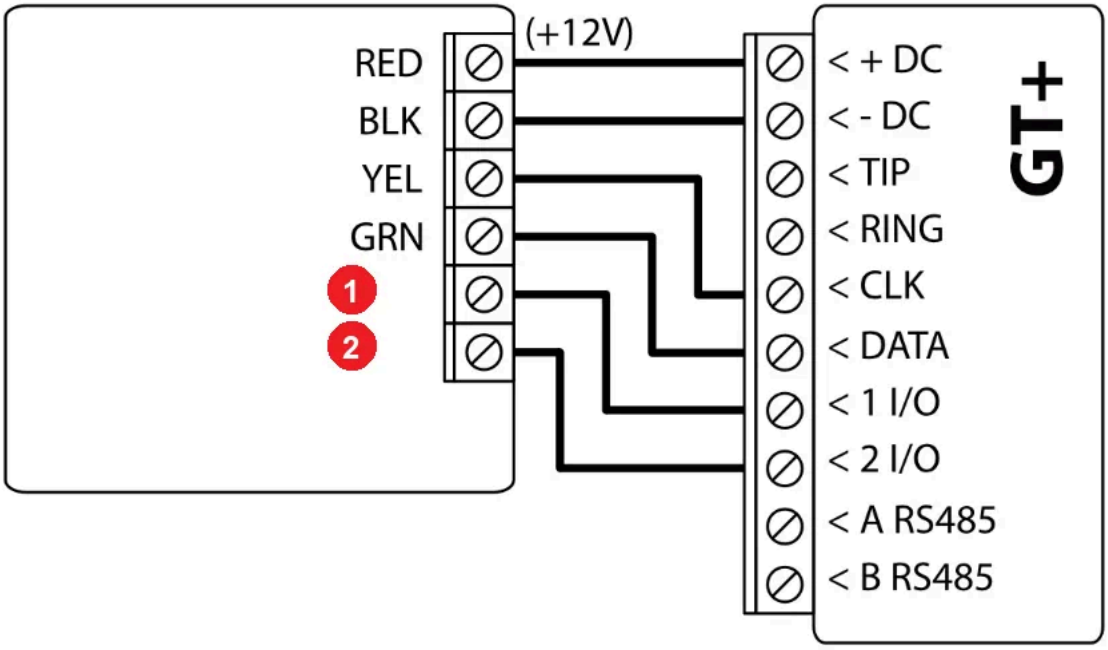


Figura 23. Armado y desarmado con zona de llave («Zones (keyswitch)»), con conexión al bus de datos o serie («Keypad bus or serial»): borne RED de la central de alarma («Control panel terminals») → +DC, BLK → −DC, YEL → CLK, GRN → DATA; zona de la partición 1 → 1 I/O, la de la partición 2 → 2 I/O.

- 1 zona de llave de la partición 1 («1-st Area»)
- 2 zona de llave de la partición 2 («2-nd Area»)

Con la conexión por línea telefónica (TIP/RING), la central envía los eventos por su marcador, y el armado y desarmado se hacen igualmente a través de la zona de llave:

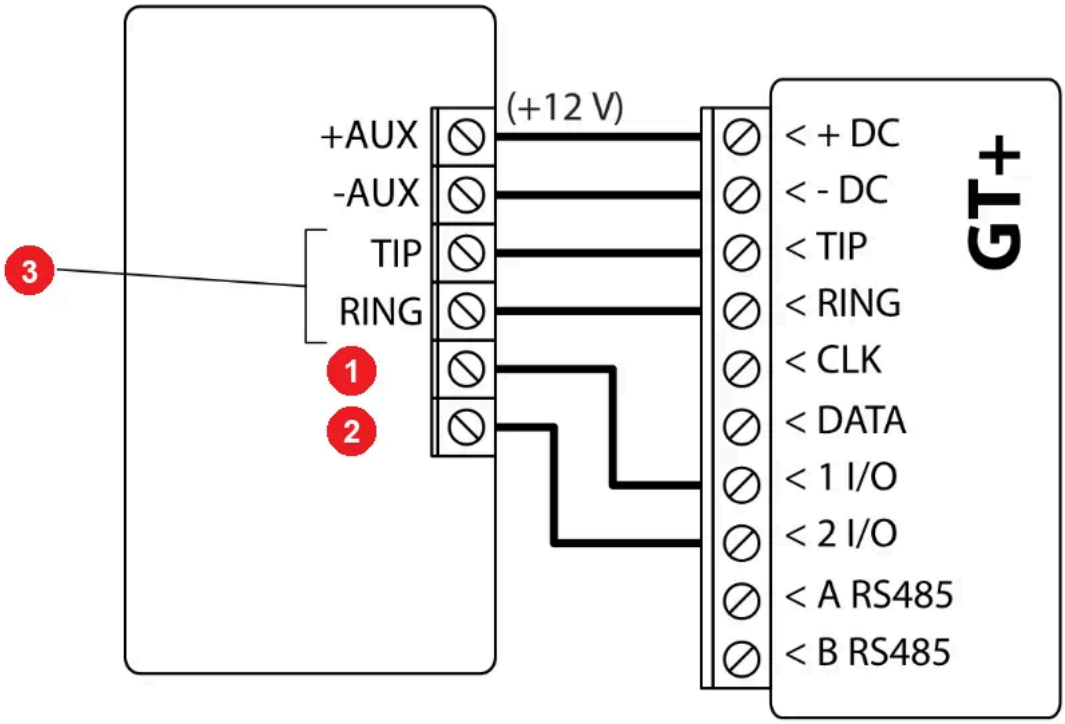


Figura 24. Armado y desarmado con zona de llave («Zone (keyswitch)»), con conexión por línea telefónica: borne +AUX de la central de alarma («Control panel») → +DC, −AUX → −DC, TIP → TIP, RING → RING; zona de la partición 1 → 1 I/O, la de la partición 2 → 2 I/O.

- 1 zona de llave de la partición 1 («1-st Area»)
- 2 zona de llave de la partición 2 («2-nd Area»)
- 3 bornes del marcador telefónico de la central («Telephone line communicator terminals»)

La zona de llave puede ser de impulso o de dos posiciones; en la aplicación Protegus 2 hay que configurar el mismo modo (apartado 5.2). Los detalles y las trampas del armado con zona de llave se explican en un artículo aparte: Armado a distancia con zona de llave desde la aplicación Protegus 2.

3.5 Conexión de entradas

Los dos bornes de E/S de doble función del comunicador también se pueden usar como entrada (IN) para recibir otros detectores (p. ej., interruptor de sabotaje, botón de pánico), independientemente de la central de alarma. A la entrada se puede conectar un circuito NO, NC, NO/EOL, NC/EOL, NO/DEOL o NC/DEOL; el ajuste de fábrica en los dos bornes es entrada, NO. El tipo de entrada se configura en la página **IN/OUT** de TrikdisConfig, en el campo **Type**. La entrada se conecta entre el borne I/O elegido y el borne **−DC** (COM), según el tipo elegido.

Las entradas admiten los siguientes tipos de circuito: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. La resistencia de fin de línea es de **2,2 kΩ**. Con fin de línea simple (EOL), tanto el cortocircuito como el corte cuentan como alarma; el fin de línea doble (DEOL), con dos resistencias, distingue por separado la alarma y el sabotaje (cortocircuito o corte). El ajuste de fábrica es NO (normalmente abierto); el tipo de entrada lo configuras en la página **IN/OUT** de TrikdisConfig, según el cableado.

Tipo	Estado de reposo	Alarma	Sabotaje
NC	cerrado	abierto	–
NO	abierto	cerrado	–
NC/EOL	2,2 kΩ	corte o cortocircuito	–

Tipo	Estado de reposo	Alarma	Sabotaje
NO/EOL	2,2 kΩ	cortocircuito o corte	–
NC/DEOL	2,2 kΩ	3,3–5,5 kΩ (2 × 2,2 kΩ)	corte o cortocircuito
NO/DEOL	3,3–5,5 kΩ (2 × 2,2 kΩ)	2,2 kΩ	corte o cortocircuito

Cuando se activa la entrada, el comunicador envía un evento propio a la CRA y a Protegus 2; el código Contact ID del evento y sus números de partición y de zona los puedes indicar en la página **IN/OUT**.

Conexión de los circuitos de entrada entre el punto COM y el punto INx: NO, NC, NC/EOL, NO/EOL y, con detección de sabotaje, NO/DEOL y NC/DEOL, con resistencias de fin de línea de 2,2 kΩ; cada estado (cortocircuito, circuito abierto, 2,2 kΩ, 3,3–5,5 kΩ) se explica en la tabla del apartado 3.5.

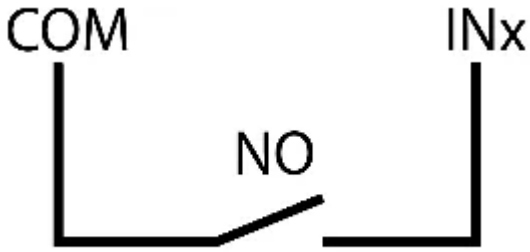


Figura 25. NO – circuito abierto en reposo: cerrado – alarma; abierto – estado de reposo.

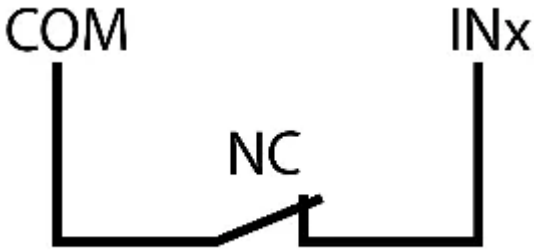


Figura 26. NC – circuito cerrado en reposo: abierto – alarma; cerrado – estado de reposo.

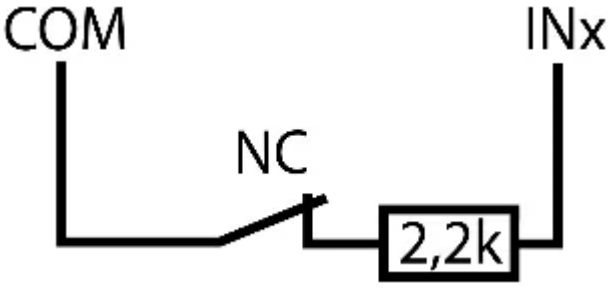


Figura 27. NC/EOL – circuito cerrado en reposo con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto – alarma; 2,2 kΩ – estado de reposo.

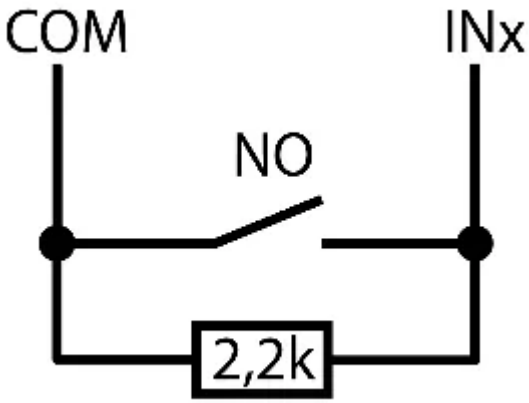


Figura 28. NO/EOL – circuito abierto en reposo con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto – alarma; 2,2 kΩ – estado de reposo.

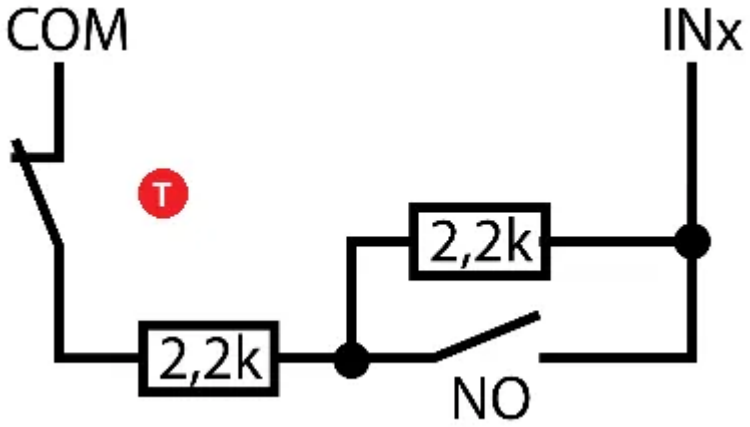


Figura 29. NO/DEOL – circuito abierto en reposo con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto – sabotaje; 2,2 kΩ – alarma; 3,3–5,5 kΩ – estado de reposo.

- T contacto de sabotaje («Tamper»), indica la apertura de la carcasa del detector

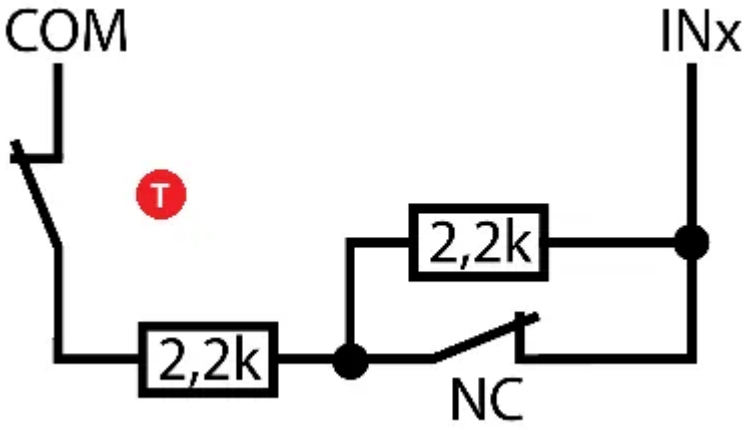


Figura 30. NC/DEOL – circuito cerrado en reposo con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto – sabotaje; 2,2 kΩ – estado de reposo; 3,3–5,5 kΩ – alarma.

- T contacto de sabotaje («Tamper»), indica la apertura de la carcasa del detector

Si necesitas más entradas o salidas, conecta al comunicador un expansor Trikdis **iO-8** (apartado 3.7); su conexión también se describe en el manual del iO-8.

3.6 Conexión de una salida con relé

Como salida, los bornes I/O son salidas de colector abierto (OC): en estado activo llevan la carga conectada al negativo, con 0,15 A como máximo y hasta 30 V DC. Con los contactos de un relé puedes encender y apagar distintos aparatos eléctricos: un extremo de la bobina del relé va a **+DC** y el otro al borne **x I/O**, y la carga la conmutan los contactos del relé (NC, C, NO). El borne I/O usado hay que configurarlo como salida (**OUT**) en la página **IN/OUT** de TrikdisConfig.

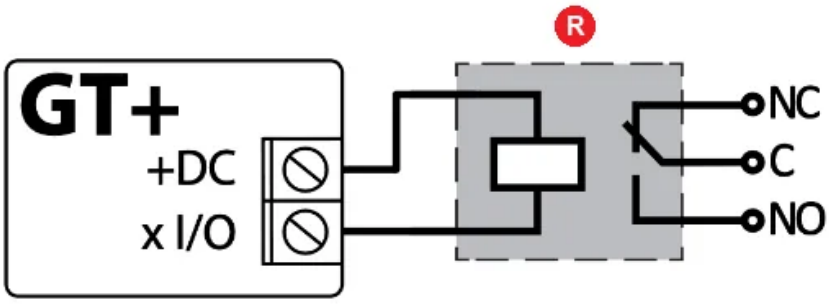


Figura 31. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne x I/O, y los contactos (NC, C, NO) conmutan la carga.

- R relé («Relay»)

Las salidas las puedes accionar desde la aplicación Protegus 2 o con un comando SMS (capítulo 5).

3.7 Conexión del expansor iO-8

Si necesitas más entradas o salidas, al bus RS485 del comunicador se pueden conectar hasta cuatro expansores **iO-8**; cada uno añade 8 E/S de doble función más. Conecta los bornes **A 485** y **B 485** con los bornes **A (RS485)** y **B (RS485)** del módulo; tanto el comunicador como el expansor se alimentan de la salida de alimentación auxiliar de la central (**+AUX** → **+DC**, **–AUX** → **–DC** en los dos equipos). El expansor hay que añadirlo y configurarlo en la página **RS485 modules** de TrikdisConfig (apartado 6.8).

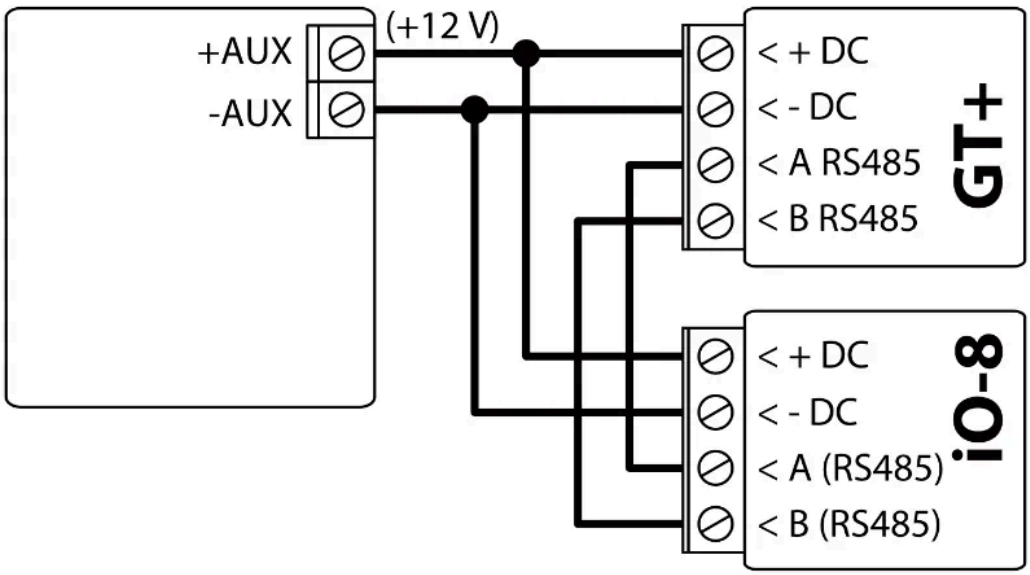


Figura 32. Conexión del expansor iO-8 al bus RS485 del comunicador; la alimentación, desde la salida AUX de la central de alarma («Control panel»), para los dos equipos.

