mobilamb
TRIKDIS Official Distributor

Comunicador GET – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Trikdis GET Ethernet + 4G: conexión a la central de alarma, configuración de LAN y SIM en TrikdisConfig, transmisión a la CRA y la aplicación Protegus 2.



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

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Versiones: GET, 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

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 Colocación en la caja de la central, antena
3.3 Conexión a la central de alarma
3.3.1 DSC – bus de datos (Keybus)
3.3.2 Paradox – puerto serie
3.3.3 Paradox SP/MG – Keybus y TIP/RING
3.3.4 UTC Interlogix (Caddx) – bus de datos
3.3.5 Texecom – puerto serie
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – bus de datos
3.3.9 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 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 Honeywell Vista
4.2.2 Marcador de 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

6. La configuración en detalle

6.1 Conexión con el comunicador

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Canales del receptor (CMS settings)

6.4.2 Test, PING y orden de las conexiones

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 y SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Restablecer la configuración 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 GET es el **comunicador Ethernet + 4G** de Trikdis: transmite los eventos de la central de alarma por la red local cableada (LAN) o por la red móvil a la CRA y a la aplicación Protegus 2. Se puede 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 comunicador telefónico de cualquier central** (TIP/RING) que envíe los eventos en formato Contact ID con tonos DTMF. El comunicador transmite a la CRA toda la información 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 el comunicador GET con módem LTE (4G); las diferencias entre el GET, el GT y el GT+ 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, a través de la red cableada o de la red móvil, al receptor por software o por 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). Hacia un receptor SUR-GARD convierte los códigos Contact ID recibidos de la central en códigos SIA; la tabla de conversión está en el anexo de la documentación en inglés de docs.trikdis.com. Comprueba la conexión con el receptor cada 30 segundos (o con el intervalo configurado) mediante un mensaje PING; si el canal principal se interrumpe, pasa al canal de respaldo. Con un canal paralelo, los eventos van a la vez a dos receptores. El orden de las vías de conexión –LAN, SIM1, SIM2– lo puedes fijar tú: si la vía principal no funciona, el comunicador pasa a la vía de respaldo (apartado 6.4.2). 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 equipos conectados (iluminación, puerta, ventilación, calefacción, riego, etc.). En la aplicación, los permisos del administrador, del instalador y del usuario son distintos. El GET no envía avisos por SMS ni por llamada: los avisos llegan a través de la aplicación Protegus 2.
- **Controla la central directamente.** Conectado al bus de datos o al puerto serie, el comunicador también ve los estados de las particiones y de las 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.
- **Tiene entradas y salidas propias.** Dos bornes I/O de doble función se pueden usar como entrada (IN) o como salida controlable (OUT); de fábrica, los dos son salidas. Las salidas se accionan desde la aplicación Protegus 2. Los bornes **A 485** y **B 485** no se usan en el GET; al GET no se puede conectar ningún módulo de ampliación RS485.
- **Se configura con dos herramientas.** La configuración se puede hacer con el programa TrikdisConfig para Windows (con cable USB-C o a distancia) y –con firmware 1.08 o posterior– también desde la aplicación Protegus 2 (Settings → Advanced settings). 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 se puede configurar a distancia, y su firmware también se puede actualizar a distancia.

La estructura del sistema se ve en la figura siguiente: la central de alarma se conecta al comunicador; el comunicador llega a internet de dos maneras –por la red móvil (LTE) o a través del router (LAN)– 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.

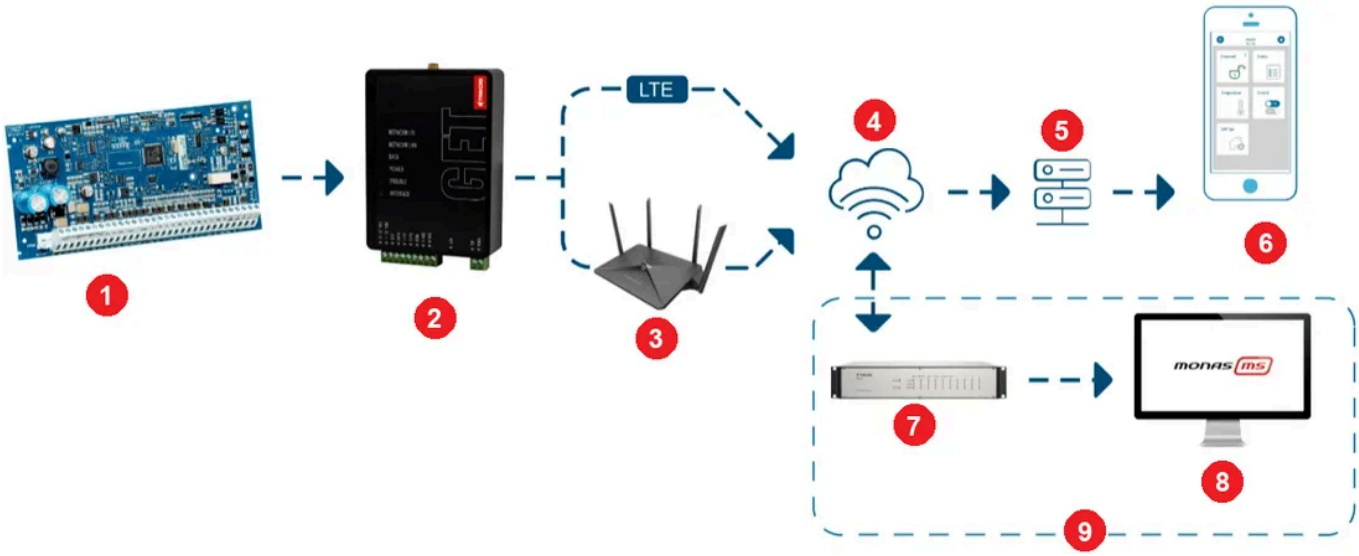


Figura 1. El lugar del comunicador en el sistema: central de alarma → GET → red móvil (LTE) o router (LAN) → internet → receptor de la CRA y servidor de Protegus → aplicación Protegus 2.

- 1 central de alarma («Alarm panel»)
- 2 comunicador LTE GET («LTE communicator»)
- 3 router («Router»)
- 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 la CRA («Monitoring software»)
- 9 la central receptora de la empresa de seguridad («Monitoring station in security company»), en el marco discontinuo

1.2 Versiones: GET, GT y GT+

El GET es el hermano con puerto Ethernet de los comunicadores GT y GT+: la conexión y la programación de la central de alarma, la gama de centrales compatibles, el módem, los protocolos de transmisión y el uso de Protegus 2 son iguales, por eso los manuales de los tres comunicadores tienen también el mismo orden de capítulos. Las diferencias se resumen en la tabla siguiente.

	GET	**GT**	**GT+**
Conexión de red	**LTE (4G) y Ethernet (LAN, RJ45)**; el orden de las vías de conexión se puede fijar (Main / Backup / Backup 2: LAN, SIM1, SIM2; apartado 6.4.2)	LTE (4G)	LTE (4G)
Tarjeta SIM	**2 ranuras nano-SIM** (SIM1, SIM2); se pueden poner una o dos tarjetas	1 nano-SIM	1 nano-SIM
Tensión de alimentación	10–18 V DC	10–18 V DC	10–32 V DC
Consumo	como máximo 100 mA en reposo, 300 mA durante el envío de datos	como máximo 100 / 200 mA	como máximo 100 / 200 mA
Tamaño, peso	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g

	GET	**GT**	**GT+**
Bornes	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; toma **LAN** (RJ45) aparte y TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Configuración de fábrica de los bornes I/O	salida (OUT)	entrada (IN, NO)	entrada (IN, NO)
Bus RS485, ampliación iO-8	los bornes A 485 / B 485 **no se usan**; no se puede conectar ninguna ampliación	como máximo 4 iO-8	como máximo 4 iO-8
LED	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (no se usa)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
Destellos del LED TROUBLE	1 = conexión física LAN (cable), 2 = fallo de la SIM1, 3 = fallo de la SIM2, 7 = central	1–8 (SIM, PIN, APN, red, receptor, central, ICCID)	1–8
SMS y llamada	sin avisos por SMS, sin comandos SMS y sin llamadas: los avisos y el control se hacen desde Protegus 2	avisos por SMS y por llamada, comandos SMS	avisos por SMS y por llamada, comandos SMS
Central DSC en el bus de datos y en los bornes TIP/RING a la vez	no	no	sí
Ajuste de la conexión TIP/RING (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (también se puede elegir **3. MANUAL**)
Configuración desde la aplicación Protegus 2	sí (Advanced settings, desde el firmware 1.08)	TrikdisConfig	TrikdisConfig
Memoria de eventos	60 eventos	sin datos	sin datos
Mensajes internos (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	como el GT
Módem, protocolos de transmisión (TRK8, DC-09, TL150), cifrado, centrales compatibles, esquemas de conexión, Protegus 2	iguales	iguales	iguales

Los tres comunicadores se fabrican con los mismos tres tipos de módem; para el mercado europeo la versión adecuada es la 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 equipo.

Módem	**Red y bandas de frecuencia**
EG915U-EU (Europa)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8

Módem	Red y bandas de frecuencia
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 al comunicador directamente, por el bus de datos o por el puerto serie. La columna «control directo» indica si el usuario puede armar y desarmar desde Protegus 2 con su propio código de teclado sin ninguna conexión adicional; donde esto 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, PC5020	bus de datos (Keybus)	sí
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)	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 de por el 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, pero el firmware del comunicador debe ser como mínimo 1.21 (apartado 3.3.3).
- La central de **cualquier otro fabricante** se conecta a través de su comunicador telefónico (TIP/RING), si 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 van con tu central lo puedes consultar en el buscador de compatibilidad.

1.4 Partes del comunicador

El 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. La toma LAN y el borne TIP/RING se encuentran en el lateral de la caja, en una abertura aparte.

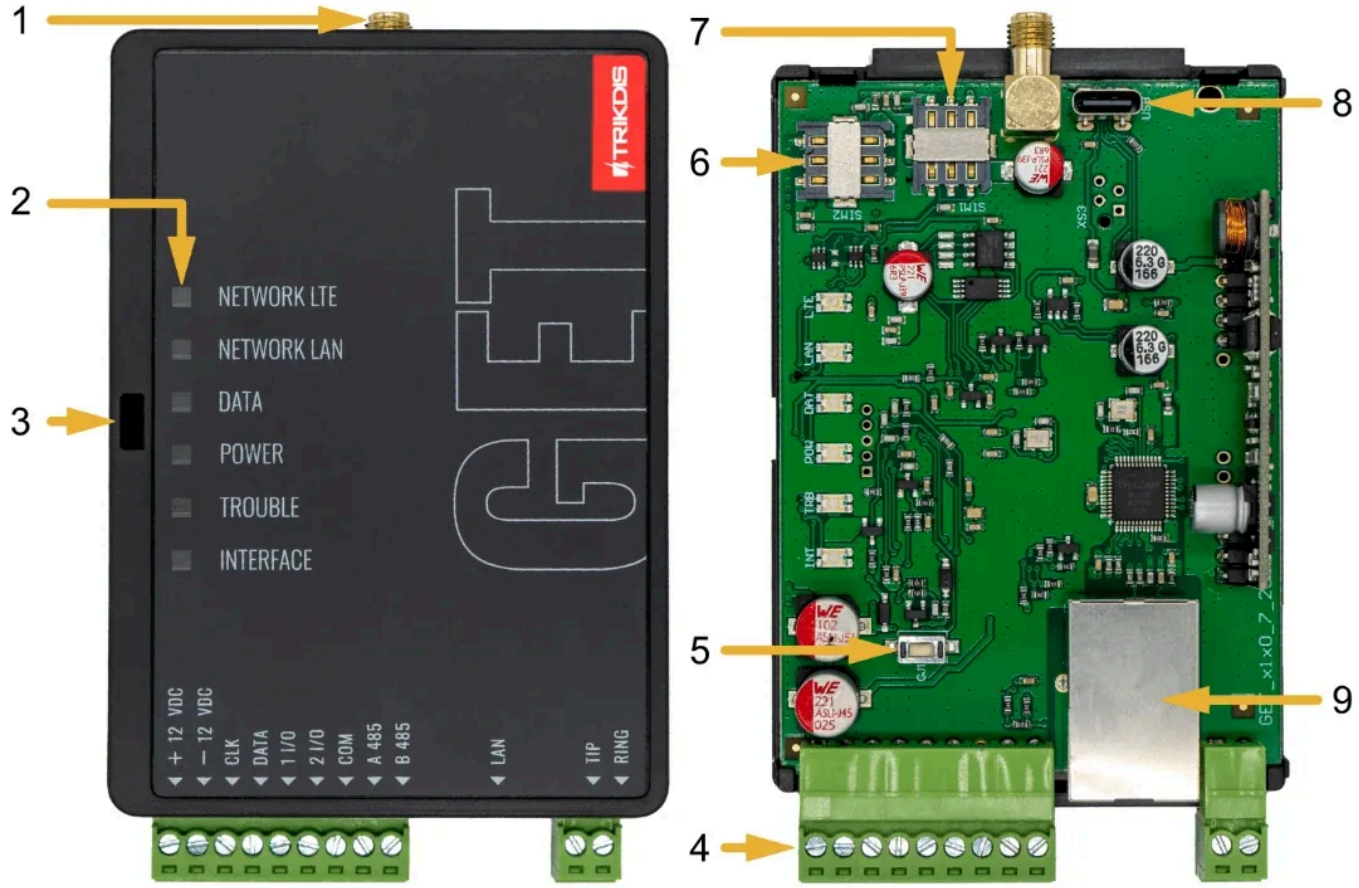


Figura 2. Partes del comunicador por delante (izquierda) y con la caja abierta (derecha).