3.8 Encendido y primera comprobación

A TRIKDIS átjelző elindítása

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

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

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

Después de la conexión, al encender la alimentación de la central de alarma también arranca el comunicador. En la tapa frontal debes ver esto:

- **POWER** encendido en verde: la alimentación es correcta;
- **NETWORK** encendido en verde y parpadeando en amarillo: se ha conectado a la red; el número de destellos amarillos es el nivel de señal: en 4G, 3 destellos es lo adecuado; si cuentas menos, la señal es débil: busca otro lugar para el comunicador o usa una antena más sensible (apartado 3.2);
- **TROUBLE** apagado.

Si TROUBLE parpadea, el número de destellos indica la causa (apartado 1.6); cualquier otra indicación LED distinta de esta también indica algún fallo, y su causa la encuentras con las tablas del apartado 1.6. Si no se enciende ningún LED, comprueba la alimentación y la conexión.

4. Programación de la central de alarma

La configuración de la central depende de cómo la hayas conectado: al bus de datos o al puerto serie (apartado 4.1), o a su marcador telefónico, en los bornes TIP/RING (apartado 4.2). En el GT+, para la conexión DSC Keybus + TIP/RING hacen falta las dos cosas: los ajustes de la conexión Keybus y la programación del marcador de la central (apartado 4.1.1).

4.1 Conexión al bus de datos o serie

Aquí describimos cómo configurar la central para que el comunicador lea sus eventos y pueda controlarla a distancia. Para el control a distancia, en la página **Panel settings** de TrikdisConfig debe estar marcada la opción **Remote Arm/Disarm** (apartado 2.2).

4.1.1 DSC

Las centrales **DSC PowerSeries** (la lista de modelos compatibles está en el apartado 1.2) no requieren ningún ajuste especial: el comunicador conectado al Keybus lee los eventos de inmediato y, tras marcar **Remote Arm/Disarm**, el usuario arma y desarma desde la aplicación con su propio código de teclado. Los detalles del control directo –estados de zona, anulación de zonas, detección automática de las particiones– se explican en un artículo aparte: Control directo para centrales de alarma DSC PowerSeries.

El comunicador no funciona con las centrales **DSC PowerSeries NEO**: el fabricante no permite dispositivos externos en el bus de la NEO. Para la NEO es adecuado un comunicador de línea telefónica (TIP/RING) – consulta DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones.

GT+, conexión Keybus y TIP/RING (apartado 3.3.2): hay que programar el marcador telefónico de la central para que envíe los eventos. La tabla siguiente se refiere a la central DSC PowerSeries PC1616 (PC1832, PC1864). En el teclado conectado a la central, entra en la programación: **[*][8][código de instalador]** y, después, introduce el número de la sección.

Sección	Valor
[301] Primer número de teléfono	Cualquier número de más de cuatro dígitos, **sin D** al principio (por ejemplo, `5555555`). La D significa esperar el tono de línea; sin ella, la central marca más rápido. El comunicador acepta todas las llamadas
[310] Identificador de abonado del sistema	El identificador de abonado de 4 dígitos, seguido de `FF` (por ejemplo, `1234FF`). En lugar del dígito 0, usa la `A` hexadecimal
[311] Identificador de abonado de la partición 1	El identificador de abonado de 4 dígitos; en lugar del 0, la `A` hexadecimal
[350] Formato del comunicador	`03` (Contact ID) para el número de teléfono 1
[351]–[376] Direcciones de llamada	Activa para el número de teléfono 1 los grupos de eventos necesarios: Alarm/Restore, Opening/Closing, Tamper Alarm/Restore, System Maintenance, Test Transmissions. Comprueba aparte el grupo Opening/Closing: en algunas centrales DSC viene desactivado de fábrica
[380] Opción 1 del comunicador	Opción 1 **ON** (comunicador activado); opción 3 **OFF** (marcación DTMF)
[381] Opción 2 del comunicador	Opción 7 **OFF** (la central genera automáticamente los códigos de reporte Contact ID)
[320]–[349] Códigos de reporte	Para los eventos que se van a transmitir, cualquier valor, siempre que no sea `00`
[015] Opción 3 del sistema	Opción 7 **OFF** (supervisión de línea telefónica, TLM, desactivada)

Desactiva la supervisión de línea telefónica (TLM): si se queda activada, la central puede indicar una avería de línea telefónica. El retardo de la avería TLM se configura en la sección **[377]**.

Los números de sección anteriores se refieren a las centrales PC1616, PC1832 y PC1864 (manual de instalación v4.x). En otros modelos DSC los números de sección pueden variar; consulta el manual de programación de la central.

4.1.2 Paradox

Las centrales **Paradox** solo hay que programarlas para el control directo; para leer los eventos no hace falta configurar nada. El firmware de la central debe ser como mínimo **V.4**.

En las centrales Paradox más nuevas (por ejemplo, las series SP+, MG+ y EVOHD+), el puerto serie puede venir **bloqueado de fábrica**: el comunicador no recibe datos hasta que desbloquees el puerto. Cómo desbloquearlo: Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox.

Para el control hay que configurar la **contraseña de PC** (PC password) de la central, y escribir la misma también en el campo **System settings** → **Security panel PC download password** de TrikdisConfig: las dos deben coincidir.

1. Entra en la programación de instalador de la central desde el teclado.
2. Abre la sección de la contraseña de PC: en las series **MAGELLAN y SPECTRA**, la sección **911**; en la serie **DIGIPLEX EVO**, la sección **3012**.
3. Introduce una contraseña de **4 caracteres**. La contraseña no puede ser 0000 y **no debe empezar por cero**.
4. Sal de la programación y **reinicia la central**: el cambio de la contraseña de PC entra en vigor tras el reinicio. Después, escribe la misma contraseña en TrikdisConfig.

Errores típicos y su solución

- El **código de teclado asignado a la partición no puede ser el código maestro**: dale al usuario otro código y, con él, el armado / desarmado desde Protegus 2 funcionará.
- **Después de cualquier cambio de códigos de teclado, reinicia el comunicador** (quitando la alimentación o con el comando SMS `RESET`): lee los códigos al arrancar y no ve los cambios posteriores.

En los comunicadores GT y GT+, el campo **Security panel PC download password** está en la página **Panel settings** de TrikdisConfig, en el grupo **Serial bus** (apartados 2.2 y 6.3).

Conexión Keybus y TIP/RING (SP / SP+ / MG / MG+, apartado 3.3.4): además, hay que programar la central para que envíe los eventos a la CRA y se pueda controlar desde Protegus 2:

Sección	Valor	Sección	Valor
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

4.1.3 Texecom

Las centrales **Texecom Premier / Premier Elite** hay que programarlas tanto para leer los eventos como para el control: hay que configurar la contraseña de 4 caracteres de la central llamada **UDL passcode**, y escribir la misma en el campo **System settings** → **Security panel PC download password** de TrikdisConfig: las dos deben coincidir.

Con el software Wintex de Texecom: el UDL passcode está en la pestaña **Options** de la ventana **Communication Options**.

Desde el teclado:

1. Introduce el código de instalador de 4 dígitos y pulsa la tecla **[Menu]** para entrar en el menú de programación.
2. Justo después, pulsa la tecla **[9]**.
3. Pulsa **[7][6]**, luego la tecla **[2]**, e introduce el UDL passcode de 4 dígitos.
4. Pulsa la tecla **[Yes]** y luego sal de la programación con la tecla **[Menu]**.

En los comunicadores GT y GT+, el campo **Security panel PC download password** está en la página **Panel settings** de TrikdisConfig, en el grupo **Serial bus**; el UDL passcode debe coincidir con él.

4.1.4 UTC Interlogix (Caddx)

El firmware de la central **UTC Interlogix (Caddx) NetworX** debe ser como mínimo **V2**. En el teclado de la central hay que configurar lo siguiente:

1. Pulsa las teclas **[*][8]** e introduce el código de instalador (de fábrica **9713**).
2. Introduce el **número de dispositivo** asignado al comunicador (device address; de fábrica **0**).
3. Programa una tras otra las filas de la tabla siguiente: introduce la posición (location), el número de segmento y luego el ajuste. Con la tecla **[*]** puedes volver al campo anterior. `12345678` significa que los ocho interruptores del segmento están activados (en la pantalla se ven todas las cifras).

Posición (location)	Segmento	Ajuste
23	3	12345678
37 (no imprescindible)	3	12345678
37 (no imprescindible)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. Cuando hayas programado todas las filas, pulsa dos veces la tecla **[Exit]** para salir de la programación.

4.1.5 InnerRange

El firmware de la central **InnerRange Inception** debe ser como mínimo **2.3.0.3507-r0**, y la central necesita conexión a Internet. La configuración se hace en la interfaz web de la central:

1. Abre en el navegador la dirección `https://skytunnel.com.au/inception/NUMERO_DE_SERIE`, donde NUMERO_DE_SERIE es el número de serie que figura en la caja de la central. Entra con la cuenta de instalador.
2. Abre la página **Configuration** → **General** → **Alarm Reporting**.
3. En el grupo **3rd Party Device Configuration**: - marca la opción **Enable 3rd Party Device Reporting**; - en el campo **3rd Party Device Type**, elige el valor **Trikdis**; - en el campo **Serial Port**, elige el valor **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Guarda los ajustes y sal de la interfaz.

El firmware de la central **InnerRange Integriti** debe ser como mínimo **19.1.0.36608**, y su software de programación (Integriti Professional), como mínimo **19.1.0.15396**. La configuración se hace en el software de programación de la central:

1. En el puerto serie (**TTL Port-0**) al que está conectado el comunicador, elige el protocolo de comunicación **Trikdis**.
2. El formato de datos debe ser **Contact ID**.
3. Ajuste del puerto: **19200, 8, N, 1**.
4. Guarda los ajustes y sal del programa.

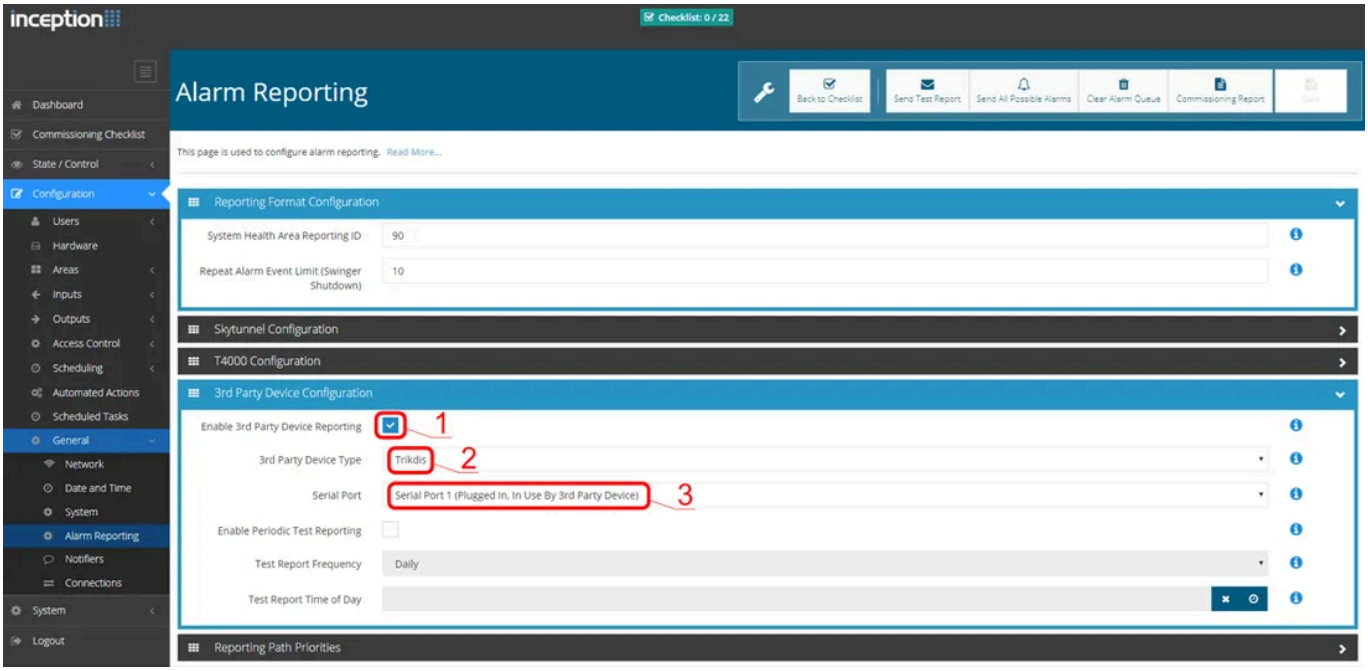


Figura 33. InnerRange Inception – Configuration → General → Alarm Reporting, grupo 3rd Party Device Configuration: Enable 3rd Party Device Reporting marcado, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

El firmware de las centrales **Honeywell Ademco Vista-20** y **Vista-48** debe ser como mínimo **V5.3**. La configuración se hace en el teclado de la central.

Entrada en la programación – de dos maneras:

- introduce el código de instalador (de fábrica **4112**) y luego las teclas **[8][0][0]**; o
- da alimentación a la central y, **en menos de 50 segundos**, pulsa a la vez las teclas **[*]** y **[#]** (esto solo funciona si antes se salió de la programación con las teclas [*][9][8]).

Ajustes:

1. Activa el envío de eventos Contact ID en la salida de radio de largo alcance (LRR): pulsa las teclas **[*][2][9][1][#]**.
2. Para el control remoto, habilita el uso de la **2.ª dirección AUI** (2nd AUI address): pulsa las teclas **[*][1][8][9][1][1][#]**.

Salida de la programación: pulsa las teclas **[*][9][9]**.

4.2 Conexión por línea telefónica (TIP/RING)

Para que la central de alarma envíe los eventos por su salida de línea telefónica, hay que activar y configurar el marcador de la central. Las direcciones de programa exactas las encontrarás en el manual de instalación de la central; lo esencial de la configuración es igual en todos los fabricantes:

1. **Activa el comunicador de línea telefónica (PSTN)** en la central.
2. **Como número de teléfono del receptor de la CRA, indica** `1234`, tanto si el comunicador se conecta a los bornes RING/TIP de la central como a la línea telefónica. Con otro número puede ocurrir que la central marque, pero el comunicador no reciba los eventos: también en una central DSC PowerSeries NEO la transmisión solo empezó a funcionar tras cambiar el número a `1234`.
3. **Modo de marcación:** DTMF (tonos), no por impulsos.

4. **Protocolo:** Contact ID.

Si quieres armar y desarmar la central a distancia con la salida del comunicador, la zona conectada a la salida debe configurarse en la central como **zona de interruptor de llave**.

La zona de interruptor de llave puede ser por impulso o biestable. La salida del comunicador da por defecto un impulso de 3 segundos; la duración del impulso o el modo biestable los puedes cambiar en los ajustes de la aplicación Protegus 2.

Las centrales DSC, Paradox, Caddx, Texecom, InnerRange y Honeywell también se pueden conectar al comunicador a través de su salida de línea telefónica (apartado 3.3.10); en ese caso, también en ellas hay que configurar el marcador, y el control directo no está disponible.

4.2.1 Programación del marcador de la Honeywell Vista

Entra en el modo de programación desde el teclado y configura estas direcciones de programa:

Dirección	Ajuste
`*41`	número de teléfono del receptor de la CRA: `1234`
`*43`	número de abonado de la central
`*47`	Tone dial = `1`, y el número de intentos de marcación
`*48`	`7` (por defecto)
`*49`	`5` (mensaje Split/Dual)
`*50`	retardo del envío de la alarma de intrusión – por defecto `2,0` (30 s); para envío inmediato `0,0`

En la central **Honeywell Vista 48**, configura además las siguientes direcciones de programa:

Dirección	Valor	Dirección	Valor	Dirección	Valor
`*41`	1234 (teléfono del receptor)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (número de abonado)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

Al terminar la programación, sal del modo de programación con el comando `*99`.

4.2.2 Marcador de la UTC Interlogix (Caddx) NX

Programación de la central Interlogix NX-4V2 (NX-6V2, NX-8V2) si el comunicador se conecta a los bornes TIP/RING de la central. En el teclado, introduce lo siguiente, uno tras otro:

Posición (location)	Teclas	Observación
	`*89713`	Entrada en la programación (`9713` es el código de instalador de fábrica)
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	Se encienden todos los LED de zona (segmento 1)
Location 4	`12345678*`	Se encienden todos los LED de zona (segmento 2)
Location 4	`12345678*#`	
Location 23	`23#`	Se encienden todos los LED de zona (segmento 3)
Location 23	`**`	Se encienden todos los LED de zona (segmento 3)
Location 23	`12345678*#`	Se encienden todos los LED de zona (segmento 3)
Location 37	`37#`	Se encienden todos los LED de zona (segmento 3)
Location 37	`**`	Se encienden todos los LED de zona (segmento 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT` `EXIT`	Salida de la programación

5. Control a distancia con la aplicación Protegus 2

Con la aplicación móvil y web Protegus 2, el usuario ve a distancia el estado del sistema, recibe avisos de los eventos, puede armar y desarmar y accionar las salidas del comunicador. La aplicación se puede descargar para Android e iOS (Google Play, App Store) o usar desde el navegador: web.protegus.app. Entra con tu nombre de usuario y tu contraseña, o regístrate con una cuenta nueva.

5.1 Añadir el equipo

Antes de añadir el equipo, comprueba:

1. La tarjeta SIM está activa y tiene funcionando la conexión de datos móviles; su código PIN está introducido en el equipo, o la petición de PIN está desactivada.
2. En la página **User reporting** → **PROTEGUS Cloud** de TrikdisConfig está marcada la opción **Enable connection** (apartado 6.5).
3. El LED **POWER** está encendido en verde.
4. El LED **NETWORK** está encendido en verde y parpadea en amarillo (el equipo está en la red).

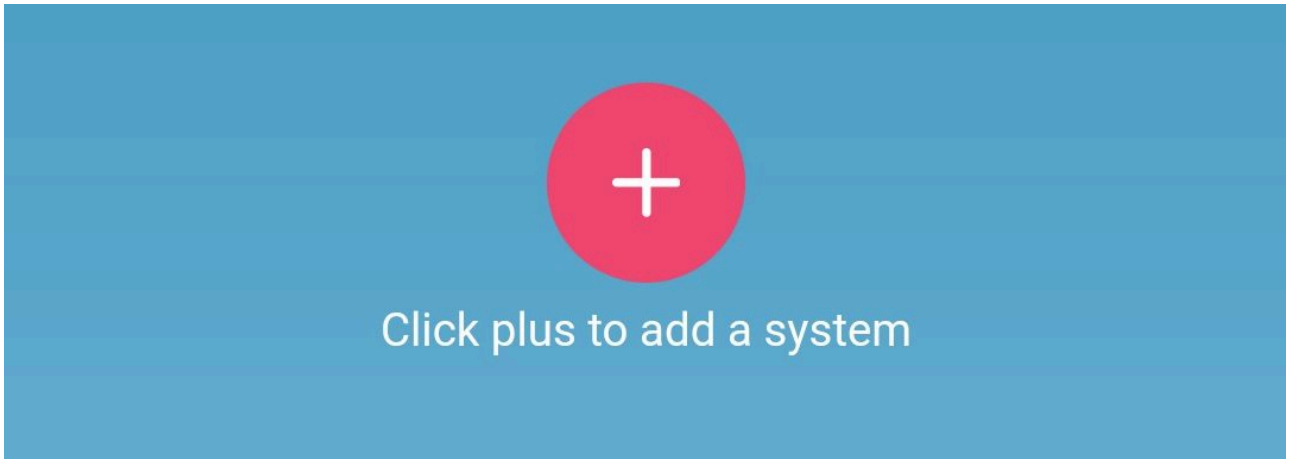
El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del operador; en uno Ethernet, que la conexión hasta el router funciona–, pero no que el dispositivo también salga a Internet. Si el LED NETWORK está en verde, pero el LED DATA sigue encendido de forma continua tras un evento o un informe de prueba, la conexión a Internet no funciona: el mensaje no puede salir. En red móvil lo más habitual es que fallen el APN o el servicio de datos de la tarjeta SIM; en Ethernet, el router, el cortafuegos o el DNS. Si el LED DATA se apaga, el mensaje se ha enviado y la conexión de datos está bien.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



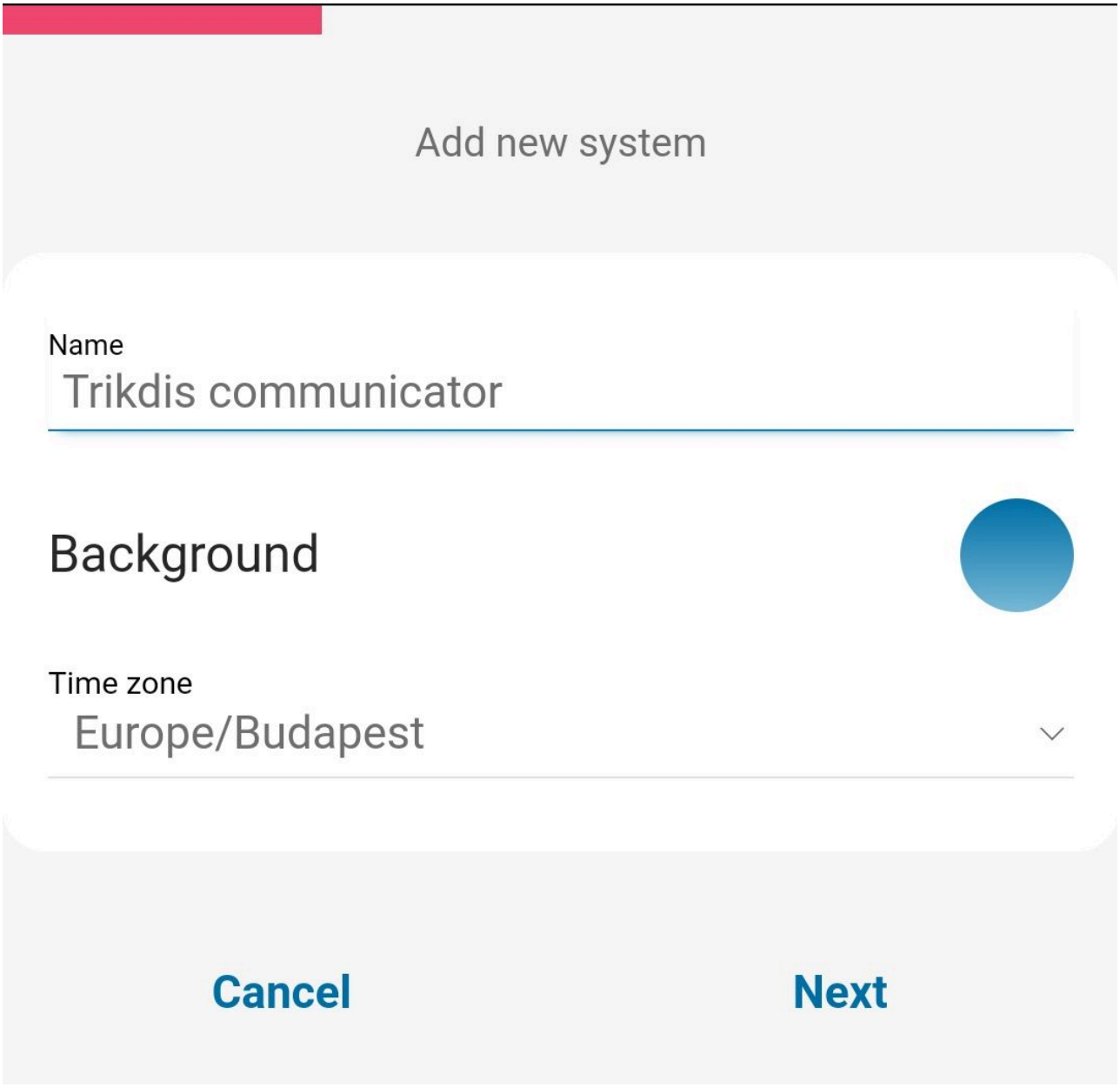
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



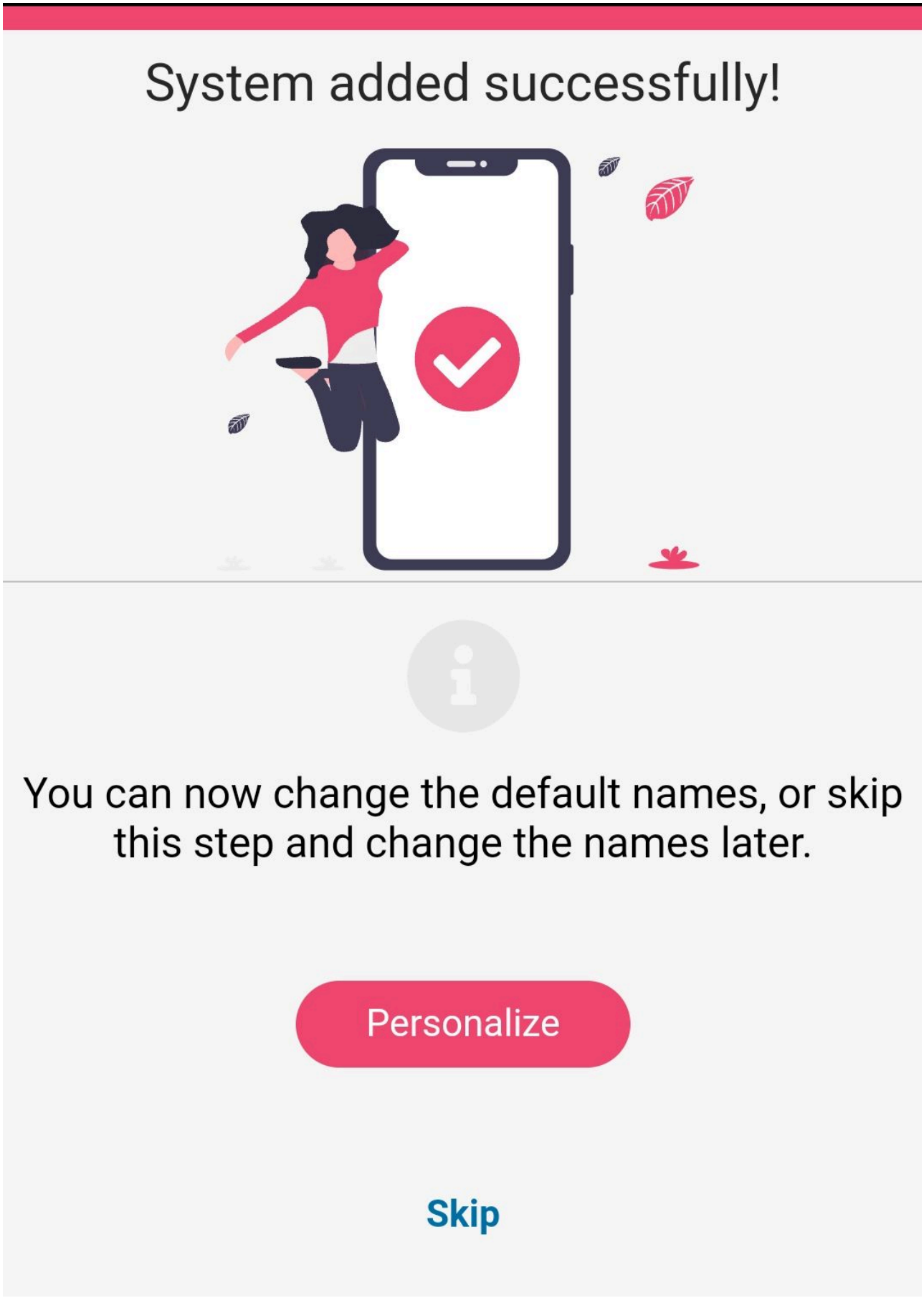
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



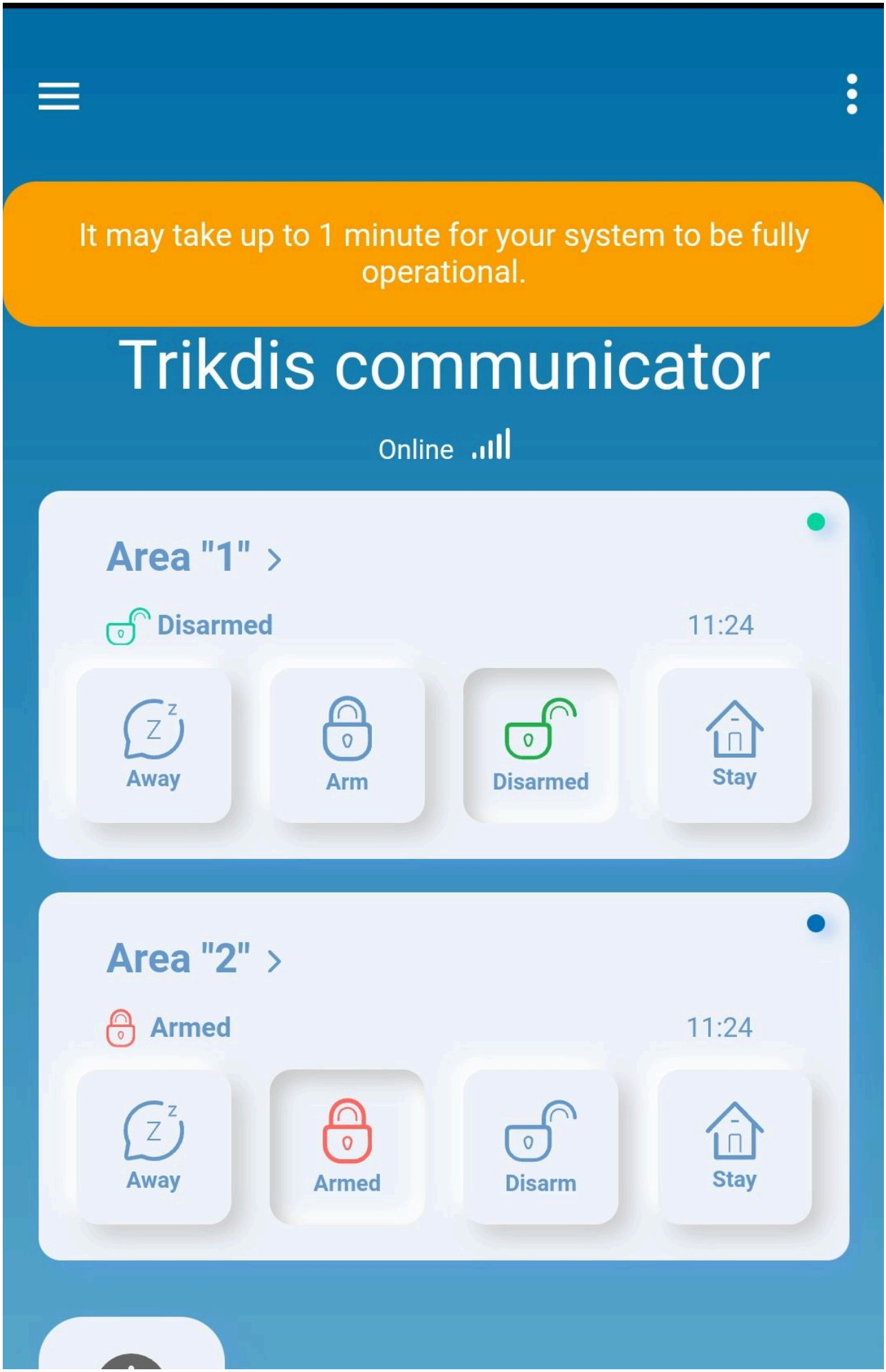
6. Add meg a rendszer nevét és válassz idozónát



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



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


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

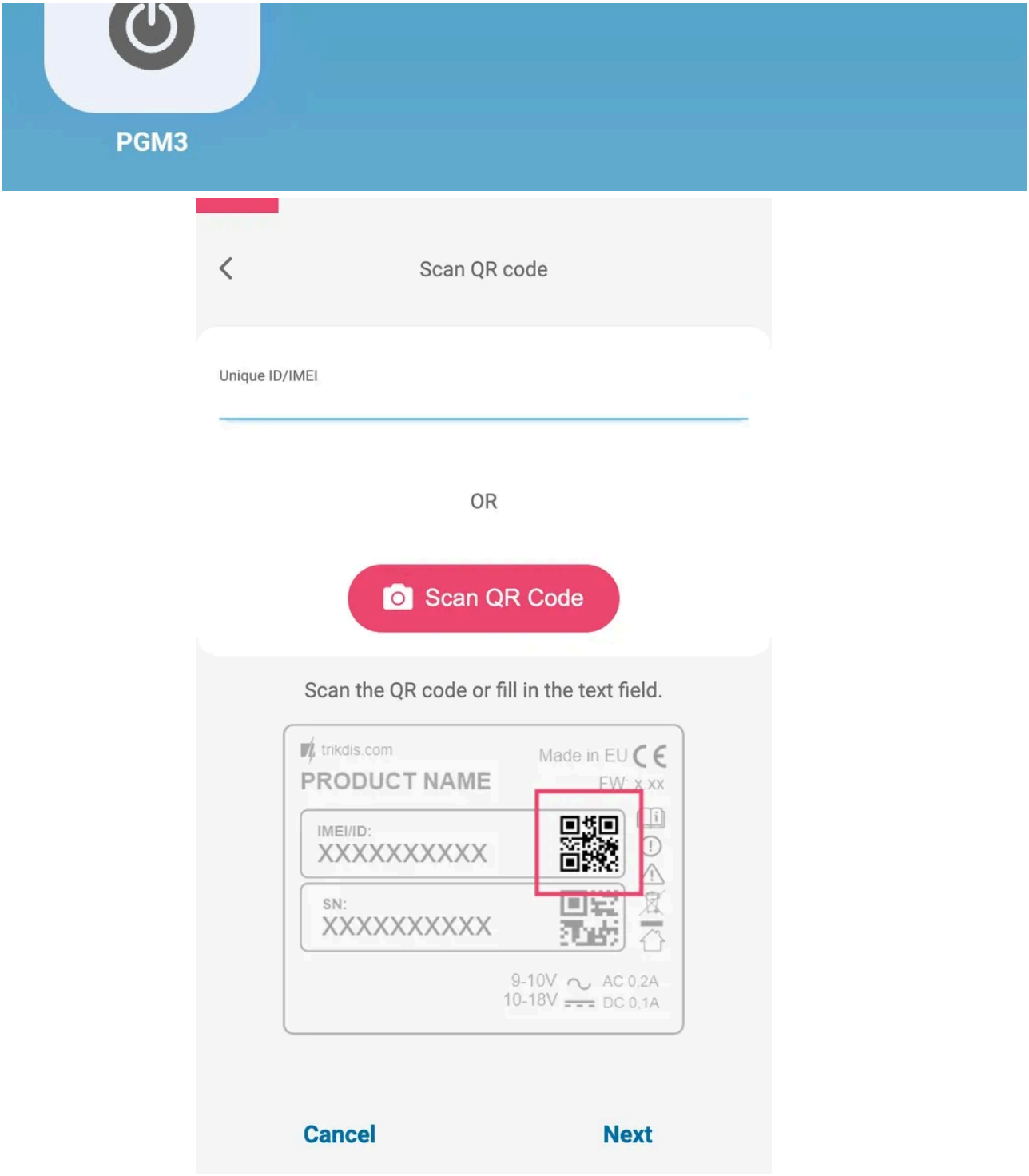


Figura 34. Protegus 2 – añadir un sistema nuevo: introducir el IMEI / Unique ID o escanear el código QR de la etiqueta y, después, Next.