- 1 Conector SMA de la antena móvil
- 2 Indicadores LED (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Abertura que ayuda a quitar la tapa frontal
- 4 Regleta de bornes extraíble para las conexiones externas
- 5 Botón RESET
- 6 Ranura de la tarjeta SIM2
- 7 Ranura de la tarjeta SIM1
- 8 Toma USB-C para la programación
- 9 Toma Ethernet (LAN) RJ45

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

1.5 Bornes

Borne	Función
+12 VDC	Alimentación, positivo: +10–18 V DC
–12 VDC	Alimentación, 0 V
CLK	Bus serie o bus de datos (reloj) para la conexión directa de la central

Borne	Función
DATA	Bus serie o bus de datos (datos) para la conexión directa de la central
1 I/O	Entrada/salida 1 (configuración de fábrica: salida, OUT)
2 I/O	Entrada/salida 2 (configuración de fábrica: salida, OUT)
COM	Punto común (negativo) para las entradas y las salidas
A 485	No se usa
B 485	No se usa (la pareja de A 485)
LAN	Toma RJ45 Ethernet (red local)
TIP	Borne TIP del comunicador telefónico de la central de alarma
RING	Borne RING del comunicador telefónico de la central de alarma

En los esquemas de conexión, los bornes de alimentación se indican con **+DC** y **–DC** (en el equipo, +12 VDC / −12 VDC), y los bornes RS485 con **A RS485** / **B RS485** (en el equipo, A 485 / B 485). La rotulación 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. Léelos en conjunto: POWER indica la alimentación, NETWORK LTE la red móvil, NETWORK LAN la red cableada y TROUBLE los fallos; el LED INTERFACE no tiene función en el GET.

NETWORK LTE – conexión a la red móvil

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

NETWORK LAN – conexión a la red cableada

Indicación	Significado
apagado	No hay conexión con la red informática
verde fijo	Conectado a la red informática

DATA – tráfico de datos

Indicación	Significado
apagado	No hay eventos pendientes de envío
verde fijo	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
verde fijo	Encendido, la tensión de alimentación es correcta
amarillo fijo	Tensión de alimentación incorrecta (11,5 V como máximo)
verde fijo, parpadea en amarillo	Listo para la programación (durante la programación)
amarillo fijo (durante la programación)	No hay conexión con el ordenador

TROUBLE – fallo

Indicación	Significado
apagado	No hay fallos
1 destello rojo	Fallo en la conexión física de la red cableada (PHY Link): comprueba el cable LAN
2 destellos rojos	Fallo de la tarjeta SIM1
3 destellos rojos	Fallo de la tarjeta SIM2
7 destellos rojos	Se ha interrumpido la conexión con la central de alarma (bus serie)

INTERFACE – no se usa en el GET.

1.7 Datos técnicos

Parámetro	Valor
Conexión de red	LTE (4G) y Ethernet (LAN)
Conexión con la central de alarma	bus serie, bus de datos (Keybus) o línea telefónica (TIP/RING, Contact ID, DTMF)
Entradas/salidas	2 I/O 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
Módem	EG915U-EU (Europa), EG915U-LA (Latinoamérica) o BG95-M5 (LTE Cat M1); las bandas de frecuencia figuran en la tabla del apartado 1.2
Tarjeta SIM	2 ranuras nano-SIM (SIM1, SIM2)
Tensión de alimentación	10–18 V DC
Consumo	como máximo 100 mA en reposo; como máximo 300 mA durante el envío de datos

Parámetro	Valor
Protocolos de transmisión	TRK8, DC-09_2007, DC-09_2012, TL150
Cifrado	AES-128
Memoria de eventos	60 eventos
Programación	TrikdisConfig (Windows) con cable USB-C o a distancia; aplicación Protegus 2 (desde el firmware 1.08)
Entorno de funcionamiento	−10 … +50 °C, humedad relativa máx. 80 % (a +20 °C)
Tamaño	113 × 70 × 25 mm
Peso	110 g

2. Puesta en marcha rápida

La configuración del comunicador se puede hacer con dos herramientas: con el programa **TrikdisConfig** para Windows –con cable USB-C o a distancia– y desde la **aplicación Protegus 2** (Settings → Advanced settings). En este capítulo describimos el camino más corto: 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. Para cada paso indicamos la ruta tanto en la aplicación como en TrikdisConfig; la explicación detallada de los ajustes está en el capítulo 6.

2.1 Preparativos

Qué vas a necesitar

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 (una o dos; la petición de PIN se puede desactivar), si usas la red móvil · cable Ethernet hasta el router o el switch, si usas la red cableada · el manual de instalación de la central de alarma.

Los accesorios necesarios se piden por separado al distribuidor.

Configuración con TrikdisConfig. El equipo se configura sobre la mesa, antes de conectarlo; después, en la instalación, solo queda conectarlo.

1. Descarga e instala el software TrikdisConfig. En la web de Trikdis (www.trikdis.com), escribe en el buscador: «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: mete el destornillador arriba, en la ranura junto a la antena, y haz palanca hacia fuera, y luego abajo, en la abertura, hacia abajo. La figura muestra también dónde está la toma USB-C, en el borde del circuito impreso.

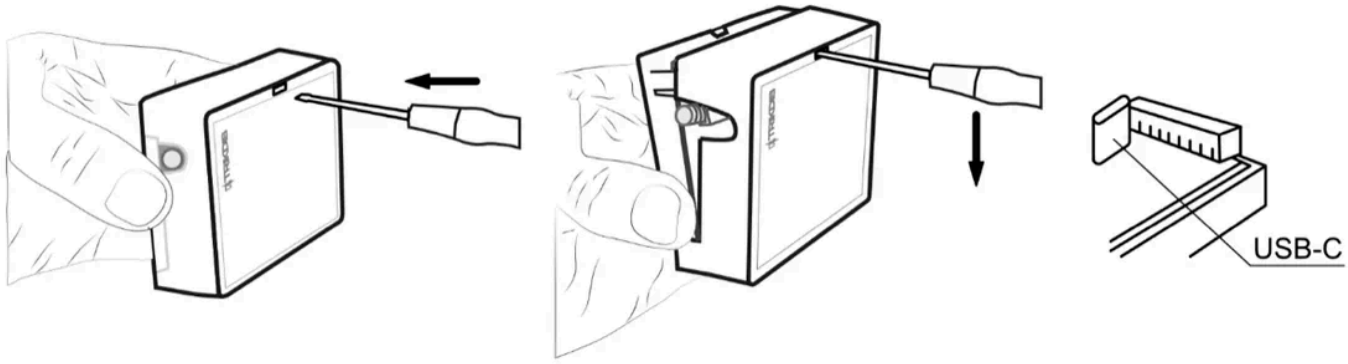


Figura 3. Cómo quitar la tapa frontal con un destornillador plano; el detalle ampliado muestra el lugar de la toma USB-C.

3. Coloca la tarjeta nano-SIM (o las tarjetas) en la ranura, en el sentido que muestra la figura: la ranura SIM1 está en el centro del circuito impreso y la SIM2 en el borde. La tarjeta debe estar activa y tener servicio de datos móviles; si puedes, desactiva la petición de PIN en un teléfono (así no tendrás que escribir el PIN en el equipo). Si usas el comunicador solo en la red cableada, no hace falta tarjeta SIM.

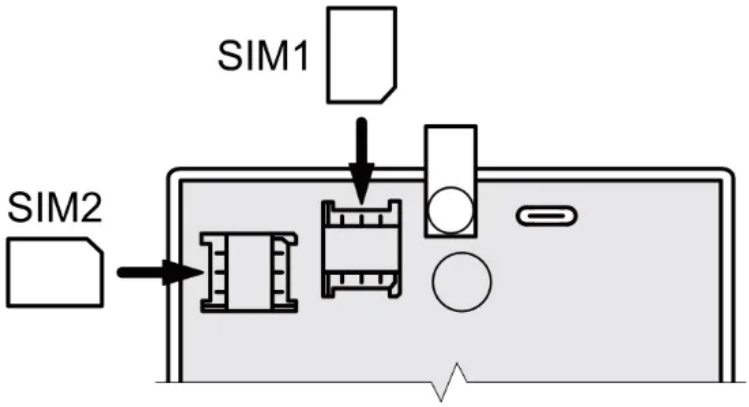


Figura 4. El lugar de las ranuras SIM1 y SIM2 en el circuito impreso; las flechas indican el sentido en que se introduce la tarjeta.

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 la configuración actual del equipo. Si pide una contraseña, introduce el código de 6 dígitos de administrador (de fábrica, `123456`) o de instalador (de fábrica, `654321`).

Configuración desde la aplicación Protegus 2. Desde la aplicación puedes configurar cuando el comunicador ya está en línea y lo has añadido a tu cuenta de Protegus (apartado 5.1). Si el comunicador todavía no puede conectarse –por ejemplo, porque la tarjeta SIM pide el código PIN o porque el operador

necesita otro APN–, haz la primera configuración con TrikdisConfig.

1. En la aplicación, abre el sistema y entra en el menú **Settings** → **Advanced settings**.
2. La primera vez, la aplicación muestra un aviso (**Proceed with Caution**): estos ajustes son para profesionales. Toca el botón **Accept the risk and continue**; con la casilla **Do not show this again**, el aviso ya no vuelve a aparecer.
3. La aplicación lee la configuración del comunicador. Si pide un **Service Access code**, introduce el código de acceso a Protegus Cloud del comunicador (de fábrica, `123456`).
4. Haz los ajustes que se describen abajo y toca el botón **Write**: la aplicación los escribe en el comunicador.

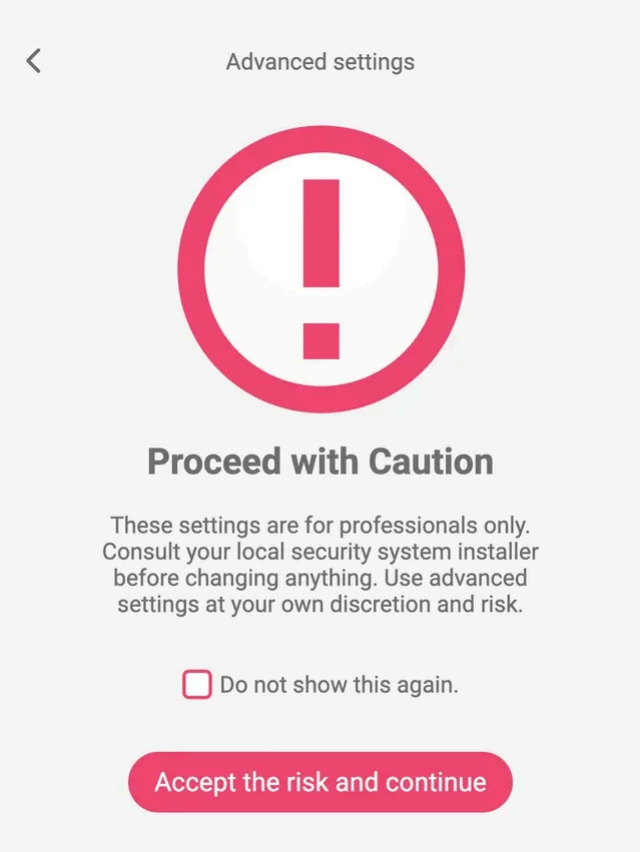


Figura 5. Protegus 2: el aviso que aparece al abrir Advanced settings por primera vez (Proceed with Caution) y el botón Accept the risk and continue.

Desde la aplicación Protegus 2, el GET se puede configurar **con firmware 1.08 o posterior** (la actualización se describe en el capítulo 9).

2.2 Conexión con la aplicación Protegus 2

En la aplicación (Settings → Advanced settings):

1. **Panel settings** → **TLF**: si el comunicador está conectado a los bornes TIP/RING de la central, **Security panel model** debe ser **AUTO**.
2. **Panel settings** → **Serial Bus**: si el comunicador está conectado al bus de datos o al puerto serie de la central, elige en el campo **Security panel model** el modelo de la central conectada.
3. En el mismo lugar, activa la opción **Remote Arm/Disarm** 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. Para el control directo de una central Paradox, introduce la **PC download password**, y en una central Texecom el **UDL passcode**; debe coincidir con la contraseña configurada en la central.
5. **User reporting** → **Cloud**: activa la opción **Enabled** y cambia el **Cloud access code** si quieres que el usuario tenga que introducirlo al dar de alta el sistema en la aplicación (de fábrica, `123456`).
6. **Network settings** → **LAN**: si el comunicador está conectado a la red cableada, activa la opción **Use DHCP**.
7. **Network settings** → **SIM** y **SIM2**: para cada tarjeta SIM colocada, introduce el **SIM card PIN** y el **APN**, y comprueba que **DNS1** y **DNS2** funcionan con tu operador.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: en los campos **Main type**, **Backup type** y **Backup type 2**, fija en qué orden usa el comunicador las conexiones **LAN**, **SIM** (SIM1) y **SIM2**.
9. Toca el botón **Write**.