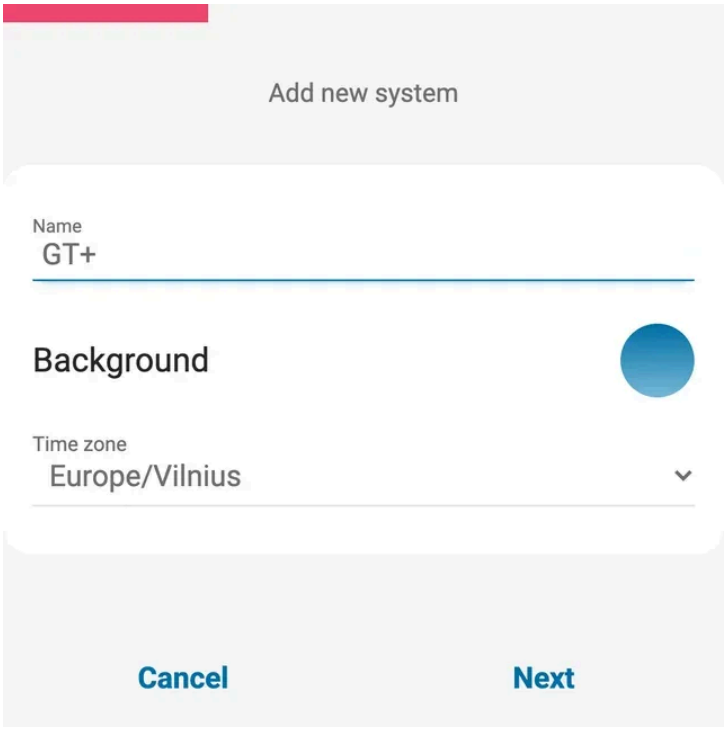


Figura 35. Protegus 2 – introducir el nombre (Name) del sistema y, después, Next.

El identificador único del equipo (**IMEI / Unique ID**) se puede leer en la etiqueta del equipo y en la pegatina de la caja, y también lo muestra la barra de estado de TrikdisConfig. Si el **PROTEGUS Cloud access Code** del equipo no es el de fábrica, la aplicación lo pide al añadir el equipo.

5.2 Armado y desarmado con una salida

Si quieres armar y desarmar la central de alarma con la salida del comunicador, a través de la zona de interruptor de llave de la central, indica en la aplicación Protegus 2, en la partición, qué salida la controla.

La zona de la central a la que se conecta la salida del comunicador debe estar programada en la central como **zona de interruptor de llave**, y la central debe comunicar los eventos de armado y desarmado: a partir de ellos Protegus 2 muestra el estado de la partición.

La configuración la puedes hacer al crear el sistema, al añadir las particiones, o más tarde en los ajustes del sistema, al editar la partición. Al crear el sistema, el asistente de Protegus 2 te guía: haz clic en el botón **Continue** (Continuar), introduce el nombre de la partición (**Area name**) y habilita el control de la salida PGM desde la aplicación Protegus 2; esto se hace con los pasos siguientes:

1. Selecciona (o añade) la partición que quieres controlar. El número de partición debe coincidir con el que envía la central en los eventos (la partición 1 con el 1, la 2 con el 2).
2. Activa la opción **Control con PGM** (Control with Protegus2) y, en el campo **salida** (Assigned Output), elige la salida del comunicador (PGM1, PGM2 …). Una salida solo puede controlar una partición.
3. Elige el modo de funcionamiento: **por impulso** (Pulse) o **biestable** (Level), el mismo que configuraste en la central para la zona de interruptor de llave. Normalmente usamos el de impulso; también se puede indicar la duración del impulso (por defecto 3 s).
4. Guarda el ajuste (**Save**). Si hay varias particiones, repítelo en cada una, con su propia salida: en el asistente añades otra partición con el botón **Click to add an area** y configuras su salida PGM de la misma manera. Cuando hayas configurado todas las particiones, continúa en el asistente con el botón **Skip**.

Protegus 2 solo puede mostrar correctamente el estado de las particiones si la central envía los eventos de armado y desarmado con el número de partición correcto. Los detalles y las trampas del armado con interruptor de llave se explican en un artículo aparte: Armado remoto con interruptor de llave desde la aplicación Protegus 2.

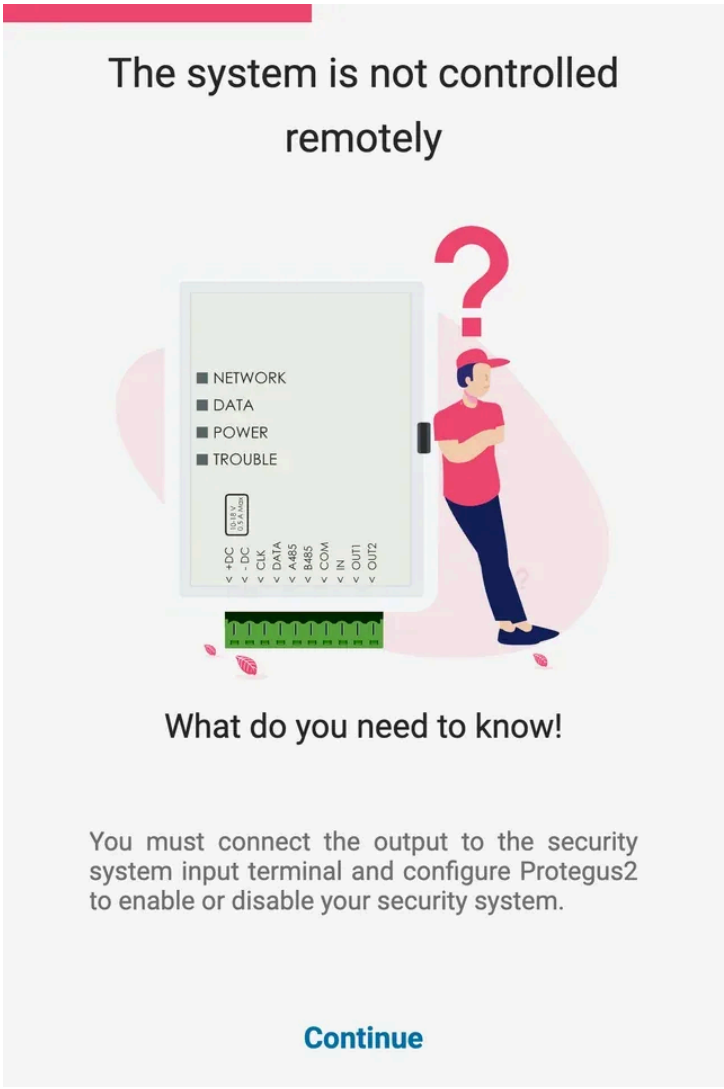


Figura 36. Protegus 2 – página «El sistema no se controla a distancia» al crear el sistema: con el botón Continue pasas a configurar la partición y la salida PGM.

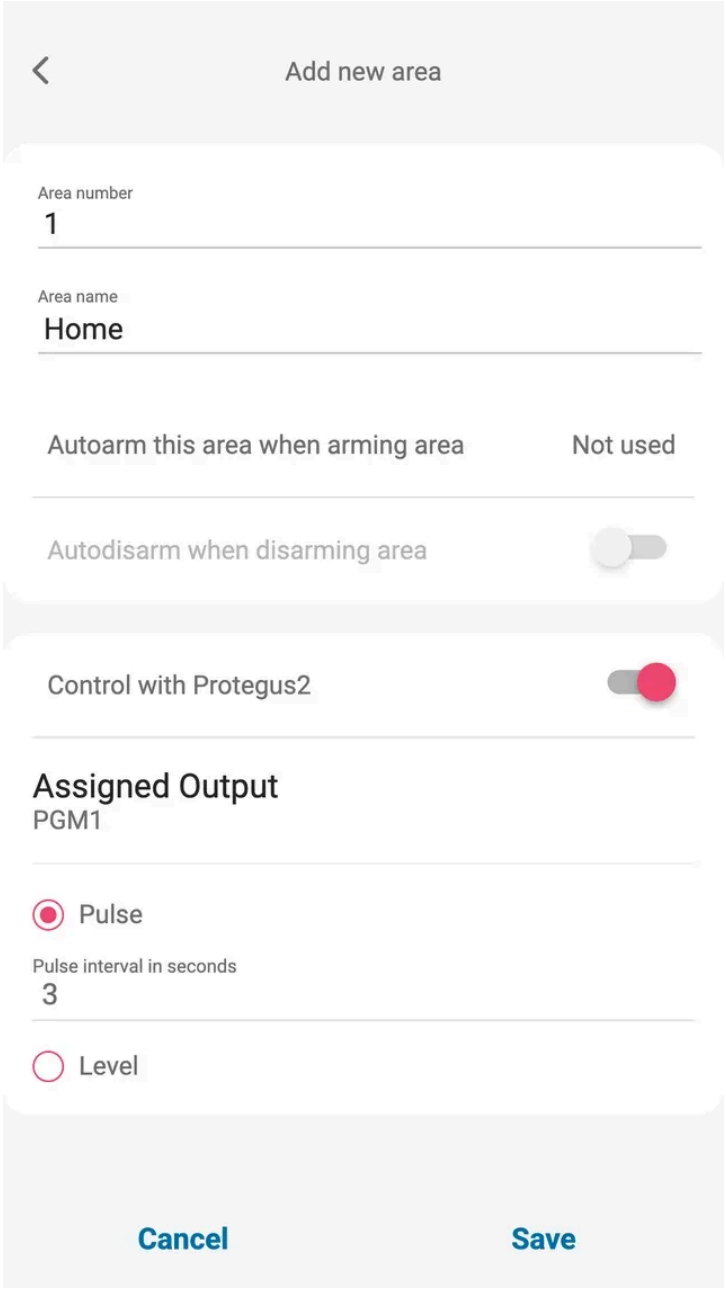


Figura 37. Protegus 2 – añadir una partición (Add new area): Area number, Area name, Control with Protegus2 activado, Assigned Output PGM1, Pulse (3 s) o Level y, después, Save.

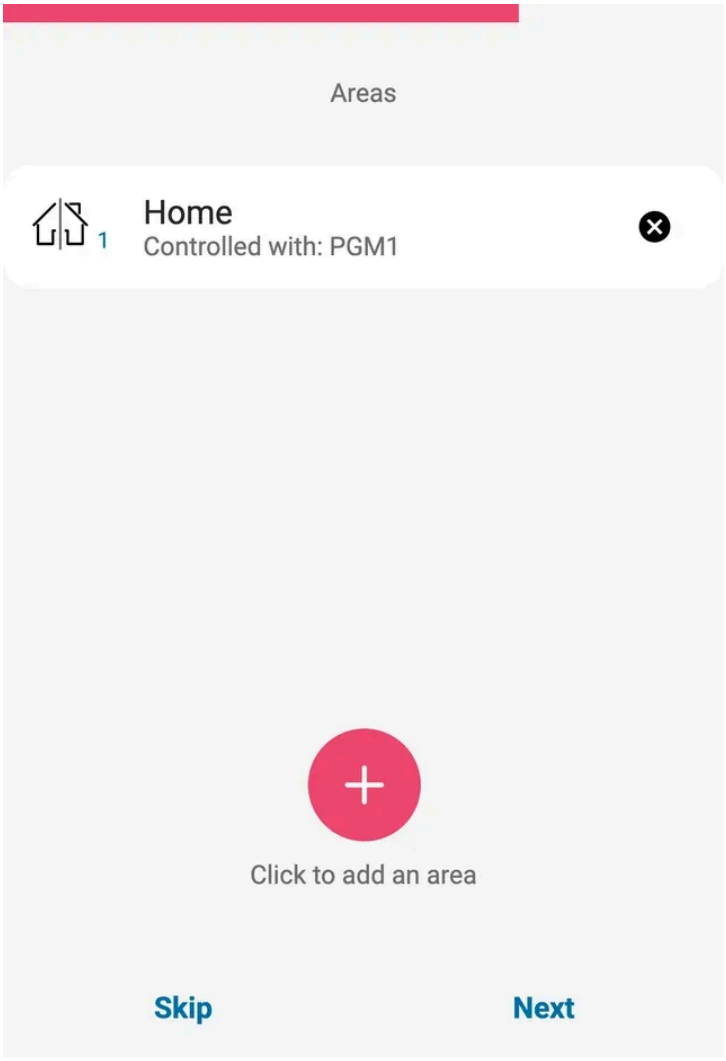


Figura 38. Protegus 2 – la lista de particiones (Areas): la partición Home la controla la PGM1; se añade otra partición con el botón Click to add an area, y el asistente se cierra con el botón Skip.

5.3 Armado y desarmado desde 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.

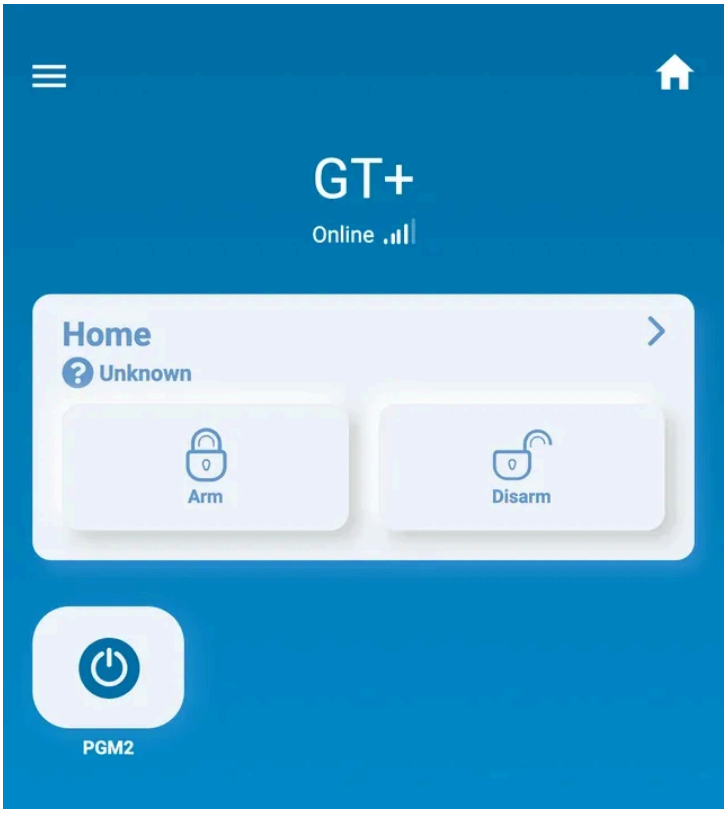


Figura 39. Protegus 2 – la pantalla de inicio del sistema: el estado de la partición, los botones Arm y Disarm y, debajo, la salida PGM que se puede accionar.

5.4 Control con mensajes SMS

El comunicador también se puede controlar con comandos SMS. Estructura del mensaje: `Contraseña Comando Datos` (separados por espacios). Como contraseña puedes usar el código de **administrador** (de fábrica, `123456`) para los comandos `INFO`, `RESET` y `OUTPUTx`, y el código de **instalador** (de fábrica, `654321`) para los comandos `INFO` y `OUTPUTx`.

Comando	Datos	Qué hace	Ejemplo
`INFO`	–	Pide información sobre el equipo. La respuesta: el tipo de equipo, su número IMEI, su número de serie y su versión de firmware.	`123456 INFO`
`RESET`	–	Reinicia el equipo (solo con el código de administrador).	`123456 RESET`
`OUTPUTx`	`ON`	Activa la salida x (x = 1 o 2).	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Desactiva la salida x.	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Activa la salida en modo de impulso durante el tiempo indicado; `tttt` es la duración del impulso en segundos, con cuatro dígitos.	`123456 OUTPUT2 PULSE=0002`

La salida solo se puede accionar si, en la página **IN/OUT** de TrikdisConfig, el borne I/O correspondiente está configurado como salida (**OUT**). Desde qué números de teléfono acepta comandos el equipo lo puedes limitar en la pestaña **User reporting** → **Control by SMS** (apartado 6.5).

6. TrikdisConfig – los ajustes en detalle

En la parte izquierda de la ventana de TrikdisConfig se ve la lista de páginas (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, RS485 modules, Event summary, Firmware); arriba, la barra de botones (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), y abajo, la barra de estado. Este capítulo recorre página por página los ajustes del GT y del GT+; donde las dos versiones son distintas, lo indicamos aparte.

6.1 La barra de estado

Después de conectar el dispositivo y leerlo (**Read [F4]**), en la parte inferior de la ventana se ven los datos más importantes del dispositivo:

Rótulo	Significado
IMEI / Unique ID, en un dispositivo Ethernet **MAC / Unique ID**	Identificador único del dispositivo: en un dispositivo con tarjeta SIM, el IMEI; en un dispositivo Ethernet, la dirección MAC. El mismo figura en la caja y en la parte trasera del dispositivo.
Status	Estado de funcionamiento actual.
Device	Tipo de dispositivo (modelo). Comprueba que aquí figura el modelo de tu dispositivo.
SN	Número de serie.
BL	Versión del bootloader.
FW	Versión del firmware.
HW	Versión del hardware.
State	Modo de conexión: USB o remoto (remote).
Administrator / Installer	Nivel de acceso de quien programa (después de introducir la contraseña).

Una vez hechos los ajustes, los escribes en el dispositivo con el botón **Write [F5]**; con los botones **Open [F8]** y **Save [F9]** puedes guardar el conjunto completo de ajustes en un archivo y cargarlo en otro dispositivo. **Save [F9]** guarda los ajustes en un archivo de configuración y **Open [F8]** abre el archivo guardado; más tarde puedes cargar los ajustes guardados también en otros dispositivos, y así configurar varios dispositivos rápidamente con los mismos ajustes.



Figura 40. La barra de estado de TrikdisConfig con un GT+ leído: identificador, estado, tipo (Device: GT+_M150), número de serie, versiones, modo de conexión y nivel de acceso.

En el campo **Device** debe figurar el tipo GT en el GT y GT+ en el GT+ (en la imagen, GT+_M150; el sufijo de letra y número indica la versión de hardware). Después de **Read [F4]**, el programa lee y muestra los valores configurados en el equipo; haz los ajustes necesarios según las descripciones de las páginas que siguen.

6.2 System settings

La página tiene dos grupos: en el grupo **General** configuras los identificadores del equipo, y en el grupo **Access**, los niveles de acceso.

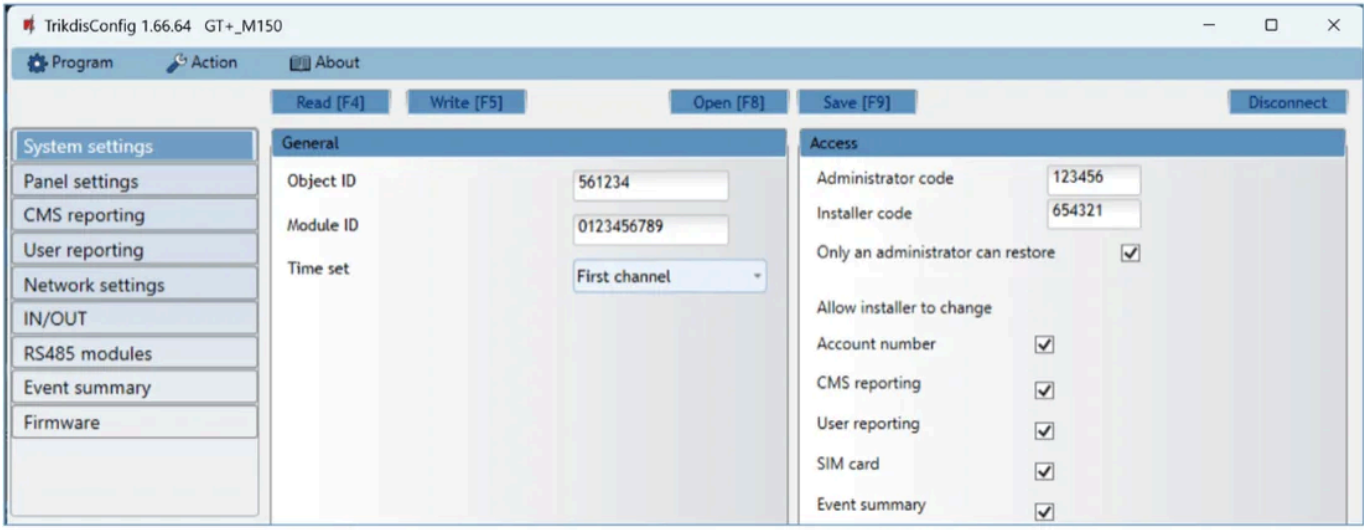


Figura 41. TrikdisConfig – página System settings: grupos General y Access.

- **Object ID** – el identificador de abonado que te da la CRA (6 caracteres hexadecimales: 0–9, A–F; no se pueden usar `FFFE` ni `FFFF`). Obligatorio si el equipo también transmite a una CRA.
- **Module ID** – el número de identificación del módulo.
- **Time set** – de qué servidor sincroniza el equipo su reloj.

En el grupo **Access** gestionas los niveles de acceso y las contraseñas.

Para los ajustes del dispositivo hay dos niveles de acceso: **administrador** e **instalador**.

- **Administrator code** – acceso a todos los ajustes (contraseña de fábrica: `123456`; la contraseña tiene 6 caracteres: dígitos o letras latinas).
- **Installer code** – acceso que se puede limitar (contraseña de fábrica: `654321`).
- **Only an administrator can restore** – marcado, solo el administrador puede iniciar el restablecimiento de los ajustes de fábrica.
- **Allow installer to change** – aquí puedes indicar qué grupos de ajustes puede modificar el instalador: **Account number** (número de abonado), **CMS reporting**, **User reporting**, **SIM card** (en un dispositivo de red móvil) o **Ethernet settings** (en un dispositivo Ethernet), **Event summary**.

¡No dejes las contraseñas de fábrica en el dispositivo!

En la puesta en marcha, cambia como mínimo la contraseña de administrador y anótala en un lugar seguro. Una contraseña olvidada no se puede borrar ni siquiera restableciendo los ajustes de fábrica, porque para ello también se necesita contraseña: solo el fabricante o el distribuidor puede restablecerla, si le haces llegar el equipo. La excepción es un equipo con botón RESET físico: mantenerlo pulsado 10 segundos restablece los ajustes de fábrica sin contraseña.

6.3 Panel settings

En esta página indicas cómo se conecta el comunicador a la central de alarma: el grupo **TLC** contiene los ajustes de la conexión por línea telefónica (TIP/RING), y el grupo **Serial bus**, los de la conexión al bus de datos o serie. Aquí están también los ajustes comunes que afectan al tratamiento de los eventos de la central.

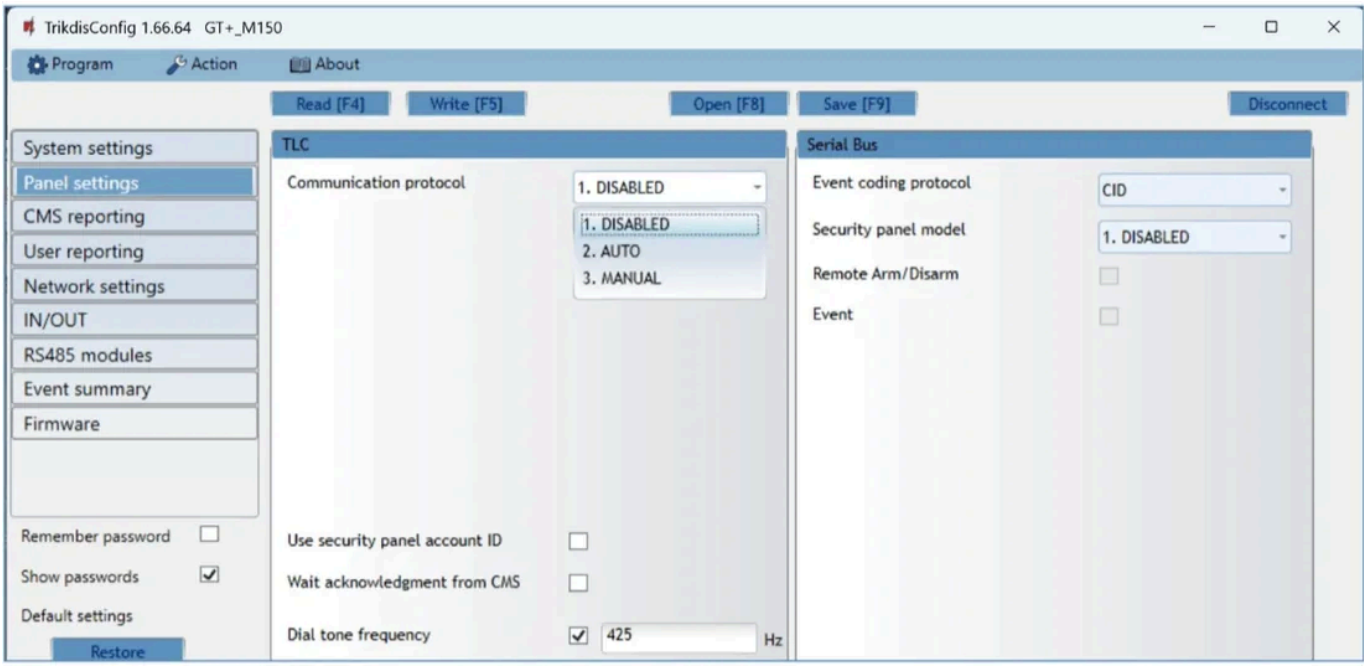


Figura 42. TrikdisConfig – Panel settings en el GT+: la lista Communication protocol del grupo TLC (1. DISABLED, 2. AUTO, 3. MANUAL); debajo, el grupo Serial bus y los ajustes comunes.

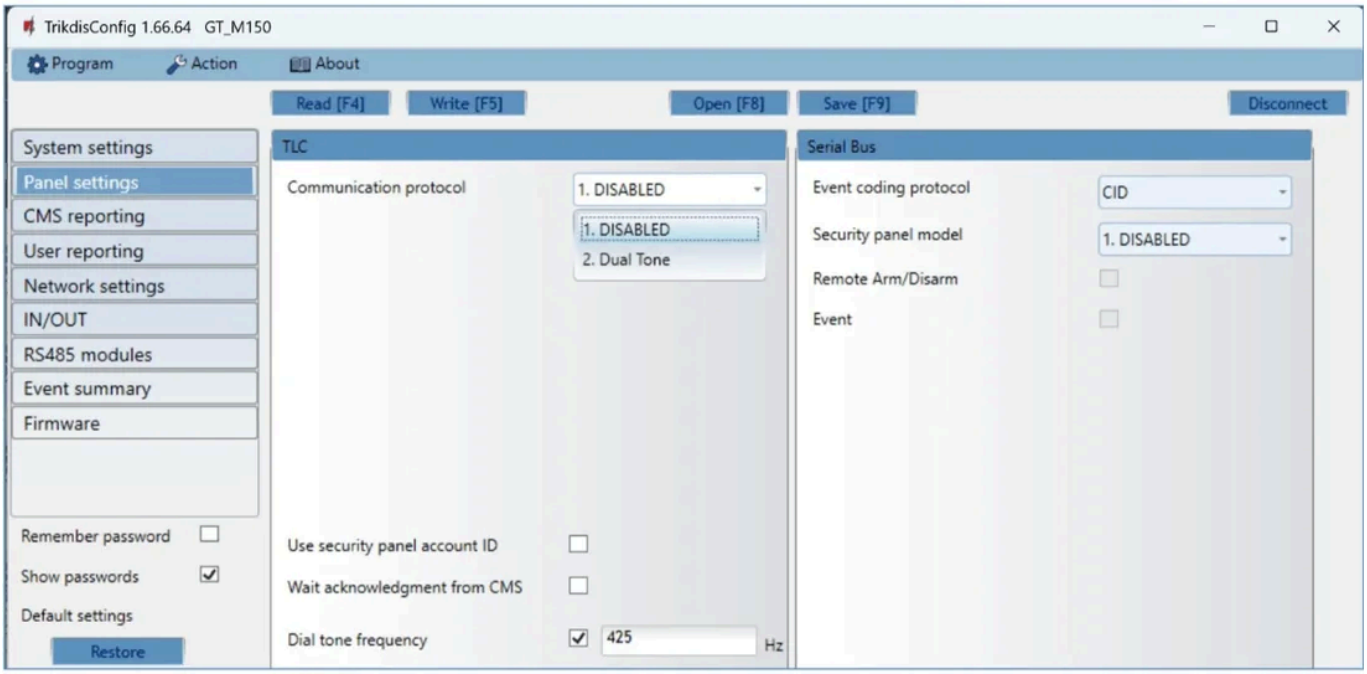


Figura 43. TrikdisConfig – Panel settings en el GT: aquí la lista Communication protocol es 1. DISABLED y 2. Dual tone.

Grupo TLC – si el comunicador se conecta a los bornes TIP/RING de la central:

- **Communication protocol** – activa o desactiva la interfaz de línea telefónica DTMF del comunicador. GT+: **1. DISABLED** (desactivada), **2. AUTO**, **3. MANUAL**; GT: **1. DISABLED**, **2. Dual tone**. Con conexión TIP/RING, elige el valor AUTO (GT: Dual tone).

Ajustes debajo del grupo, válidos para las dos conexiones:

- **Use security panel account ID** – marcado, el comunicador no usa su propio Object ID, sino el identificador de abonado configurado en la central y enviado por ella.

- **Wait acknowledgment from CMS** – marcado, después de cada evento el comunicador espera la confirmación del receptor (kiss-off) y solo después confirma a la central; si la confirmación no llega a tiempo, vuelve a enviar el mensaje. Si el equipo no transmite a una CRA, déjalo desactivado.
- **Dial tone frequency** – la frecuencia del tono de línea con la que el comunicador se comunica con el marcador de la central (por defecto, 425 Hz, que también es el tono de línea en España y en la mayor parte de Europa).



Figura 44. TrikdisConfig – Panel settings, grupo Serial bus: Event coding protocol CID, Security panel model (en la imagen, Paradox SP/MG), Remote Arm/Disarm y Event marcados, Security panel PC download password introducida.

Grupo Serial bus – si el comunicador se conecta al bus de datos o al puerto serie de la central:

- **Event coding protocol** – el protocolo de codificación de eventos (CID).
- **Security panel model** – el modelo de la central de alarma conectada, de la lista (para la conexión Keybus + TIP/RING de Paradox SP / SP+ / MG / MG+, elige el elemento **7. Paradox SP+/MG+ series KeyBus**).
- **Remote Arm/Disarm** – marcado, el comunicador controla la central directamente (armado y desarmado desde Protegus 2). Solo es visible en las centrales de control directo. Para el control directo también hay que configurar la central según el capítulo 4.
- **Security panel PC download password** – para el control directo de centrales Paradox y Texecom, la contraseña de PC o de UDL; debe coincidir con la contraseña configurada en la central, cuya introducción se describe en el capítulo 4.

6.4 CMS reporting

El comunicador envía los eventos a la CRA por la conexión de datos móviles (IP). Los eventos pueden ir por varios canales: el canal **principal** y el **paralelo** funcionan a la vez (a dos receptores a la vez), y cada uno tiene un canal **de respaldo**, que entra en funcionamiento si ese canal se corta. La comunicación está cifrada y protegida con contraseña; para recibir los eventos y reenviarlos al software de CRA hace falta un receptor Trikdis (receptor de software IPcom –Windows o Linux–, receptor IP/SMS RL14 o receptor multicanal RM14) o un receptor universal que admita el protocolo DC-09 / TL150. El GT y el GT+ solo transmiten a la CRA por canal IP; no tienen canal SMS.

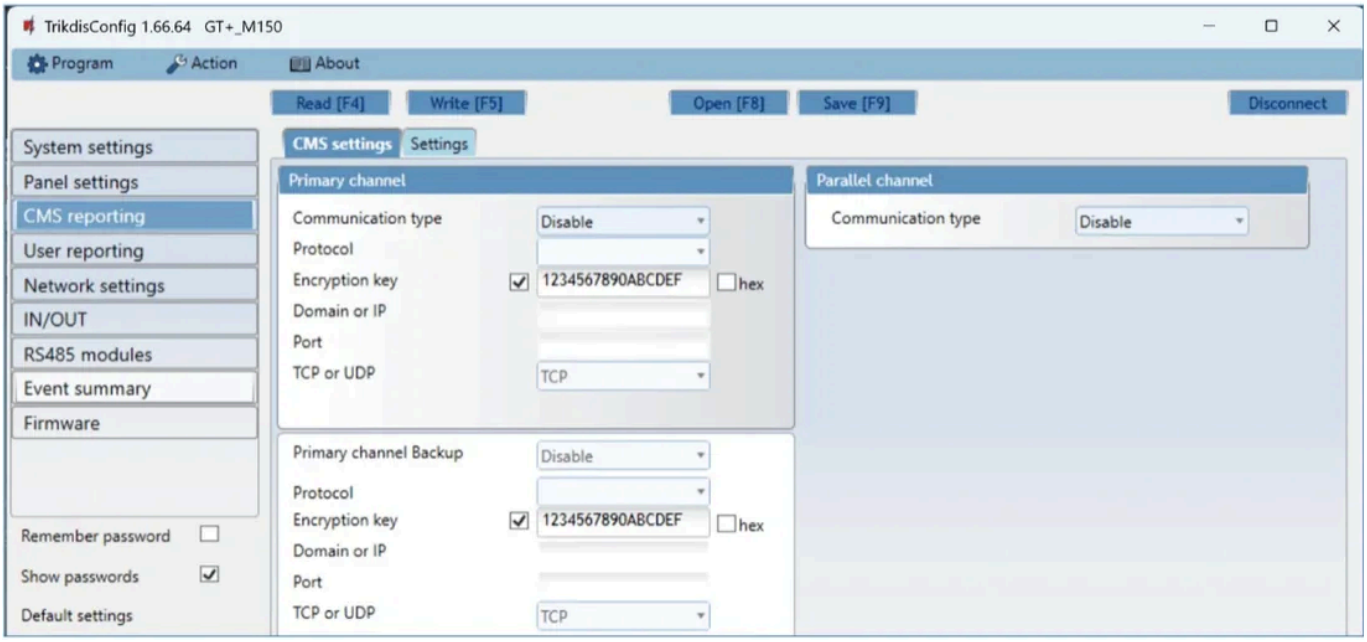


Figura 45. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal, de respaldo y paralelo.

Primary channel – canal principal

- **Communication type** – el modo de conexión con el receptor: **IP**.
- **Protocol** – **TRK8** (receptores Trikdis), **DC-09_2007** o **DC-09_2012** (receptores universales), **TL150** (receptores SUR-GARD).
- **Encryption key** – la clave de cifrado de los mensajes; en el comunicador y en el receptor debe ser la misma.
- **Domain or IP**, **Port** – el nombre de dominio o la dirección IP del receptor y su puerto.
- **TCP or UDP** – el protocolo de transmisión.

Parallel channel – canal paralelo. Además del principal, envía a la vez a un segundo receptor (por ejemplo, a la CRA local y a la central). Sus ajustes son los mismos que los del canal principal.

Primary channel Backup – canal de respaldo. Asume la comunicación si el canal principal no funciona; sus ajustes son iguales a los anteriores.