En TrikdisConfig. Primero, en la página **Panel settings**, indica cómo está conectado 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**.

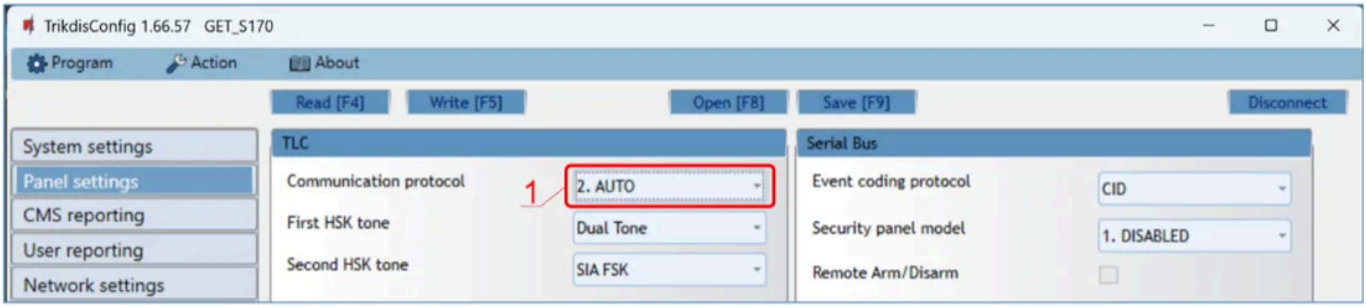


Figura 6. TrikdisConfig – Panel settings, grupo TLC.

- 1 **Communication protocol**: en la conexión TIP/RING, **2. AUTO**.

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



Figura 7. 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 una central Paradox o Texecom, la contraseña PC o UDL configurada en la central; las dos deben coincidir.

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

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

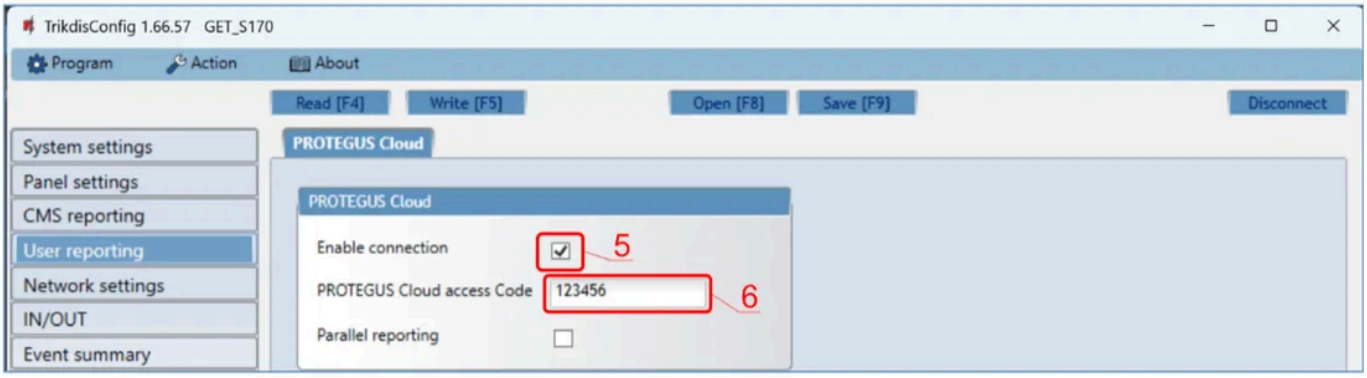


Figura 8. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- 5 **Enable connection**: márcalo; habilita la conexión con la nube de Protegus.
- 6 **PROTEGUS Cloud access Code**: el código de acceso para Protegus 2 (de fábrica, `123456`). Cámbialo si quieres que el usuario tenga que introducirlo al dar de alta el sistema en la aplicación. Si cambias el código más adelante, también hay que cambiarlo en la aplicación Protegus 2.

Si el comunicador está conectado a la red cableada, en la página **Network settings**, en la pestaña **LAN**, marca la opción **Use DHCP**: el comunicador recibe automáticamente la configuración de la red (máscara de subred, puerta de enlace) y una dirección IP.

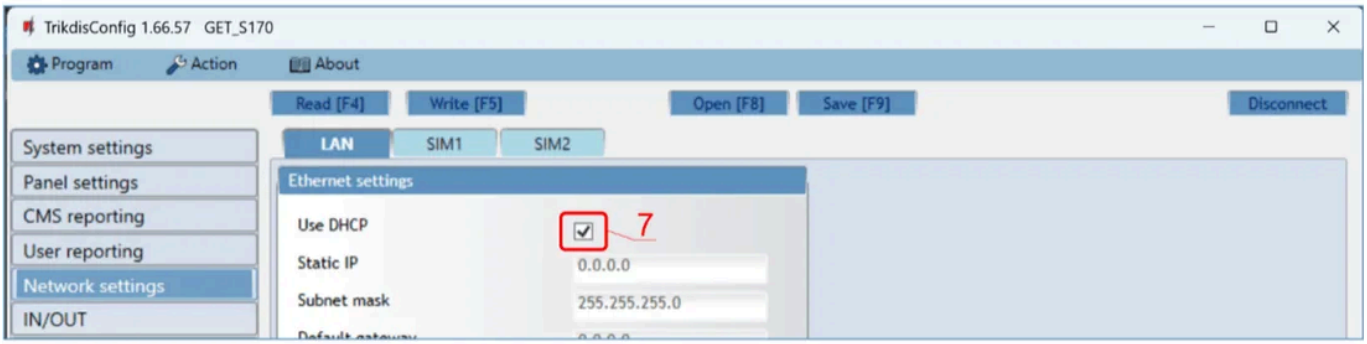


Figura 9. TrikdisConfig – Network settings, pestaña LAN (Ethernet settings).

- 7 **Use DHCP**: marcado, el comunicador recibe automáticamente del router la dirección IP y la configuración de red.

Si hay tarjeta SIM (una o dos tarjetas) en el comunicador, introduce los datos de la tarjeta en la pestaña **SIM1** (y **SIM2**).

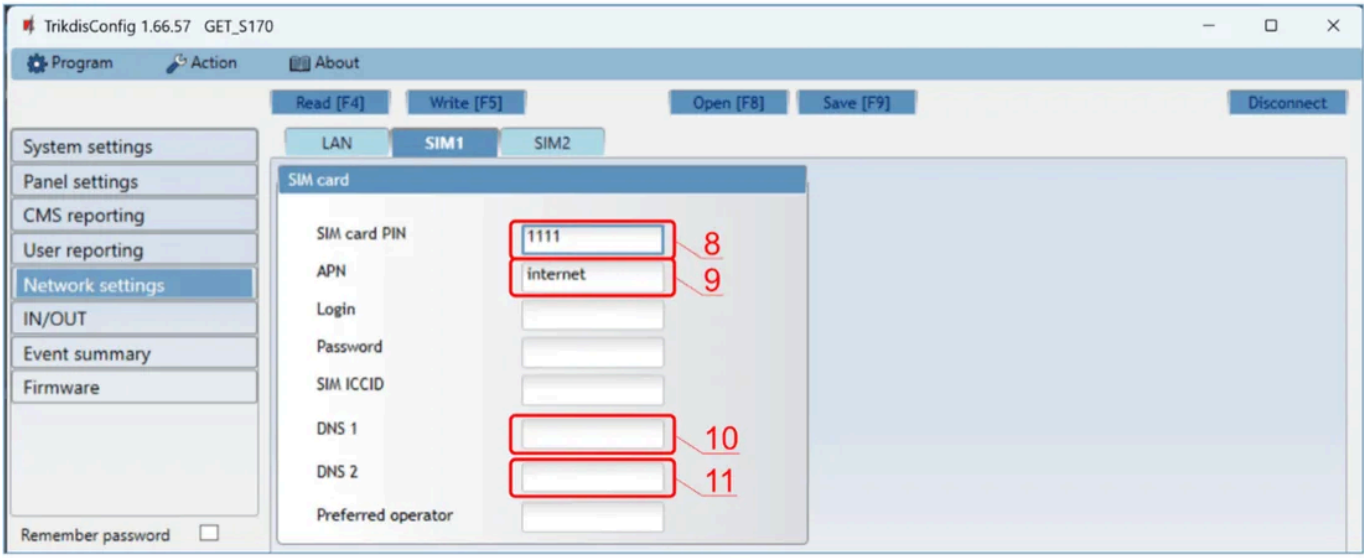


Figura 10. TrikdisConfig – Network settings, pestaña SIM1.

- 8 **SIM card PIN**: el código PIN de la tarjeta (si la petición de PIN está desactivada, puede quedar el valor de fábrica).
- 9 **APN**: el punto de acceso de datos del operador (ver más abajo).
- 10 **DNS 1**: servidor de nombres primario; de fábrica, el DNS de Google. Independientemente de la configuración IP, comprueba que las direcciones DNS funcionan con tu operador.
- 11 **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 por la red móvil. 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.

Por último, en la página **CMS reporting**, en la pestaña **Settings**, en el grupo **Reporting mode**, fija el orden de las conexiones: por esta vía envía el comunicador los mensajes a la CRA y a Protegus 2.

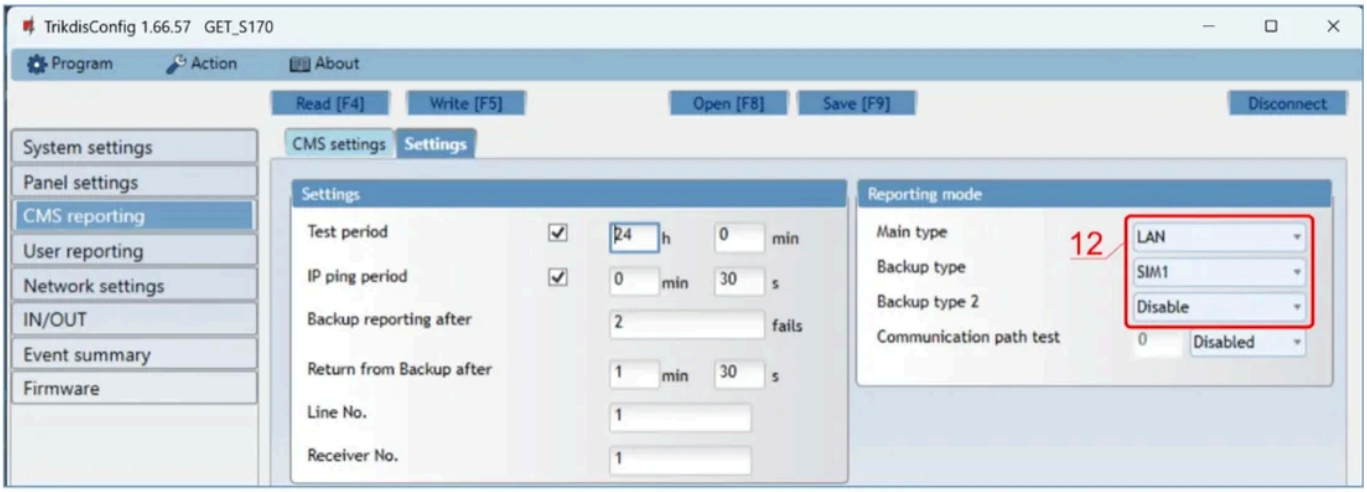


Figura 11. TrikdisConfig – CMS reporting, pestaña Settings, grupo Reporting mode (de fábrica, Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode**: **Main type**, la conexión principal (LAN, SIM1 o SIM2); **Backup type**, la de respaldo; **Backup type 2**, el segundo respaldo.

Los tipos de conexión se indican por orden. Si el comunicador no puede conectarse con la conexión **Main type**, pasa a **Backup type**, y así sucesivamente. Si la conexión de respaldo ha transmitido correctamente el mensaje a la CRA, pasado el tiempo indicado el comunicador intenta volver a la conexión principal (apartado 6.4.2).

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

En 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

En la aplicación (Settings → Advanced settings):

1. **System options** → **System general**: introduce el número de abonado recibido de la CRA (**Account No.**; 0–9, A–F; `FFFE` y `FFFF` no se pueden usar). En la versión de hardware **x1x1**, con firmware **1.31** o posterior, el número de abonado se introduce por canal: **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** Lo reconoces en la pantalla: si System general solo muestra el campo **Time set**, usa el ajuste del canal.
2. **Panel settings** → **TLF** (conexión TIP/RING): **Security panel model** debe ser **AUTO**; o **Panel settings** → **Serial Bus** (conexión al bus de datos o serie): elige el **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel**: activa la opción **Enabled** y luego introduce: **Communication type**: **IP**; la dirección **Domain or IP** y el **Port** del receptor; **TCP or UDP**; **Protocol**: **TRK8** para un receptor Trikdis, **DC-09_2007** o **DC-09_2012** para un receptor universal, **TL150** para un receptor SUR-GARD; y la clave de cifrado configurada en el receptor: con el protocolo TRK, en el campo **TRK encryption key**; con DC-09, activa la opción **Enable encryption key** e introduce la **DC-09 encryption key**.
4. (Recomendado) Configura del mismo modo el **Backup channel** (canal de respaldo).
5. **Reporting to CMS** → **CMS settings** → **Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.
6. **Network settings** → **LAN** (red cableada): activa la opción **Use DHCP**. **Network settings** → **SIM** y **SIM2** (para cada tarjeta SIM): **SIM card PIN**, **APN**, y comprueba los campos **DNS1** y **DNS2**.

7. Toca el botón **Write**.

En TrikdisConfig. Primero, en la página **System settings**, introduce el número de abonado.



Figura 12. TrikdisConfig – página System settings, grupo General.

- 1 **Object ID**: el número de abonado recibido de la CRA (6 caracteres hexadecimales, 0–9, A–F). `FFFE` y `FFFF` no se pueden usar.

En la página **Panel settings**, indica la conexión de la central si todavía no lo has hecho en el apartado 2.2: en la conexión TIP/RING, **Communication protocol** debe ser **AUTO**; en la 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 pestaña **CMS settings**, en la parte **Primary channel** (canal principal), configura los datos del receptor. La imagen muestra la ventana antes de la configuración: el campo **Communication type** del canal principal todavía está en **Disable**.

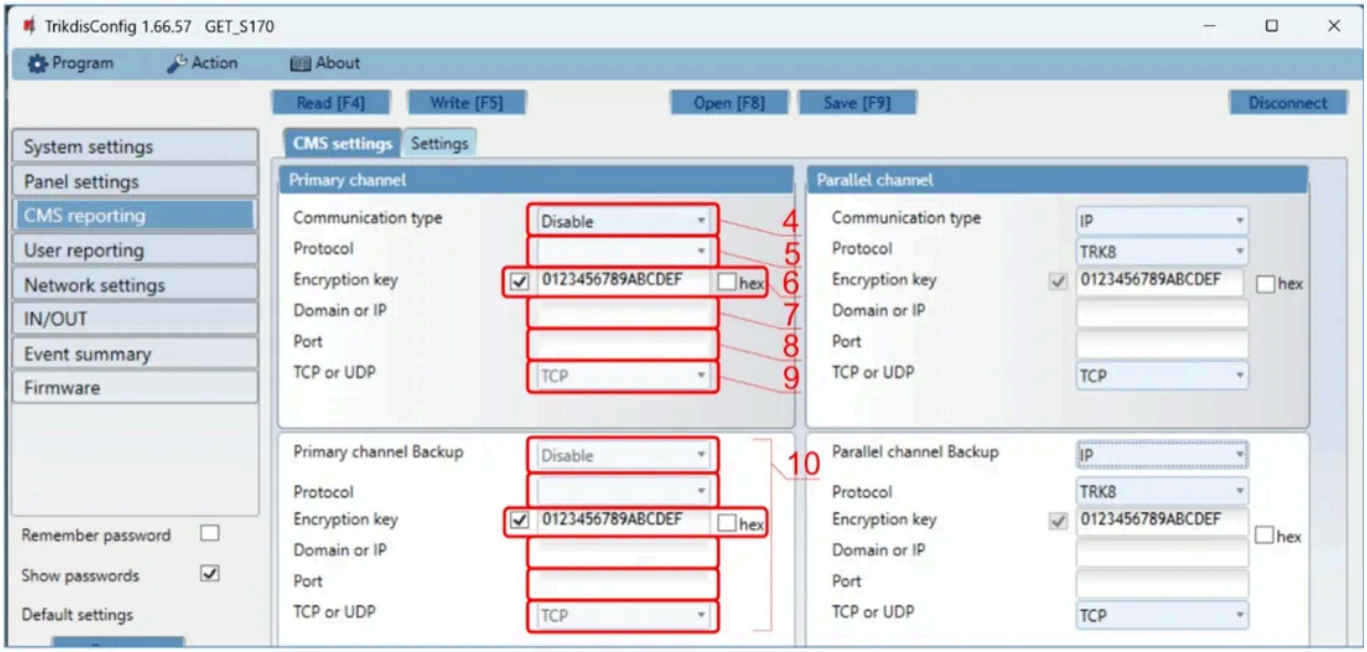


Figura 13. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 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 a la configuración del receptor.
- 10 **Primary channel Backup**: canal de respaldo para cuando falle el principal; rellénalo del mismo modo, se recomienda configurarlo.

En la pestaña **Settings**, en el grupo **Reporting mode**, fija el orden de las conexiones (**Main type**, **Backup type**, **Backup type 2**) si todavía no lo has hecho en el apartado 2.2; allí encuentras también la figura y la descripción del funcionamiento.

Por último, en la página **Network settings**, introduce los datos de la red si todavía no lo has hecho en el apartado 2.2: en la pestaña **LAN**, la casilla **Use DHCP**; en la pestaña **SIM1** (y **SIM2**), los datos de la tarjeta (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

Con el protocolo **DC-09**, introduce también en la pestaña **Settings** el número de línea y de receptor (**Line No.**, **Receiver No.**, apartado 6.4.2). El GET solo transmite a la CRA por conexión IP –por la red cableada o por internet móvil–; no tiene canal de respaldo por SMS.

Al terminar la configuración, pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB. Con esto el equipo está listo para la conexión. En la conexión por línea telefónica, aquí también 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 –o las dos– en su ranura, si no lo has hecho durante la puesta en marcha.
3. Saca el circuito impreso de la base: abre el cierre que hay 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 agujeros para los tornillos están marcados con un círculo), o con la cinta adhesiva de doble cara que se incluye, según el apartado 3.2.
5. Vuelve a poner el 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.
8. Si también envías los eventos a la CRA por la red cableada (LAN), enchufa el cable de red en la toma LAN del comunicador.

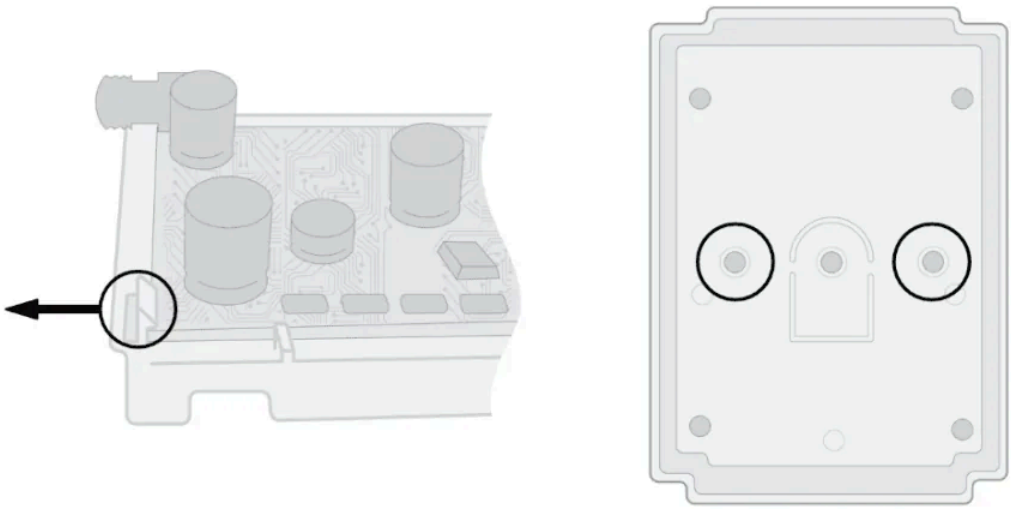


Figura 14. Cómo sacar el circuito impreso de la base (izquierda: el cierre y el sentido de extracción) y los agujeros para los tornillos de la base (derecha).

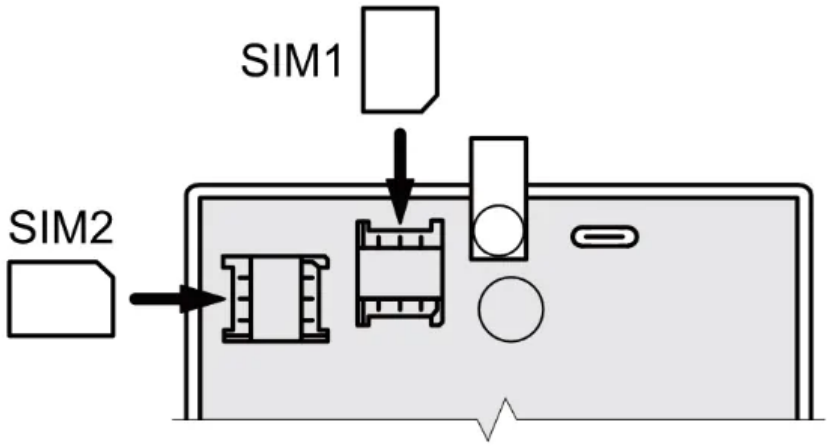


Figura 15. El lugar de las dos ranuras SIM en el circuito impreso: la SIM1 en el centro de la placa, la SIM2 en el borde izquierdo; las flechas indican el sentido en que se introduce la tarjeta.

En el comunicador se pueden poner una o dos tarjetas SIM. La tarjeta 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 Colocación en la caja de la central, antena

El comunicador debe colocarse en la **caja de la central de alarma protegida con interruptor de tamper de tapa**. Fíjalo a la pared interior del fondo de la caja con la cinta de espuma acrílica de doble cara, de calidad industrial, que se incluye: pega la cinta sobre una superficie limpia y seca, presionando con fuerza, para que sujete con seguridad. Si la caja de la central no permite esta fijación segura, el comunicador también se puede montar en una caja aparte protegida con tamper.

- **En 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 un cable más largo.
- Antes de la fijación definitiva, **comprueba el nivel de señal**: el número de destellos amarillos del LED NETWORK LTE debe ser como mínimo 3 en 4G (apartado 1.6). Si es menor, busca un lugar mejor para la antena, o cambia a una antena más sensible que se pueda colocar más lejos.
- Mantén la antena y el comunicador lejos del transformador de la central y de los cables de red eléctrica.

- Pasa el cable LAN por la entrada de cables de la caja hasta la toma RJ45 del lateral del comunicador; el cable no debe tirar de los bornes.



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

Sigue, de los esquemas siguientes, el que corresponde a tu central. En los esquemas, **+DC** y **–DC** son los bornes de alimentación **+12 VDC** / **–12 VDC** del comunicador, y **A RS485** / **B RS485** son los bornes **A 485** / **B 485** (en el GET no hay que conectarlos). El comunicador recibe la alimentación de la salida de alimentación auxiliar (AUX) de la central, así que, durante un corte de corriente, la batería de la central alimenta también al comunicador.

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**.

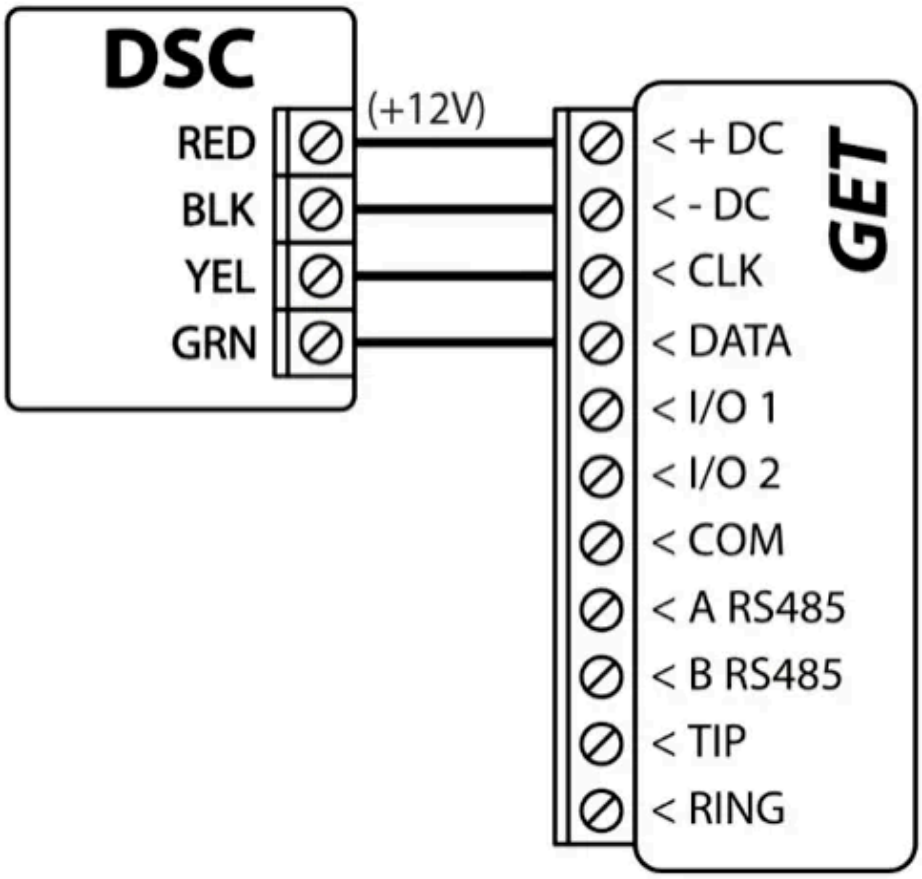


Figura 16. Conexión de una central DSC por el bus de datos (Keybus, «Keypad bus»): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

El GET gestiona la central DSC solo por el bus de datos; la conexión simultánea del Keybus y de los bornes TIP/RING solo existe en el comunicador GT+. Conectado solo al Keybus, el comunicador recibe de la central el estado general de las zonas, pero no el tipo de zona (incendio, intrusión, fuga de agua, etc.), por eso transmite todas las alarmas como **alarma general, con el código Contact ID E130**. Si la CRA necesita los códigos propios de la central (por ejemplo, alarma de incendio: E110), puedes enviar los eventos con el marcador telefónico de la central, con la conexión TIP/RING (apartados 3.3.9 y 4.2); en ese caso no hay control directo.