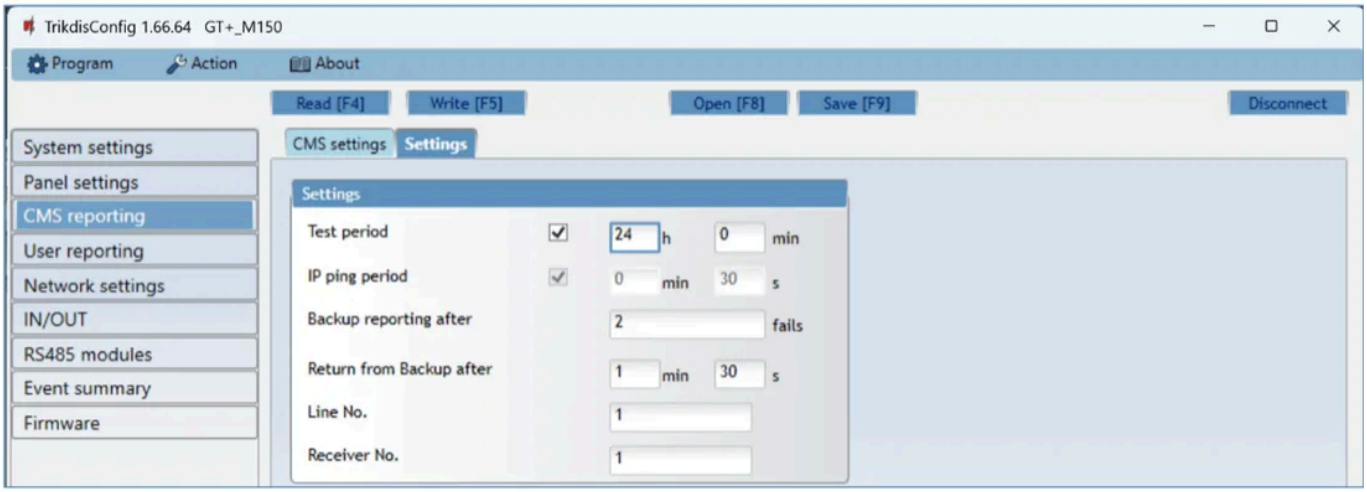


Figura 46. TrikdisConfig – CMS reporting, pestaña Settings: informe de prueba, PING, temporizaciones del canal de respaldo y datos DC-09.

En la pestaña **Settings** configuras las temporizaciones y los datos DC-09.

- **Test period** – intervalo del informe de prueba periódico (por defecto 24 horas). El informe de prueba se envía como mensaje Contact ID a la CRA y a Protegus 2.
- **IP ping period** – intervalo de la señal de vida (PING) en el canal IP (por defecto 30 s). Lo activas con la casilla y el tiempo lo indicas en los apartados de minutos (**min**) y segundos (**s**) del campo; es necesario para supervisar la conexión. El receptor no reenvía los PING al software de la CRA, para no sobrecargarlo; el software solo recibe un mensaje si el receptor no recibe ningún PING durante el triple del tiempo configurado. Por ejemplo, si el periodo de PING es de 3 minutos, la pérdida de conexión se señaliza pasado el minuto 9.
- **Backup reporting after** – tras este número de intentos de envío fallidos, el dispositivo pasa al canal de respaldo (por defecto 2).
- **Return from Backup after** – tras este tiempo vuelve al canal principal (por defecto 1 minuto 30 s).

El PING mantiene viva la conexión entre el dispositivo y el receptor, y de él dependen también el acceso, el control y la programación remotos. Por eso **no recomendamos un periodo de PING superior a 5 minutos**.

DC-09 Settings (a la derecha de la pestaña) – solo hay que rellenarlo si envías por algún canal con el protocolo DC-09_2007 o DC-09_2012; el grupo aparece cuando en el campo **Protocol** de algún canal está seleccionado DC-09_2007 o DC-09_2012:

- **Object ID in DC-09** – identificador hexadecimal de 3 a 16 caracteres; te lo da la CRA.
- **DC-09 line No** – número de línea.
- **DC-09 receiver No.** – número de receptor.

En la pestaña Settings del GT y del GT+, en el grupo DC-09 figuran los campos **Line No.** (número de línea) y **Receiver No.** (número de receptor); el grupo aparece cuando en el campo **Protocol** de alguno de los canales está seleccionado DC-09_2007 o DC-09_2012.

6.5 User reporting

En la pestaña **PROTEGUS Cloud** activas el servicio Protegus, con el que el usuario supervisa y controla a distancia el comunicador y el sistema conectado a él; más información: www.protegus.app.

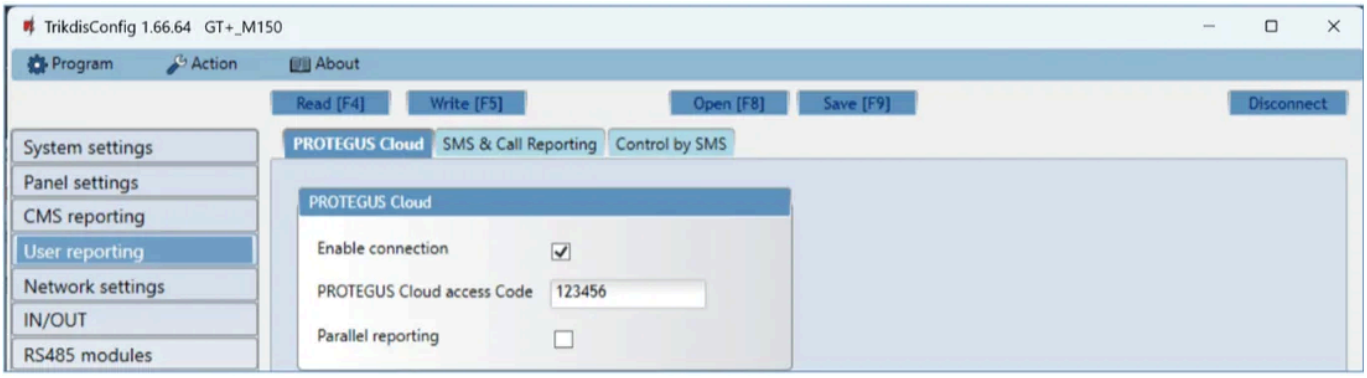


Figura 47. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- **Enable connection** – activa el servicio Protegus: el equipo intercambia datos con la aplicación Protegus 2, y TrikdisConfig también puede acceder a él a distancia.
- **PROTEGUS Cloud access Code** – código de 6 dígitos para conectarse a Protegus 2 (de fábrica, `123456`). Si lo cambias en TrikdisConfig, también hay que cambiarlo en la aplicación Protegus 2.
- **Parallel reporting** – marcado, los mensajes van a la vez por el canal principal (a la CRA) y a Protegus 2.

En la pestaña **SMS & Call Reporting**, el usuario también puede recibir avisos de los eventos por SMS o por llamada telefónica.

En caso de alarma, el dispositivo envía primero el SMS a todos los números de teléfono introducidos y después los llama uno a uno, de Tel 1 a Tel 4. Cada número se llama una vez y suena durante 20 segundos; la llamada se considera correcta si el número suena (también basta con que se conteste o se rechace). El módem realiza la llamada por 2G o VoLTE. Donde el operador ha apagado el 2G y no ha aprobado el módem para VoLTE, el SMS llega, pero el teléfono no suena. No es un error de configuración. En esos lugares, utilice el SMS y la aplicación Protegus 2.

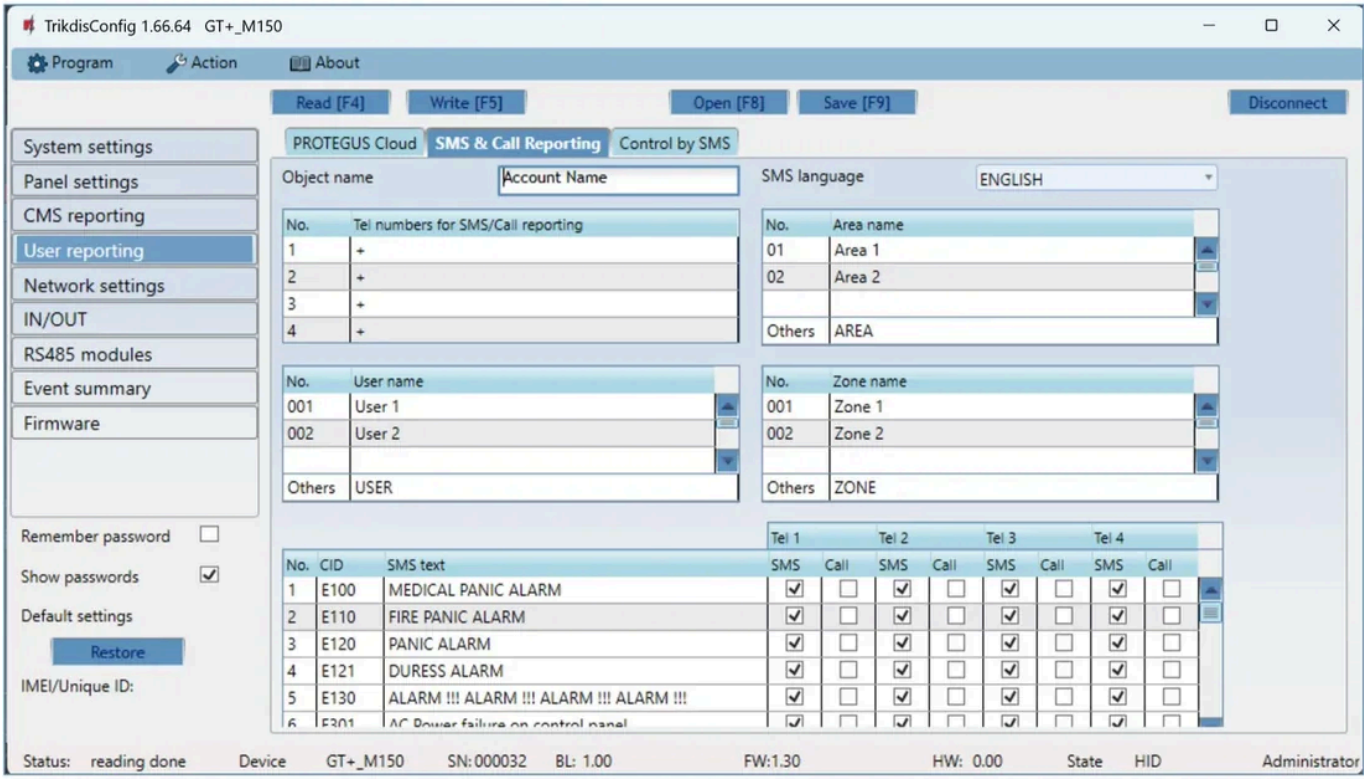


Figura 48. TrikdisConfig – User reporting, pestaña SMS & Call Reporting.

- **Object name** – el nombre del sistema; figura en cada SMS.
- **SMS language** – el idioma de los SMS (los mensajes también se pueden enviar con los caracteres propios del idioma).
- **Tel numbers for SMS/Call reporting** – hasta 4 números de teléfono que reciben SMS o llamadas sobre los eventos; introdúcelos con el prefijo del país (por ejemplo, `+34...`, `0034...` o `34...`).
- **Area name, User name, Zone name** – los nombres de las particiones, usuarios y zonas; el equipo los usa en el texto de los SMS. En la tabla correspondiente escribe el número de la partición, del usuario o de la zona y, a su lado, su nombre.
- **CID event table** – para cada evento se puede configurar qué número recibe SMS o llamada. El texto SMS y el código Contact ID de los eventos predeterminados se pueden modificar, y también se puede añadir un evento nuevo con su descripción.

En la pestaña **Control by SMS** configuras la recepción de comandos SMS: con los comandos se pueden accionar las salidas y pedir información sobre el equipo (los comandos se describen en el apartado 5.4).

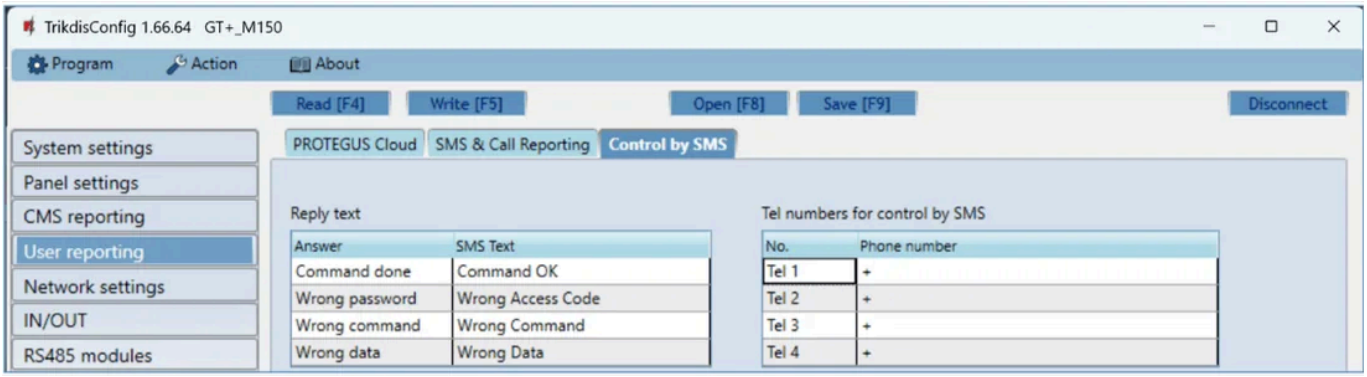


Figura 49. TrikdisConfig – User reporting, pestaña Control by SMS.

- **Reply text** – el texto de los mensajes de respuesta a un comando SMS: comando correcto (Command done), contraseña incorrecta (Wrong password), comando incorrecto (Wrong command), datos incorrectos (Wrong data). Los textos se pueden editar.
- **Tel numbers for control by SMS** – los números de teléfono desde los que el equipo acepta comandos.

Si aquí no hay ningún número de teléfono, el equipo acepta el comando desde cualquier número. Incluso en ese caso, la seguridad la da que en el comando es obligatoria la contraseña de administrador o de instalador.

6.6 Network settings

Antes de usarlo, asegúrate de que la tarjeta SIM está activa y funciona. Si envías los eventos por canal IP o a Protegus 2 por internet móvil, la tarjeta también debe tener activado el servicio de datos móviles.

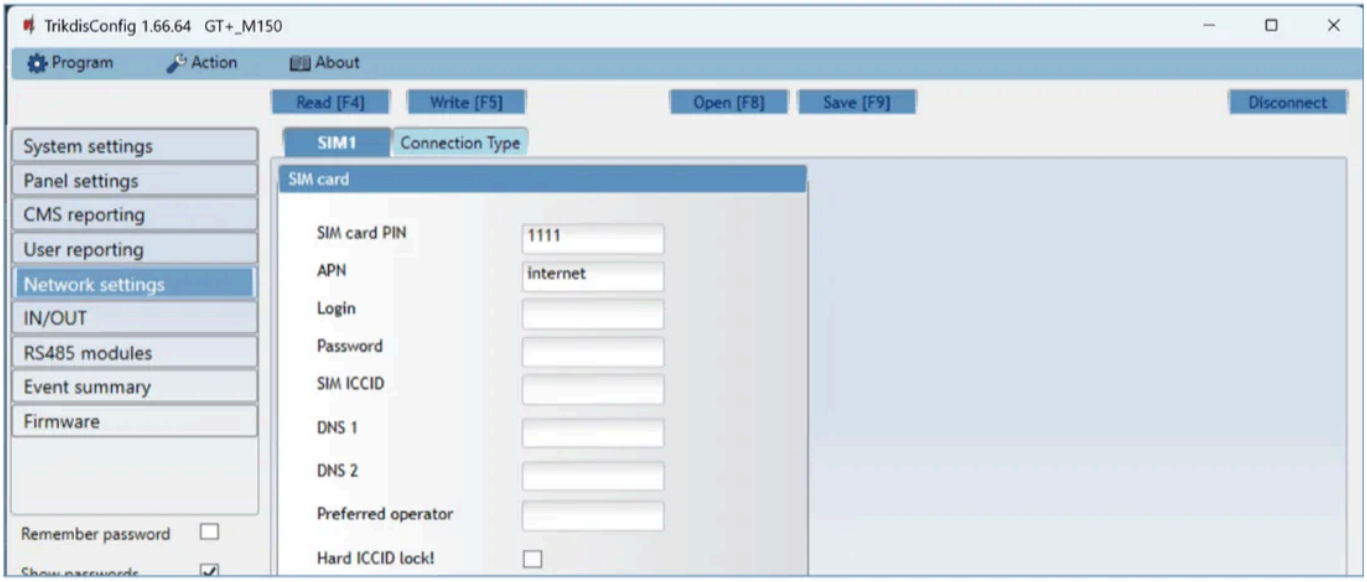


Figura 50. TrikdisConfig – Network settings, pestaña SIM1: los datos de la tarjeta SIM.

Pestaña SIM1, grupo SIM card

- **SIM card PIN** – el código PIN de la tarjeta. La petición de PIN la puedes desactivar poniendo la tarjeta en un teléfono móvil y desactivándola allí; en ese caso, el campo puede quedarse con el valor de fábrica.
- **APN** – el punto de acceso del operador (Access Point Name); sin él, el equipo no se conecta a internet. El valor lo encuentras en la web del operador de la tarjeta SIM; `internet` es genérico y funciona en las redes de muchos operadores. Los APN conocidos de los operadores los recoge el artículo de los APN (con una tarjeta IoT / M2M, el operador da un APN aparte; ver el apartado 2.2).

- **Login, Password** – nombre de usuario y contraseña para la conexión a internet, si el operador los pide.
- **SIM ICCID** – el número ICCID de la tarjeta SIM, si quieres que el equipo solo funcione con esta tarjeta. Si el ICCID de la tarjeta colocada no coincide, el LED TROUBLE da 8 destellos (apartado 1.6).
- **DNS 1, DNS 2** – servidores de nombres (DNS, Domain Name System: da la dirección IP que corresponde a un nombre de dominio); hacen falta si has introducido el receptor en el campo **Domain or IP** con un nombre de dominio y no con una dirección IP. Por defecto, el DNS público de Google. Independientemente de los ajustes IP, comprueba que las direcciones DNS funcionan con tu operador.
- **Preferred operator** – el código del operador móvil (MCC + MNC); si lo introduces, el equipo solo se conecta a la red del operador elegido.
- **Hard ICCID lock** – marcado, y después de reiniciar el equipo, el comunicador queda vinculado estrictamente a la tarjeta SIM con el número ICCID indicado.