3.3.2 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**.

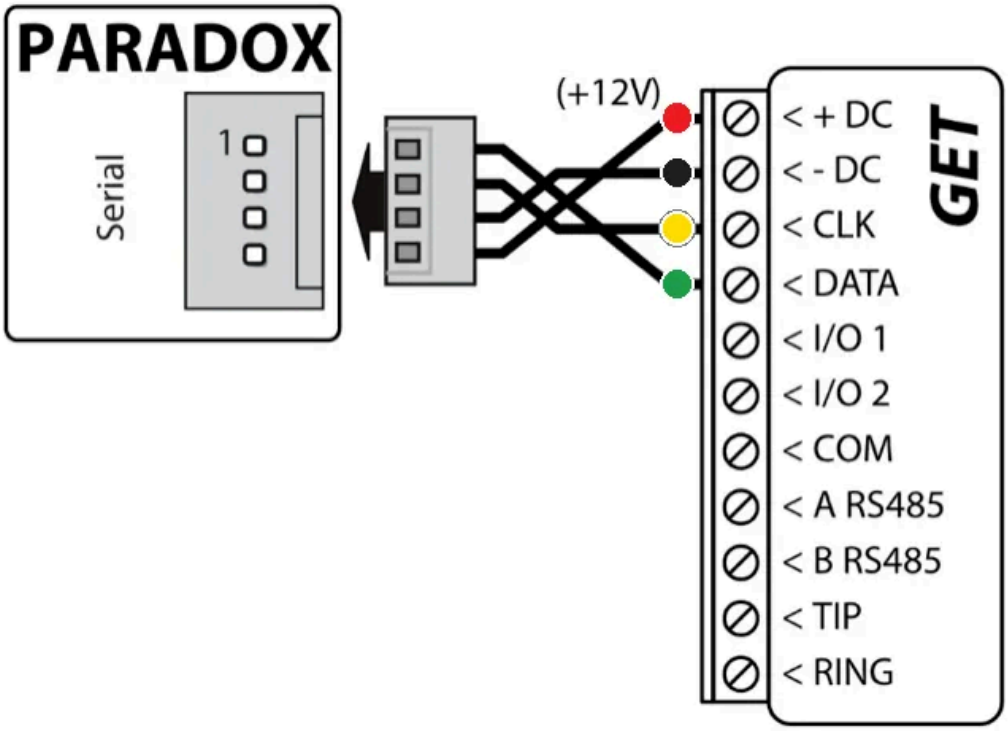


Figura 17. Conexión de una central Paradox por el puerto serie con el cable EX-CRP2.4 (se pide por separado; «Use the EX-CRP2.4 cable (ordered separately)»): rojo → +DC, negro → −DC, amarillo → CLK, verde → DATA.

- 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.

3.3.3 Paradox SP/MG – Keybus y TIP/RING

Las centrales Paradox Spectra SP, SP+ y Magellan MG, MG+ también se pueden conectar, en lugar de por el 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 además **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.

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

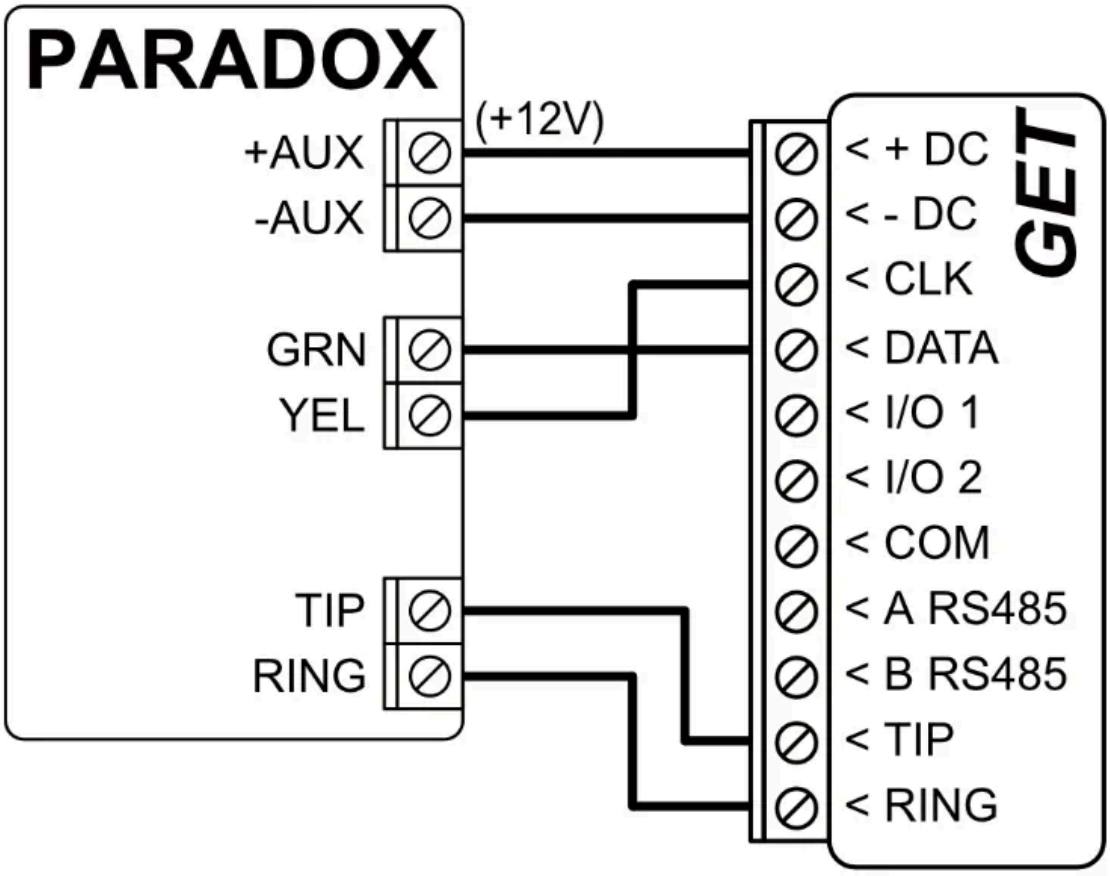


Figura 18. Conexión de una central Paradox SP / SP+ / MG / MG+ por el Keybus (bus de datos, «Keypad bus») y por los bornes TIP/RING a la vez: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

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

1. **Communication protocol**: **2. AUTO**.
2. **Security panel model**: elige de la lista el elemento **Paradox SP+/MG+ series KeyBus** (en la imagen, 7. PARADOX SP+/MG+).
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 PC configurada en la central; las dos deben coincidir.

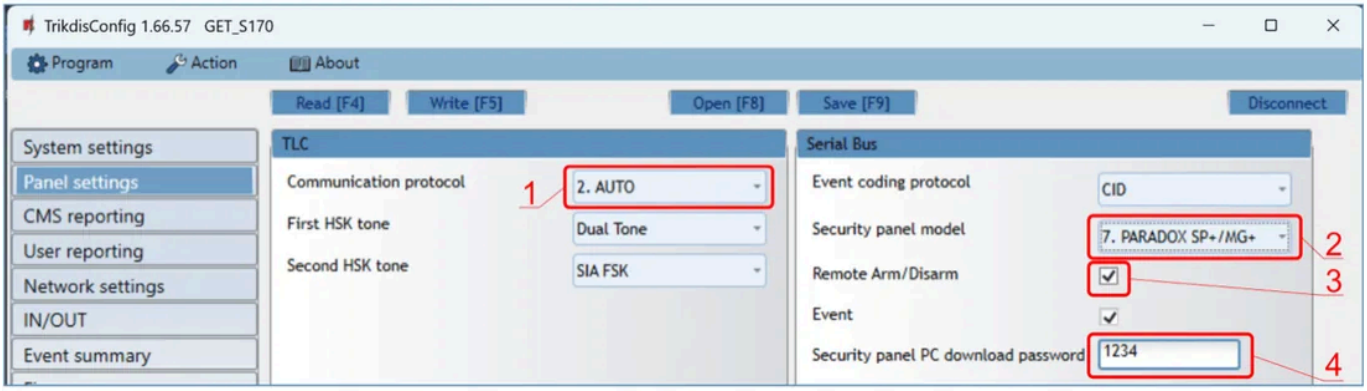


Figura 19. TrikdisConfig – Panel settings para la conexión Keybus + TIP/RING: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm marcado (3), Security panel PC download password introducida (4).

En la aplicación Protegus 2, estos mismos ajustes están en las páginas **Panel settings** → **TLF** (Security panel model = Communication protocol) y **Panel settings** → **Serial Bus** (apartado 6.3).

La central Paradox también hay que programarla para que envíe los eventos a la CRA y se pueda controlar desde Protegus 2: en el teclado conectado a la central, configura las celdas siguientes:

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

La contraseña PC escrita en la celda **911** debe coincidir con el campo **Security panel PC download password** del comunicador (apartado 4.1.2).

3.3.4 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 CLK, TIP y RING no hacen falta.

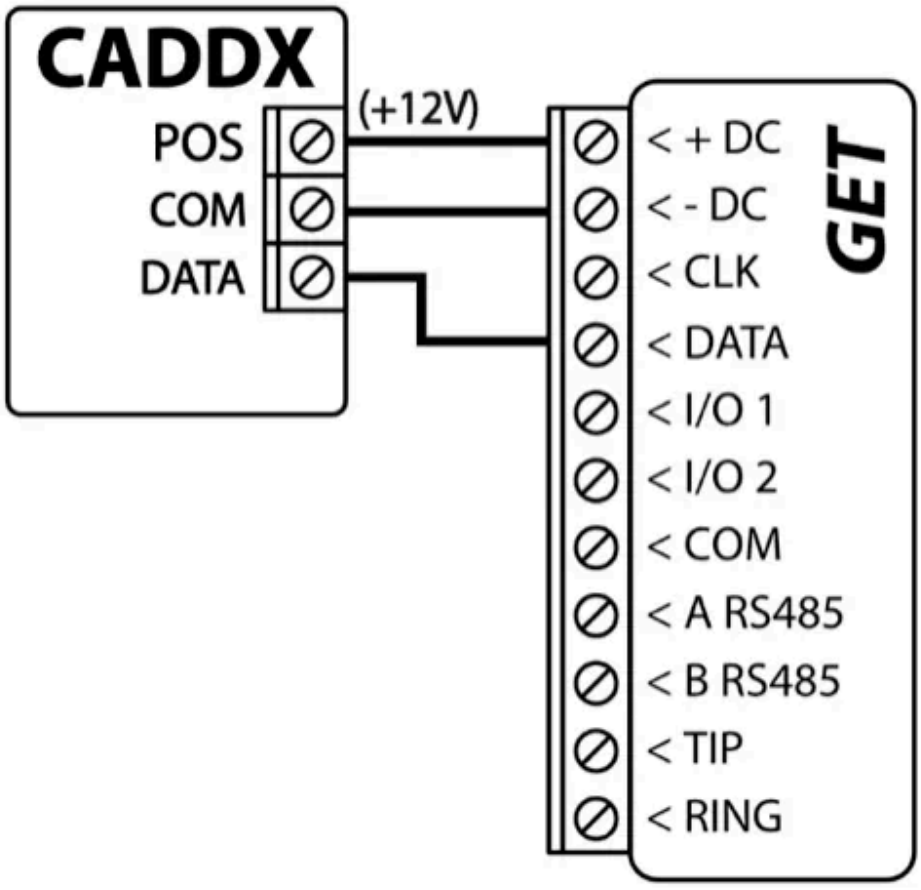


Figura 20. Conexión de una central UTC Interlogix (Caddx) NetworX por el bus de datos («Keypad bus»): POS → +DC, COM → −DC, DATA → DATA.

3.3.5 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**.

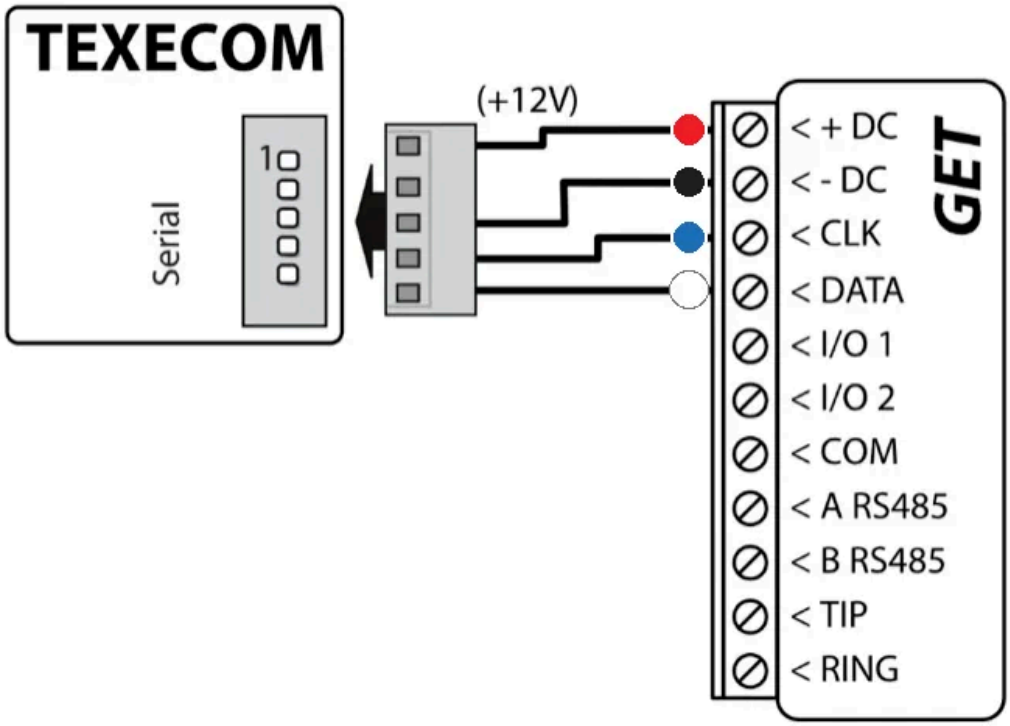


Figura 21. Conexión de una central Texecom por el puerto serie con el cable EX-CRP4 (se pide por separado; «Use the EX-CRP4 cable (ordered separately)»): rojo → +DC, negro → −DC, azul → CLK, blanco → DATA.

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

3.3.6 InnerRange Inception

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

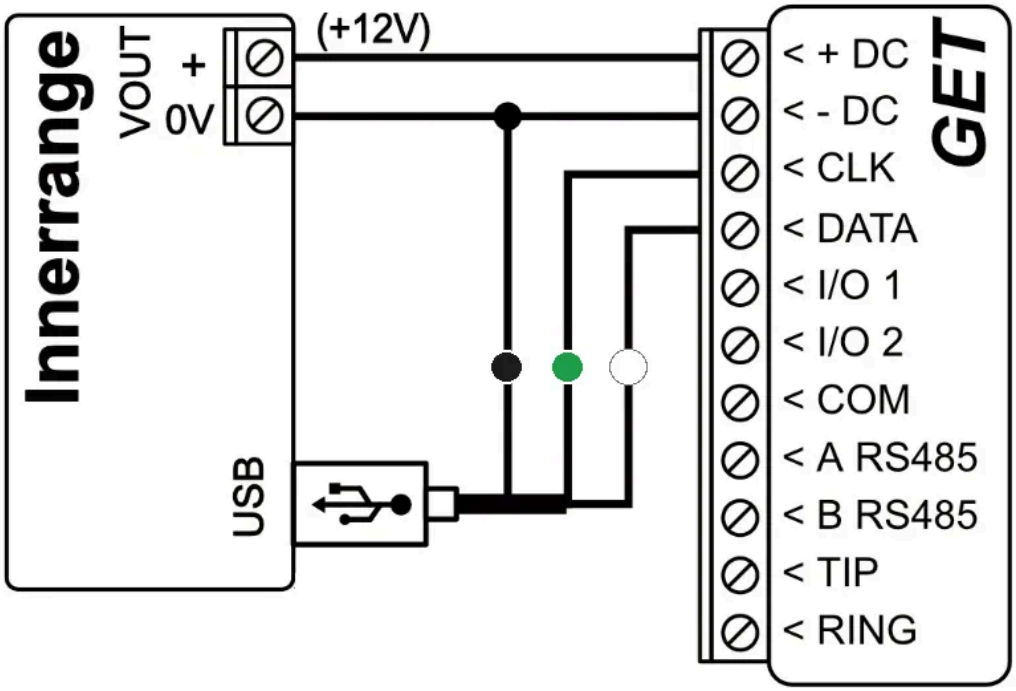


Figura 22. Conexión de InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; desde el puerto USB, con el cable 993030USB («Cable, Inner Range part number 993030USB»), negro → −DC, verde → CLK, blanco → DATA.

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

3.3.7 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**.

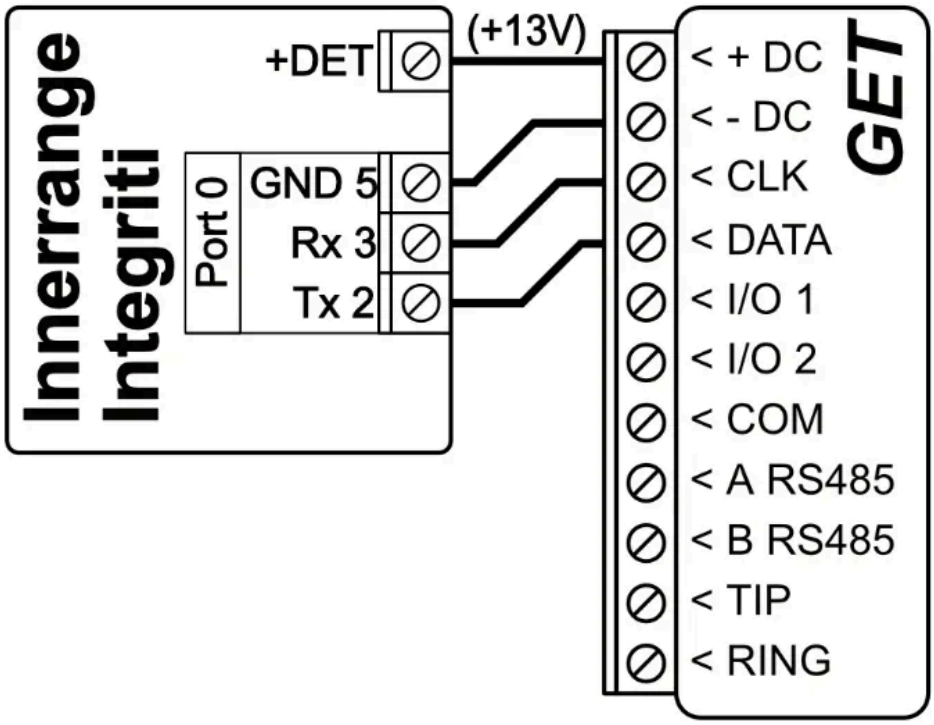


Figura 23. Conexión de InnerRange Integriti al Port 0 con el cable INTG-996795 («Cable, Inner Range part number INTG-996795»): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – bus de datos

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

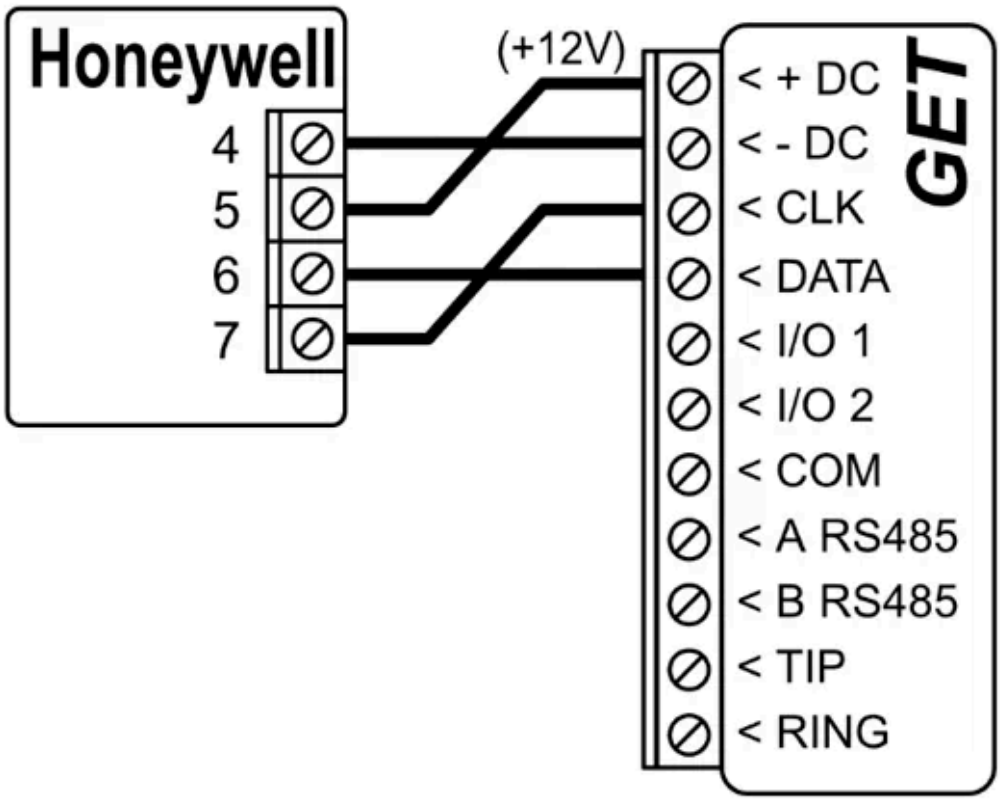


Figura 24. Conexión de una central Honeywell Vista-15 / -20 / -48 por el bus de datos («Keypad bus»): borne 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Cualquier central – TIP/RING

Cualquier otra central se puede conectar a través de su comunicador 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).

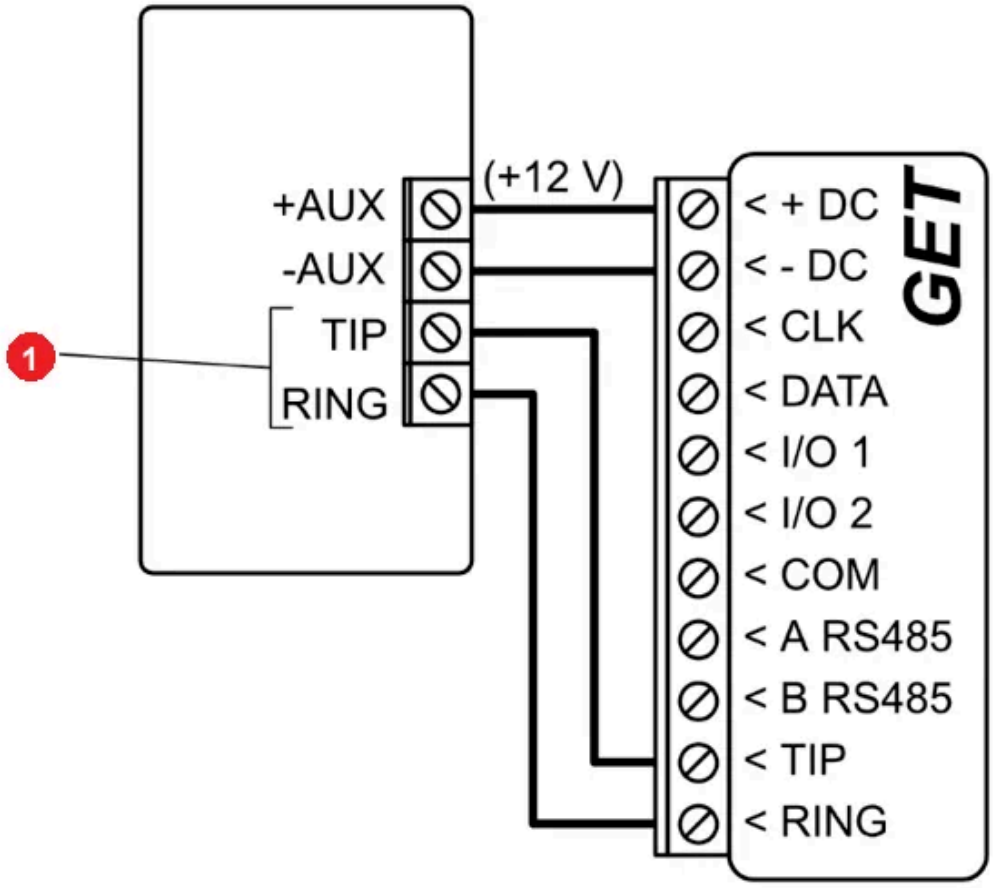


Figura 25. Conexión al comunicador telefónico de la central («Control panel»): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 los bornes del comunicador 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 del comunicador (PGM) accione la **zona de llave** de la central, sigue esta conexión. Los dos bornes I/O de doble función del comunicador funcionan como salidas (OUT, PGM) –en el GET, de fábrica, los dos son salidas–, 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 la casilla **Remote Arm/Disarm**, los bornes deben estar en función **OUT** en la página **IN/OUT** (apartado 6.7) y, en la aplicación Protegus 2, asigna las salidas a las particiones según el apartado 5.2.