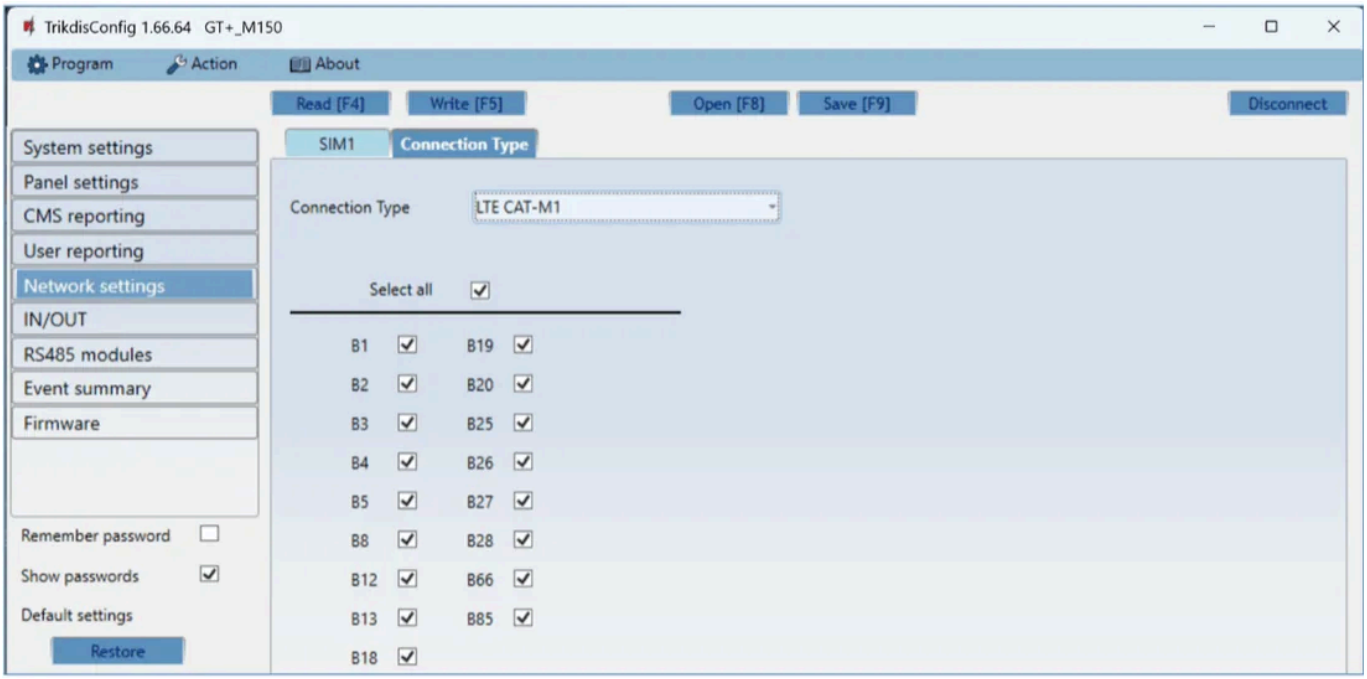


Figura 51. TrikdisConfig – Network settings, pestaña Connection Type: selección de las bandas LTE de la versión con módem CAT-M1.

Pestaña Connection Type – solo válida en la versión con módem CAT-M1 (BG95-M5): aquí puedes indicar en qué bandas de frecuencia LTE funciona el módem del equipo (**Select all** = todas).

6.7 IN/OUT

Aquí indicas la función de los dos bornes de E/S de doble función del comunicador: **Off** (no usado), **IN** (entrada) u **OUT** (salida). En una entrada, en el campo **Type** también hay que indicar el tipo de circuito conectado (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

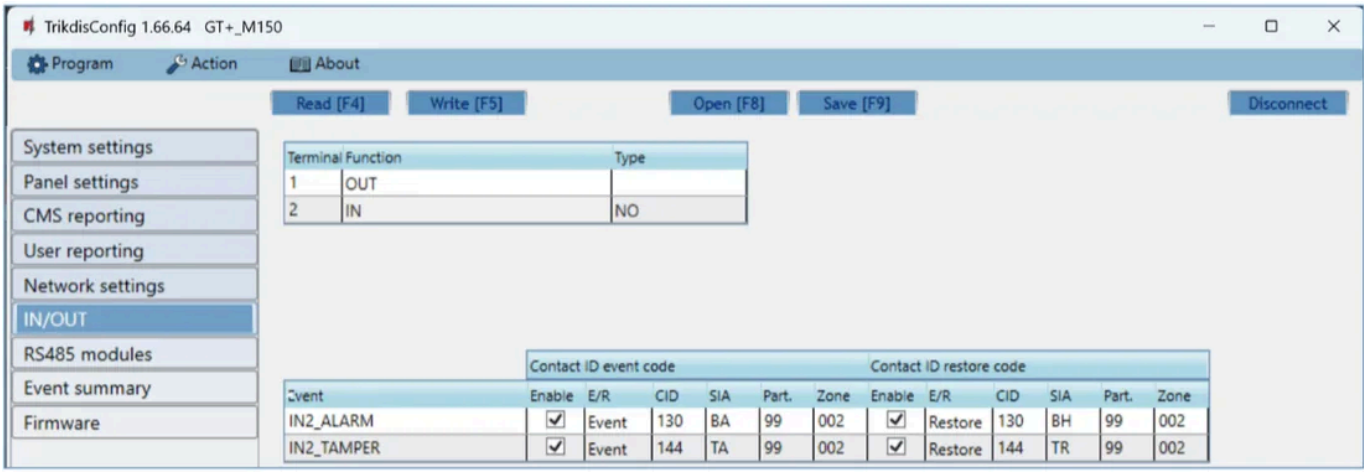


Figura 52. TrikdisConfig – página IN/OUT: el borne 1 como salida (OUT), el 2 como entrada (IN, NO); debajo, los eventos de alarma y de sabotaje de la entrada 2 con código CID y SIA.

Cuando se activa el detector conectado a la entrada, el comunicador envía un evento propio (**INx_ALARM**, Contact ID 130, SIA BA; restauración BH), y cuando se activa el circuito de sabotaje, un evento de sabotaje (**INx_TAMPER**, 144, SIA TA; restauración TR) a la CRA y a Protegus 2; en la tabla aparecen los eventos de todos los bornes configurados como entrada. Columnas de la tabla:

- **Enable** – activa el envío del mensaje a la CRA y a Protegus 2.
- **E/R** – el tipo de mensaje: Event (evento) o Restore (restauración).
- **CID** – el código Contact ID (se puede cambiar o dejar el de fábrica).
- **SIA** – el código SIA (se puede cambiar o dejar el de fábrica).
- **Part.** – el número de partición en el mensaje.
- **Zone** – el número de zona en el mensaje.

6.8 RS485 modules

Con expansores **iO-8** conectados al bus RS485 se pueden añadir más entradas y salidas al comunicador. Los expansores conectados hay que añadirlos en la pestaña **Modules list**.

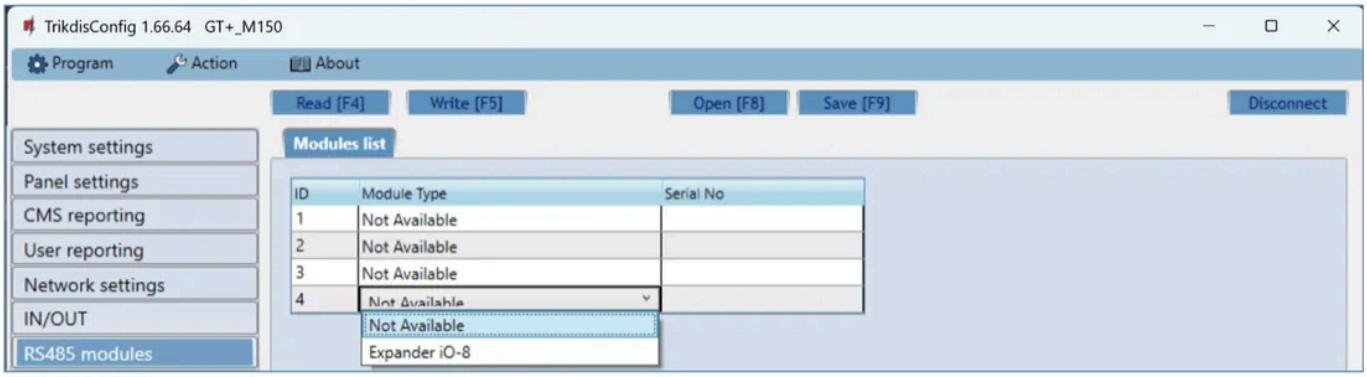


Figura 53. TrikdisConfig – RS485 modules, pestaña Modules list: en la posición 4, la lista Module type (Not Available, Expander iO-8).

- **Module type** – el tipo de módulo conectado al bus, de la lista (**Expander iO-8**).
- **Serial No** – el número de serie de 6 dígitos del módulo (en la caja del módulo y en la pegatina del embalaje).

Después de elegir el módulo e introducir el número de serie, ve a la pestaña **RS485 modules** → **Module**: para el módulo añadido aparece una pestaña propia, numerada (Module 1 …), con sus ajustes.

Expansor iO-8 – 8 bornes de E/S de doble función; al comunicador se pueden conectar hasta cuatro iO-8.

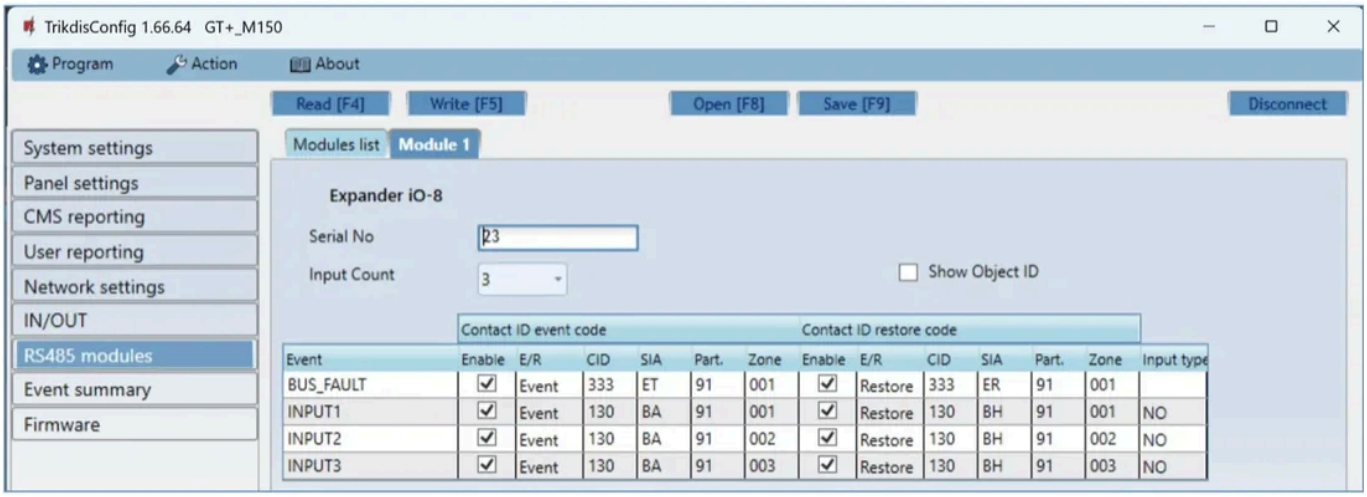


Figura 54. TrikdisConfig – RS485 modules, pestaña Module 1 (iO-8): Input Count, Show Object ID y los eventos BUS_FAULT, INPUT1–INPUT3 con código CID y SIA, con la partición 91.

- **Input Count** – cuántos bornes serán entradas (IN); el resto serán salidas (OUT). La función de las salidas (armado / desarmado o accionamiento de un dispositivo) se configura directamente en la aplicación Protegus 2.
- En la tabla puedes asignar un código de evento y de restauración al fallo del bus (**BUS_FAULT**, Contact ID 333) y a las entradas (**INPUTx**, 130); cuando se activa la entrada, el comunicador envía un evento con el código configurado al receptor de la CRA y a Protegus 2. Columnas de las filas de evento (Contact ID event code) y de restauración (Contact ID restore code): **Enable** (activación), **E/R** (Event o Restore), **CID** (código Contact ID), **SIA** (código SIA), **Part.** (la partición; depende automáticamente del número del módulo: 91 en el módulo 1, 94 en el módulo 4), **Zone** (el número de zona).
- **Object ID** – para la entrada también se puede indicar un identificador de abonado distinto del del comunicador (la columna aparece al marcar **Show Object ID**).
- **Input type** – el tipo de entrada: NO, NC o EOL.

6.9 Event summary

En esta página puedes activar o desactivar los **mensajes internos propios** del dispositivo y modificar su código Contact ID y sus números de partición y de zona. Un mensaje desactivado aquí no lo envía el dispositivo por ningún canal. De fábrica, los mensajes se envían con la partición 99 y la zona 999.

Mensaje	Contact ID	Cuándo se genera
COMMUNICATION	350	Se ha interrumpido la comunicación entre el comunicador y la central de alarma (desactivado de fábrica). El comunicador conectado al bus o al puerto serie lo detecta directamente; el comunicador de línea telefónica, solo con **Line supervision** activado.
POWER	302	Tensión de alimentación inadecuada (baja); su restablecimiento es un mensaje aparte.
REMOTE_STARTED	411	Ha comenzado una programación remota con TrikdisConfig.
REMOTE_FINISHED	412	La programación remota ha terminado.
START	700	El dispositivo se ha conectado a la red (arranque).
TEST	602	Informe de prueba periódico.

Mensaje	Contact ID	Cuándo se genera
PING	760	El mensaje de señal de vida PING. No figura en la lista de todos los dispositivos: en la pantalla de la versión de hardware anterior sí, pero en la página Event summary de las versiones más nuevas no hay esta fila. Su intervalo se ajusta en el campo **CMS reporting → Settings → IP ping period**.

- **Enable** – habilita el envío del mensaje a la CRA y a Protegus 2.
- **E/R** – tipo de mensaje: Event (evento) o Restore (restablecimiento); la fila indica que el evento se ha producido o que se ha restablecido.
- **Part.** – número de partición (área) que envía el dispositivo con el evento interno y con el restablecimiento.
- **Zone** – número de zona que envía el dispositivo con el evento interno y con el restablecimiento.
- El código **CID**, la **partición** y la **zona** se pueden cambiar en cualquier evento; donde hay restablecimiento (Restore), su código se puede indicar por separado.

Los eventos de las entradas propias (**INx_ALARM**, **INx_TAMPER**) se configuran en la página **IN/OUT**, y los eventos de los módulos de ampliación (**BUS_FAULT**, **INPUTx**), en la página **RS485 modules**, en la pestaña del módulo. La habilitación y el intervalo del informe de prueba se ajustan en el campo **CMS reporting → Settings → Test period**.

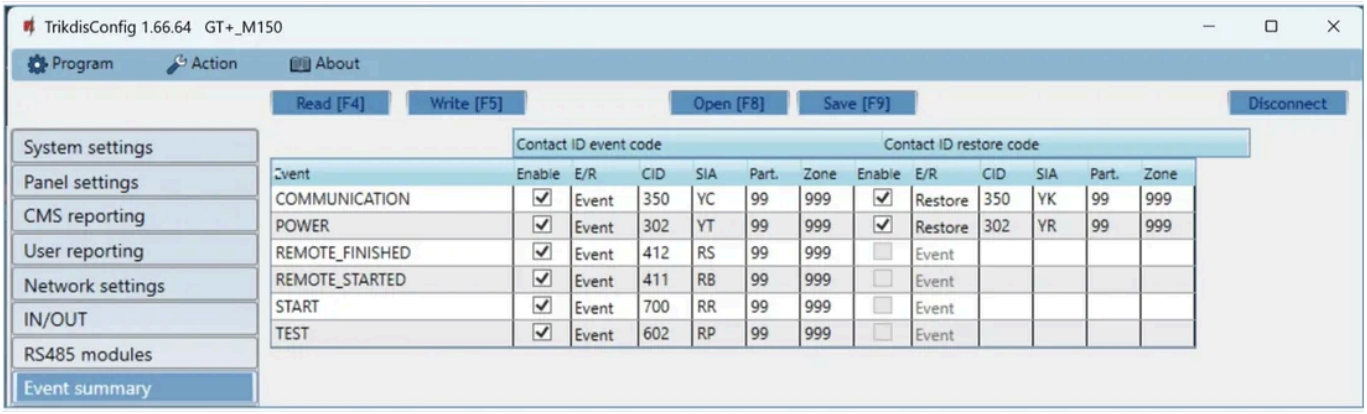


Figura 55. TrikdisConfig – página Event summary: los mensajes internos del equipo con código CID y SIA (COMMUNICATION 350, POWER 302, REMOTE_FINISHED 412, REMOTE_STARTED 411, START 700, TEST 602).

En la lista del GT y del GT+ figuran los mensajes **COMMUNICATION**, **POWER**, **REMOTE_FINISHED**, **REMOTE_STARTED**, **START** y **TEST**, cada uno también con su código SIA. El mensaje COMMUNICATION indica un fallo de la conexión entre la central y el comunicador: con la conexión al bus de datos o serie, el comunicador lo detecta directamente (el LED TROUBLE da 7 destellos).

6.10 Restablecer los ajustes de fábrica

Para restablecer los ajustes 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 todos los ajustes –también las contraseñas–, así que conviene guardar antes la configuración en un archivo (**Save [F9]**).

Con la contraseña de instalador solo es posible si el administrador no lo ha bloqueado en la página **System settings → Access**.



Figura 56. TrikdisConfig – el botón Restore del grupo Default settings.

Los ajustes de fábrica también se pueden restablecer en el propio equipo, sin ordenador: con la alimentación encendida, pulsa y mantén pulsado el botón **RESET** de la placa de circuito impreso (apartado 1.4) **durante 10 segundos**, hasta que se apaguen los LED NETWORK, POWER y TROUBLE y después se encienda el LED POWER. Entonces suelta el botón: los ajustes de fábrica se han restablecido.