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

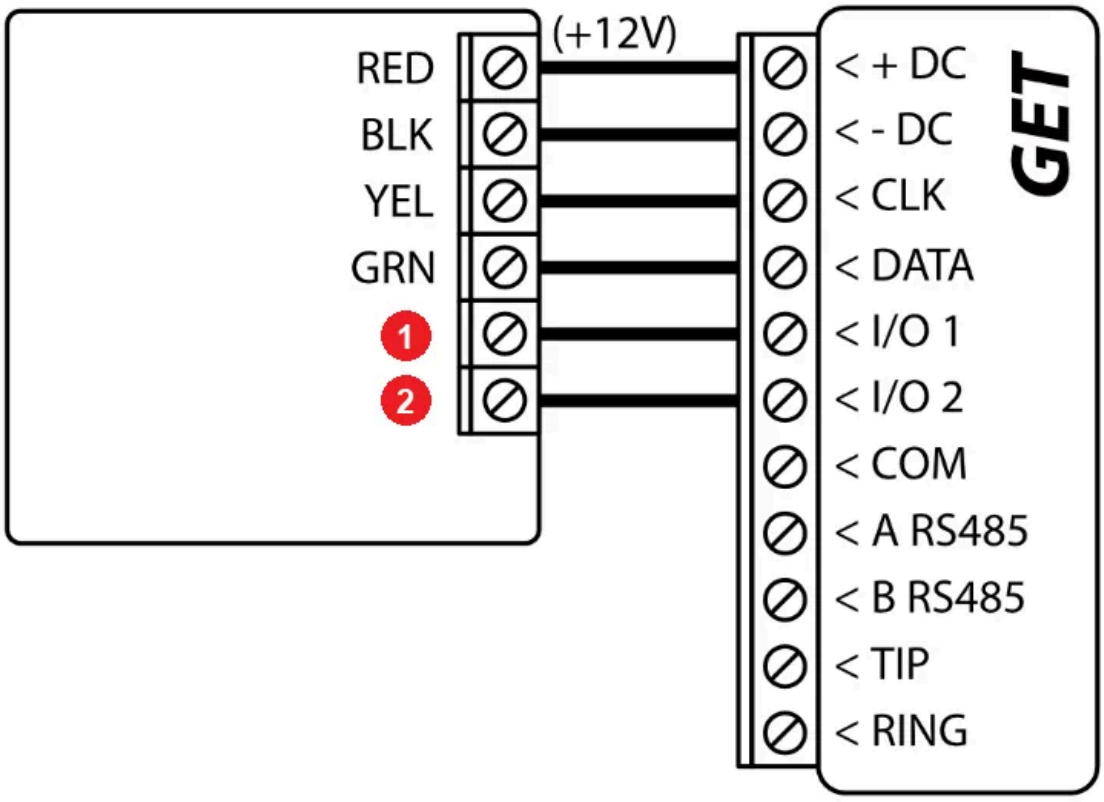


Figura 26. Armado y desarmado con zona de llave («Zone (keyswitch)»), en la conexión al bus de datos o serie («Keypad bus or Serial port»): borne RED de la central de alarma («Control panel») → +DC, BLK → −DC, YEL → CLK, GRN → DATA; la zona de la partición 1 → 1 I/O, la de la partición 2 → 2 I/O.

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

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

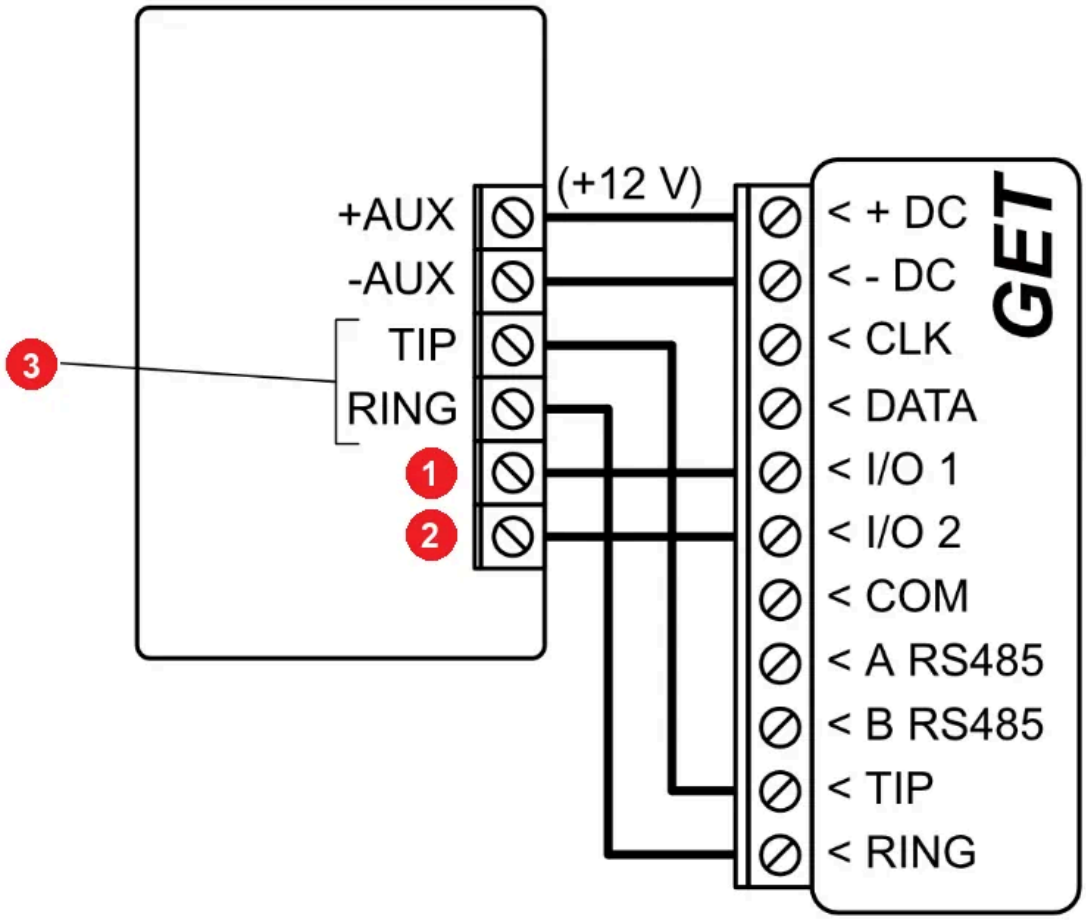


Figura 27. Armado y desarmado con zona de llave («Zone (keyswitch)»), en la conexión por línea telefónica: borne +AUX de la central de alarma («Control panel») → +DC, −AUX → −DC, TIP → TIP, RING → RING; la zona de la partición 1 → 1 I/O, la de la partición 2 → 2 I/O.

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

La zona de llave puede ser de impulso o biestable; 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 I/O de doble función del comunicador también se pueden usar como entradas (IN) para recibir otros detectores (por ejemplo, un interruptor de tamper o un pulsador 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. En el GET, los bornes son salidas de fábrica: pon el borne que uses en función **IN** en la página **IN/OUT** de TrikdisConfig e indica en el campo **Type** el tipo de circuito conectado; en la aplicación Protegus 2, lo mismo está en la página **Advanced settings** → **IN/OUT**, en el campo **Type** del borne 1 o 2 (apartado 6.7). La entrada se conecta entre el I/O elegido y el borne **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	–
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 los puntos COM e 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.

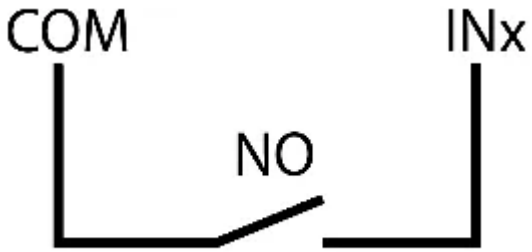


Figura 28. NO – circuito abierto en reposo: cerrado = alarma, abierto = reposo.

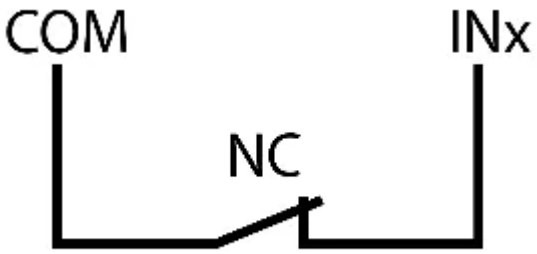


Figura 29. NC – circuito cerrado en reposo: abierto = alarma, cerrado = reposo.

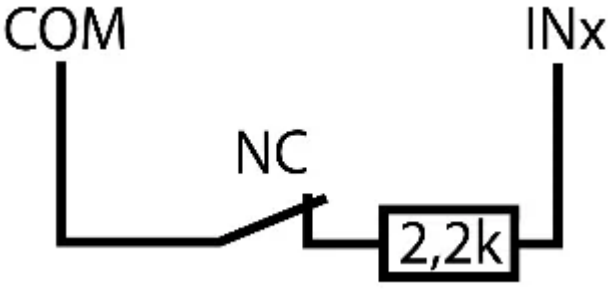


Figura 30. NC/EOL – circuito cerrado en reposo con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto = alarma, 2,2 kΩ = reposo.

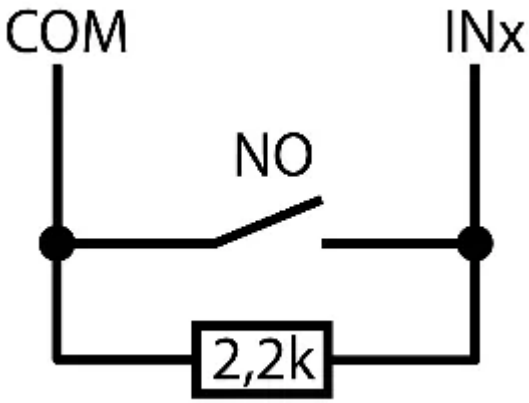


Figura 31. NO/EOL – circuito abierto en reposo con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto = alarma, 2,2 kΩ = reposo.

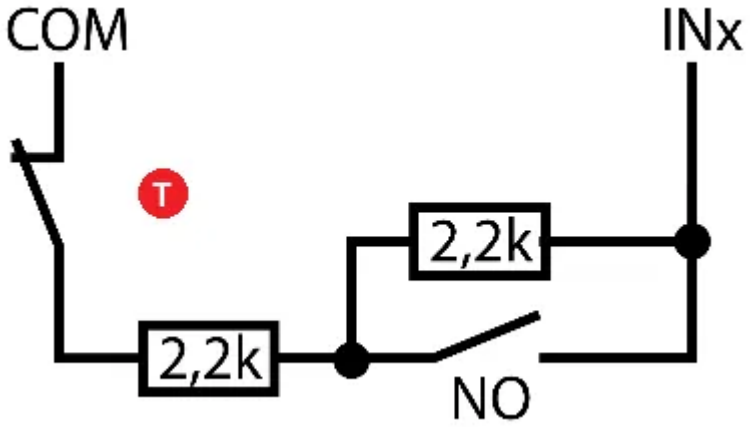


Figura 32. NO/DEOL – circuito abierto en reposo con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto = sabotaje, 2,2 kΩ = alarma, 3,3–5,5 kΩ = reposo.

- T contacto de tamper («Tamper»), señala la apertura de la carcasa del detector

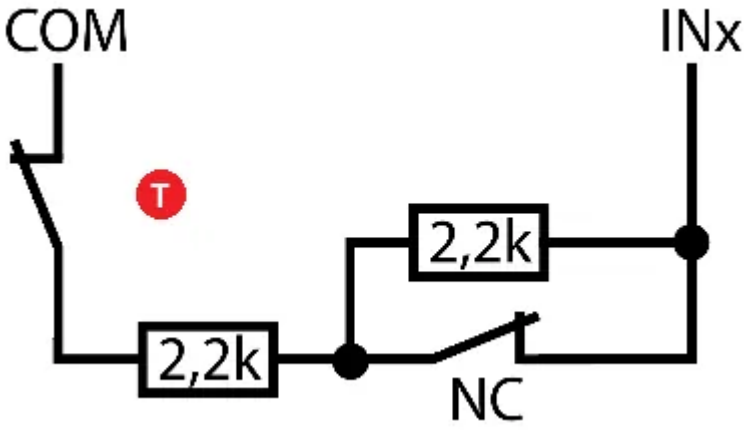


Figura 33. NC/DEOL – circuito cerrado en reposo con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto = sabotaje, 2,2 kΩ = reposo, 3,3–5,5 kΩ = alarma.

- T contacto de tamper («Tamper»), señala la apertura de la carcasa del detector

3.6 Conexión de una salida con relé

Como salidas, los bornes I/O son salidas de colector abierto (OC): en estado activo llevan a negativo la carga conectada, con un máximo de 0,15 A 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**; el consumidor lo conmutan los contactos del relé (NC, C, NO). El borne I/O que uses debe ser salida (**OUT**) en la página **IN/OUT** de TrikdisConfig (o en la página IN/OUT de la aplicación); en el GET esta es la configuración de fábrica.