7. Programación a distancia

TrikdisConfig accede a los dispositivos Trikdis no solo por cable USB, sino también **a distancia, a través de la nube Protegus**. Así puedes modificar los ajustes de un dispositivo ya instalado sin tener que desplazarte al lugar.

Para el acceso remoto se necesita:

1. El dispositivo debe estar encendido y tener conexión de red (los LED **POWER** y **NETWORK** se iluminan en verde; en un dispositivo de red móvil, el NETWORK también parpadea en amarillo). En un dispositivo de red móvil, la tarjeta SIM insertada debe estar activa y su código PIN debe estar indicado en el dispositivo, o la petición de PIN debe estar desactivada; en un dispositivo Ethernet, el cable de red (LAN) debe estar enchufado y el dispositivo debe tener salida a Internet.
2. En la página **User reporting** → **PROTEGUS Cloud** de TrikdisConfig debe estar marcado **Enable connection** (configúralo por USB, en la primera puesta en marcha).
3. Debes conocer el **identificador único** del dispositivo (IMEI o MAC, que figura en la caja y en la parte trasera del dispositivo) y la contraseña de administrador o de instalador.

Pasos:

1. Inicia el software TrikdisConfig.
2. En la sección **Remote access**, escribe en el campo **Unique ID** el identificador único del dispositivo (IMEI o MAC).
3. Si quieres, da un nombre al sistema en el campo **System name**: el programa lo recuerda y la próxima vez podrás elegirlo de la lista desplegable.
4. Pulsa el botón **Configure**.
5. En la ventana que se abre, haz clic en el botón **Read [F4]** (leer) e introduce la contraseña. Con la casilla **Remember password**, el programa la recuerda durante esta sesión.
6. Haz los cambios y luego envíalos al dispositivo con el botón **Write [F5]** (escribir).

El programa guarda los sistemas programados antes a distancia que tienen nombre; puedes listarlos con la flecha junto al campo **System name**. Para borrar uno, selecciona el identificador en la lista, pulsa la tecla **Delete** y confírmalo.

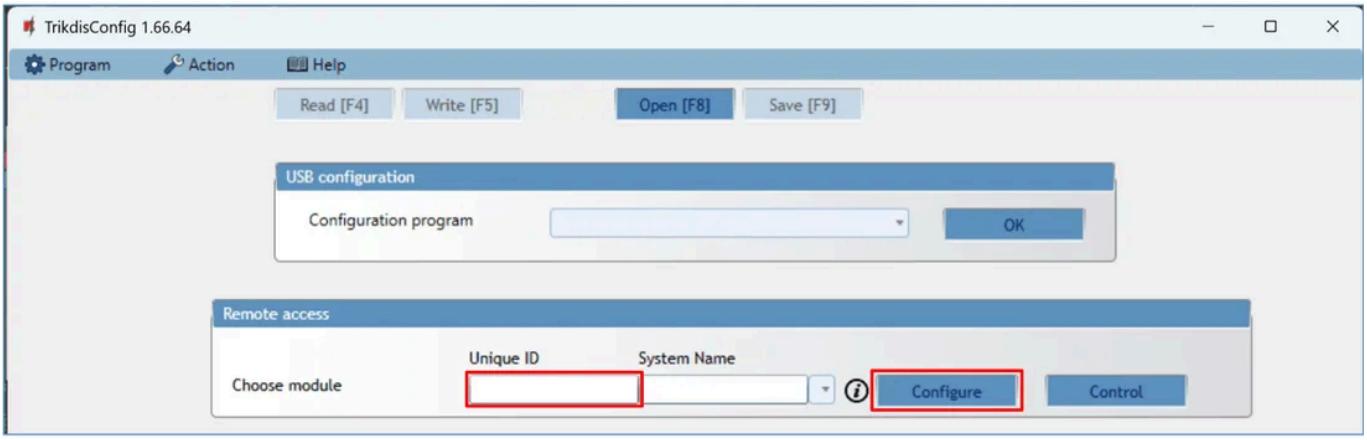


Figura 57. TrikdisConfig – el grupo Remote access: el campo Unique ID, la lista System name y el botón Configure.

El identificador único del GT y del GT+ es el **IMEI**; se puede leer en la etiqueta del equipo y en la pegatina de la caja. Para el acceso a distancia, la tarjeta SIM debe estar activa, con su código PIN introducido o la petición de PIN desactivada; en la página **User reporting** → **PROTEGUS Cloud** debe estar marcada la opción **Enable connection** (apartado 6.5); el LED **POWER** debe estar encendido en verde, y el LED **NETWORK**, encendido en verde y parpadeando en amarillo.

8. Comprobación del funcionamiento del comunicador

Después de la programación y el cableado, comprueba siempre toda la cadena: central de alarma → comunicador → CRA y/o Protegus 2.

Antes, mira si hay alimentación (el LED **POWER** se ilumina en verde) y si hay conexión de red (el LED **NETWORK** se ilumina en verde).

1. **Provoca un evento.** Arma y luego desarma el sistema desde el teclado o, con el sistema armado, viola una zona para que se produzca una alarma.
2. **Comprueba la recepción.** Mira si el evento ha aparecido en el software de la CRA y/o en la lista de eventos de la aplicación Protegus 2, con el número de partición y de zona correctos.
3. **Entradas.** Activa el detector conectado a una entrada propia del comunicador y comprueba el evento correspondiente.
4. **Salidas.** Activa la salida desde la aplicación Protegus 2 y comprueba que el dispositivo conectado (relé, zona de interruptor de llave) realmente se acciona.
5. **Armado remoto.** Si la central se puede controlar a distancia, ármala y desármala también desde la aplicación Protegus 2.
6. **Central DSC con conexión Keybus + TIP/RING (GT+).** Arma el sistema y provoca una alarma en una zona de incendio. La CRA debe recibir el evento con el código Contact ID que corresponde al tipo de zona (por ejemplo, E110 – alarma de incendio), no como alarma genérica (E130).

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!

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.

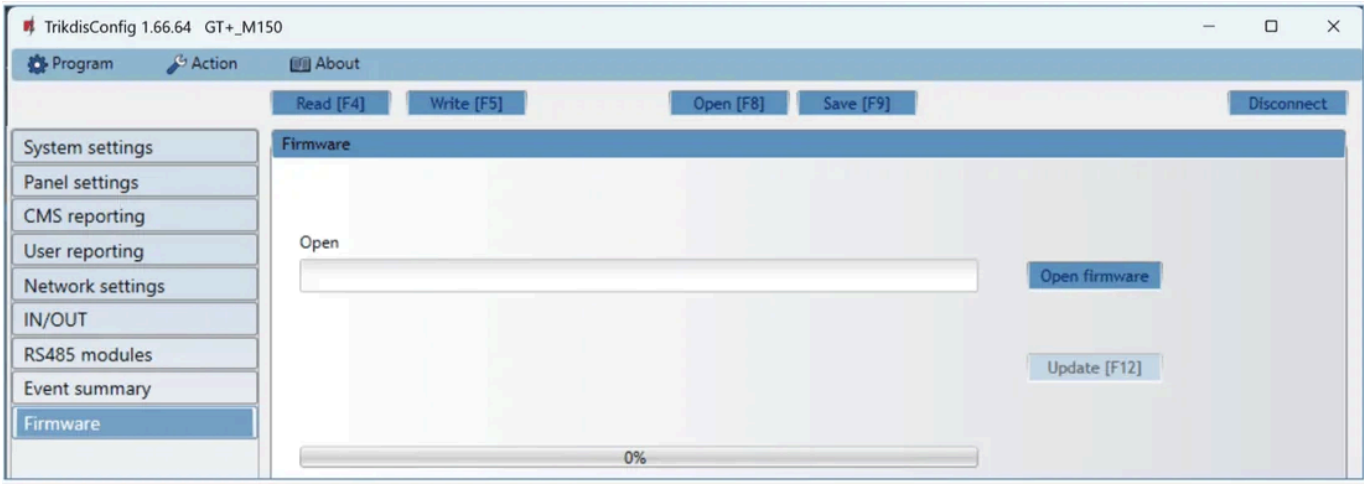


Figura 58. TrikdisConfig – página Firmware: botón Open firmware, botón Update [F12] y la barra de progreso.

Para la actualización hace falta conexión a internet. Un antivirus, un cortafuegos o una configuración estricta del acceso a internet pueden impedir la actualización automática del firmware; en ese caso hay que modificar los ajustes del antivirus. Para la conexión Keybus + TIP/RING de Paradox SP / SP+ / MG / MG+ (apartado 3.3.4) hace falta como mínimo el firmware 1.21.

10. Búsqueda de averías y preguntas frecuentes

Las preguntas y averías más frecuentes, partiendo de las indicaciones LED. Si la respuesta remite al capítulo detallado, allí encuentras el lugar exacto del ajuste.

El LED NETWORK no se enciende – no hay red

1. Mira los destellos del LED **TROUBLE**: 1 = no hay SIM, 2 = PIN incorrecto, 3 = no hay APN, 4 = no puede registrarse en la red móvil, 5 = no puede conectarse a la red de datos (apartado 1.6).
2. Comprueba que la tarjeta SIM está activa, tiene servicio de datos y está bien colocada en la ranura.
3. Si la petición de PIN está activada en la tarjeta, introduce el PIN en la pestaña **Network settings** → **SIM1**, o desactiva la petición de PIN con un teléfono.
4. Comprueba el APN (apartado 2.2): con una tarjeta IoT / M2M, el operador da un APN aparte.
5. Comprueba la antena: está enroscada, no está dentro de una caja metálica y el nivel de señal es adecuado (el LED NETWORK da al menos 3 destellos amarillos; apartados 1.6 y 3.2).

Hay red, pero la CRA no recibe eventos

El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del operador; en uno Ethernet, que la conexión hasta el router funciona–, pero no que el dispositivo también salga a Internet. Si el LED NETWORK está en verde, pero el LED DATA sigue encendido de forma continua tras un evento o un informe de prueba, la conexión a Internet no funciona: el mensaje no puede salir. En red móvil lo más habitual es que fallen el APN o el servicio de datos de la tarjeta SIM; en Ethernet, el router, el cortafuegos o el DNS. Si el LED DATA se apaga, el mensaje se ha enviado y la conexión de datos está bien.

1. Los 6 destellos del LED **TROUBLE** indican que no hay conexión con el receptor: comprueba la dirección del receptor, el puerto, el ajuste TCP/UDP, el protocolo y la clave de cifrado (**CMS reporting**).
2. Si el receptor está introducido con un nombre de dominio, comprueba el ajuste DNS (**Network settings** → **SIM1** → **DNS 1, DNS 2**).
3. Comprueba que el plan de datos de la tarjeta SIM no bloquea el puerto necesario (algunas tarjetas M2M solo permiten determinadas direcciones).

El LED TROUBLE da 7 destellos – no hay conexión con la central

1. Con la conexión al bus de datos o serie, comprueba los hilos CLK y DATA, y que en el campo **Panel settings** → **Security panel model** está seleccionado el modelo de la central conectada (apartado 6.3).
2. En una central Paradox, comprueba que el puerto serie no está bloqueado (apartado 4.1.2); en las centrales Texecom y Paradox, la **Security panel PC download password** debe coincidir con la configurada en la central.
3. Con la conexión por línea telefónica, el marcador de la central debe estar activado, en modo DTMF, con formato Contact ID y con un número de teléfono introducido (apartado 4.2), y el **Communication protocol** debe ser AUTO (GT: Dual tone).

El LED TROUBLE da 8 destellos – ICCID distinto

El número introducido en el campo **Network settings** → **SIM1** → **SIM ICCID** no coincide con el ICCID de la tarjeta SIM colocada: el equipo solo funciona con la tarjeta indicada. Vuelve a poner la tarjeta original, o cambia (borra) el ICCID; con **Hard ICCID lock**, después del cambio reinicia el equipo (apartado 6.6).

DSC: todas las alarmas llegan como alarma genérica E130

Conectado solo al Keybus, el comunicador recibe de la central el estado de las zonas, pero no el tipo de zona; por eso transmite todas las alarmas con el código E130 (apartado 3.3.1). Si la CRA espera el código que corresponde al tipo de zona (por ejemplo, incendio: E110): conecta el **GT+**, además de al Keybus, también a los bornes TIP/RING, y programa el marcador de la central (apartados 3.3.2 y 4.1.1). En el GT no existe esta conexión doble; allí los códigos propios de la central se envían con el marcador de la central, solo con conexión TIP/RING, pero entonces no hay control directo y para el armado hace falta una zona de llave (apartado 3.4).

Paradox: el puerto serie está bloqueado, o no hay conexión

En las centrales Paradox más nuevas (SP+, MG+, EVOHD+) el puerto serie puede venir bloqueado de fábrica; el desbloqueo se explica en el apartado 4.1.2 y en el artículo Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox. En las centrales Spectra SP / SP+ y Magellan MG / MG+, en lugar del puerto serie también se puede usar la conexión Keybus + TIP/RING (apartado 3.3.4), que no necesita desbloqueo, pero el firmware del comunicador debe ser como mínimo el 1.21 (capítulo 9).

No puedo armar desde Protegus 2

1. Con el control directo, la opción **Panel settings** → **Remote Arm/Disarm** debe estar marcada, y la central debe estar configurada según el apartado 4.1 (Paradox: contraseña de PC, firmware V.4 o superior; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: los ajustes descritos). En la tabla del apartado 1.3, comprueba si la central es de control directo.
2. Con el armado por zona de llave (apartado 3.4), el borne debe estar en **OUT** en la página **IN/OUT**, la zona de la central debe ser una zona de llave, y en Protegus 2 la salida debe estar asignada a la partición, en el mismo modo que en la central (de impulso o de dos posiciones; apartado 5.2).
3. Protegus 2 muestra el estado de la partición a partir de los eventos de armado y desarmado de la central: la central debe transmitirlos (Opening/Closing).

Protegus 2 no ve el equipo

1. En la página **User reporting** → **PROTEGUS Cloud** debe estar marcada la opción **Enable connection**.
2. Al añadirlo, hay que introducir el **PROTEGUS Cloud access Code** configurado en el equipo; si cambiaste el código en TrikdisConfig, cámbialo también en la aplicación.
3. Escribe el IMEI exactamente, desde la etiqueta del equipo o la pegatina de la caja (o escanea el código QR).
4. El servicio de datos de la tarjeta SIM y el APN deben estar correctos (el LED NETWORK está en verde, y el LED DATA se apaga después de un evento).

No puedo entrar a distancia con TrikdisConfig

1. El equipo debe estar en línea (LED NETWORK en verde, parpadeando en amarillo) y la conexión Protegus debe estar activada (**Enable connection**).
2. El **CMS reporting** → **Settings** → **IP ping period** no debe ser superior a 5 minutos: el PING mantiene la conexión necesaria para el acceso a distancia.
3. Comprueba la contraseña de administrador o de instalador.

He olvidado la contraseña

Con TrikdisConfig no se puede, porque el restablecimiento también requiere contraseña. Sí se puede con el botón **RESET** del equipo (apartado 6.10): con la alimentación conectada, mantenlo pulsado 10 segundos. Se borran todos los ajustes.

¿GT o GT+? ¿Cuál necesito?

La conexión, la configuración y el funcionamiento de las dos versiones son iguales; las diferencias se resumen en la tabla del apartado 1.2. El GT+ también funciona con una alimentación de 10–32 V DC (también en sistemas de 24 V) y, en las centrales DSC, también admite la conexión Keybus + TIP/RING, así que los eventos se envían con los códigos Contact ID propios de la central. Si no necesitas esto, el GT hace lo mismo.

¿Cuánto tráfico de datos usa el equipo?

Los mensajes de eventos y los PING son muy pequeños; el tráfico depende sobre todo del periodo de PING y de la frecuencia de los informes de prueba. En un sistema doméstico medio, el tráfico mensual suele quedar por debajo de 10 MB. El valor exacto depende de los ajustes y de la unidad de facturación del operador; por eso, con una tarjeta con límite de datos, conviene comprobar el tráfico del primer mes.

11. 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.

- La instalación y el mantenimiento de los equipos de seguridad solo los puede realizar un instalador cualificado.
- Antes de la instalación, lee el manual; no seguir las instrucciones puede provocar un funcionamiento incorrecto o una avería del equipo.
- Antes de la conexión, en cada conexión eléctrica y antes de cualquier reparación, desconecta el equipo de la alimentación.
- Las modificaciones, transformaciones y reparaciones no autorizadas por el fabricante anulan la garantía.
- Respeta las normas locales de gestión de residuos: no tires el equipo inservible ni sus piezas a la basura doméstica. El símbolo del contenedor de basura tachado (RAEE) en el equipo indica que hay que entregarlo por separado como residuo electrónico.

Ver también

- Buscador de compatibilidad: qué comunicador Trikdis y qué conexión corresponde a tu central de alarma.
- Comunicador Trikdis + central de alarma DSC: guía rápida de instalación: los pasos de la conexión DSC, en resumen.
- Comunicador Trikdis + central de alarma Paradox: guía rápida de instalación: los pasos de la conexión Paradox, en resumen.
- DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones: por qué la NEO no se puede conectar al bus de datos y cuál es la solución.
- Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox: desbloqueo del puerto serie de las centrales SP+, MG+ y EVOHD+.
- Armado a distancia con zona de llave desde la aplicación Protegus 2: los detalles y las trampas del armado con zona de llave.
- Configuración del APN – lista de operadores móviles europeos: los APN de los operadores, también para tarjetas IoT / M2M.
- Documentación en inglés: docs.trikdis.com; en la página del GT y del GT+ también está la tabla de conversión de códigos Contact ID → SIA (anexo).

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

Productos relacionados

Trikdis GT 4G comunicador inteligente | **Trikdis GT+ 4G comunicador inteligente**

Trikdis iO8 módulo expansor cableado

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-gt