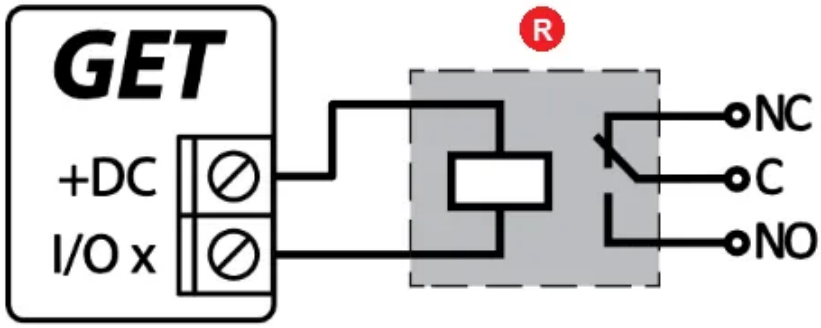


Figura 34. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne x I/O, los contactos (NC, C, NO) conmutan el consumidor.

- R relé («Relay»)

Las salidas las puedes accionar desde la aplicación Protegus 2 (capítulo 5).

3.7 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 arranca también el comunicador. En la tapa frontal debes ver esto:

- **POWER** verde fijo: la alimentación es correcta;
- **NETWORK LTE** verde fijo y parpadeo amarillo: se ha conectado a la red móvil; 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 para la antena, o usa una antena más sensible (apartado 3.2);
- **NETWORK LAN** verde fijo, si también has enchufado el cable de red: se ha conectado a la red cableada;
- **TROUBLE** apagado.

Si TROUBLE parpadea, el número de destellos indica la causa (apartado 1.6); cualquier otra indicación LED distinta de esta también señala algún fallo; busca la causa 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: por el bus de datos o por el puerto serie (apartado 4.1), o a través de su comunicador telefónico, en los bornes TIP/RING (apartado 4.2). En la conexión Keybus + TIP/RING de las centrales Paradox SP / SP+ / MG / MG+, la configuración de las celdas de la central está en la tabla del apartado 3.3.3.

4.1 Conexión al bus de datos o serie

Aquí describimos cómo hay que configurar la central para que el comunicador lea sus eventos y la pueda controlar a distancia. Para el control a distancia, la opción **Remote Arm/Disarm** debe estar marcada en la página **Panel settings** de TrikdisConfig (en la aplicación: **Panel settings** → **Serial Bus**) (apartados 2.2 y 6.3).

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.

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 el comunicador GET, el campo **Security panel PC download password** está en la página **Panel settings** de TrikdisConfig, en el grupo **Serial bus**; en la aplicación Protegus 2, en **Panel settings** → **Serial Bus** → **PC download password** (apartados 2.2 y 6.3).

Conexión Keybus y TIP/RING (SP / SP+ / MG / MG+, apartado 3.3.3): además, la central hay que programarla para que envíe los eventos a la CRA y se pueda controlar desde Protegus 2; los valores de las celdas (801, 811, 812, 815, 911) están en la tabla del apartado 3.3.3.

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 el comunicador GET, el campo **Security panel PC download password** está en la página **Panel settings** de TrikdisConfig, en el grupo **Serial bus** (en la aplicación, **Panel settings** → **Serial Bus** → **PC download password**); 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

Posición (location)	Segmento	Ajuste
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.

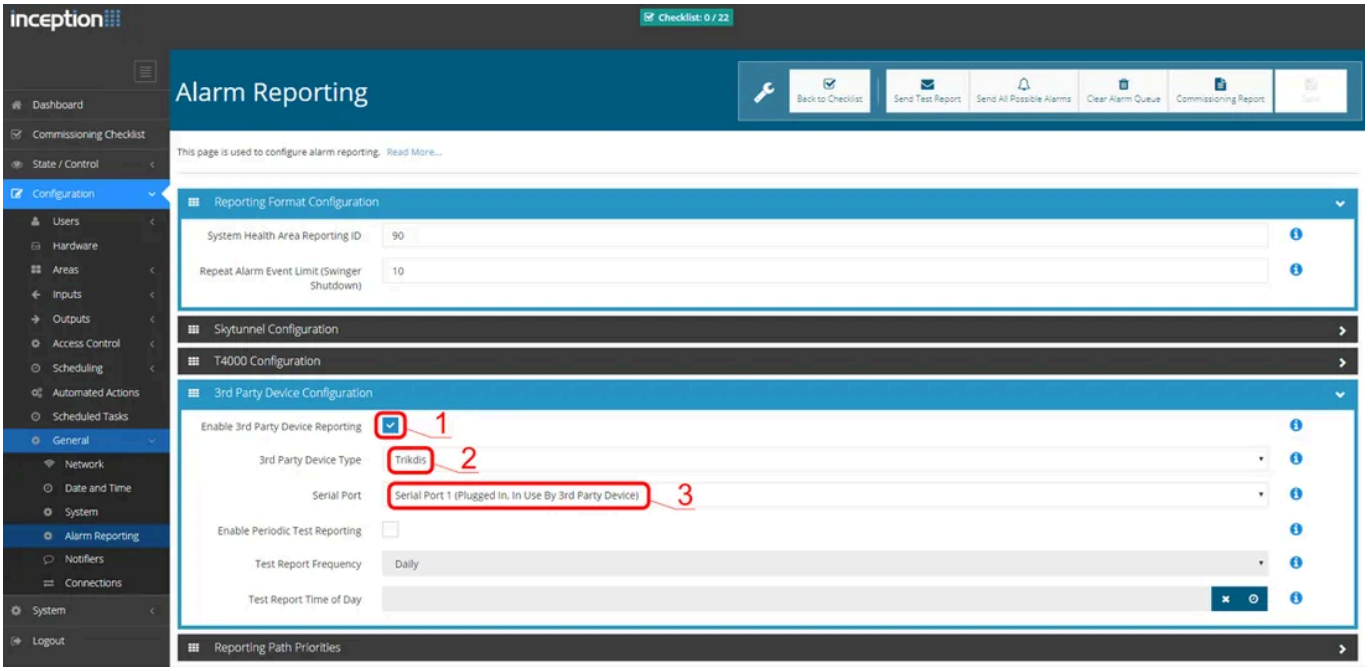


Figura 35. InnerRange Inception – Configuration → General → Alarm Reporting, grupo 3rd Party Device Configuration: Enable 3rd Party Device Reporting marcado, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

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 3.3.9); 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 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 UTC Interlogix (Caddx) NX

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

Posición (location)	Teclas	Observación
	`*89713`	Entrada en 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 puede accionar las salidas del comunicador. La aplicación se descarga para Android e iOS (Google Play, App Store), o se usa desde el navegador: web.protegus.app. Entra con tu nombre de usuario y tu contraseña, o regístrate con una cuenta nueva. El GET no avisa por SMS ni por llamada telefónica, y tampoco acepta comandos SMS: el control a distancia y los avisos se hacen a través de la aplicación; la configuración del comunicador también es accesible desde la aplicación (**Settings** → **Advanced settings**, capítulo 6).

5.1 Añadir el equipo

Antes de añadir el equipo, comprueba lo siguiente:

1. La tarjeta SIM está activa y su código PIN está introducido en el equipo, o la petición de PIN está desactivada; **o bien** el comunicador está conectado a la red local con un cable de red (LAN).
2. En la página **User reporting** → **PROTEGUS Cloud** de TrikdisConfig está marcada la opción **Enable connection** (apartado 6.5).
3. El LED **POWER** está verde fijo.

4. El LED **NETWORK LTE** está verde fijo y parpadea en amarillo (el equipo está en la red móvil); si solo hay conexión cableada, el LED **NETWORK LAN** está verde fijo.

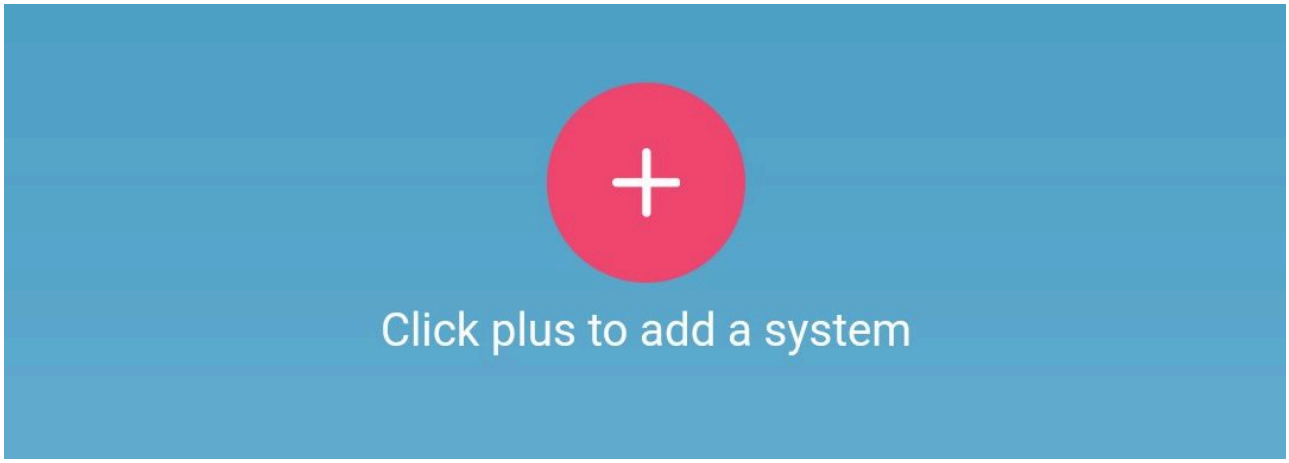
El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del 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



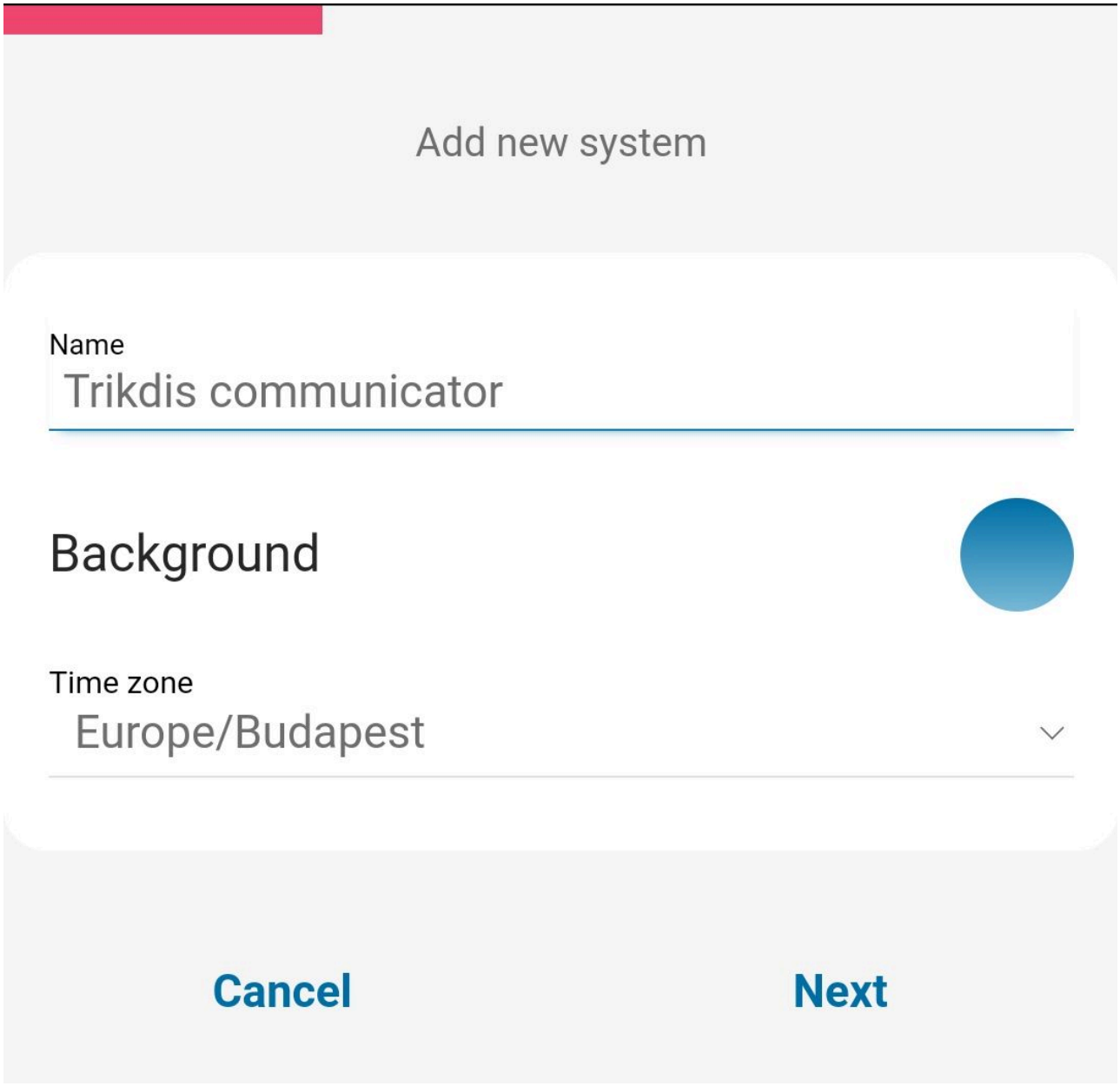
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



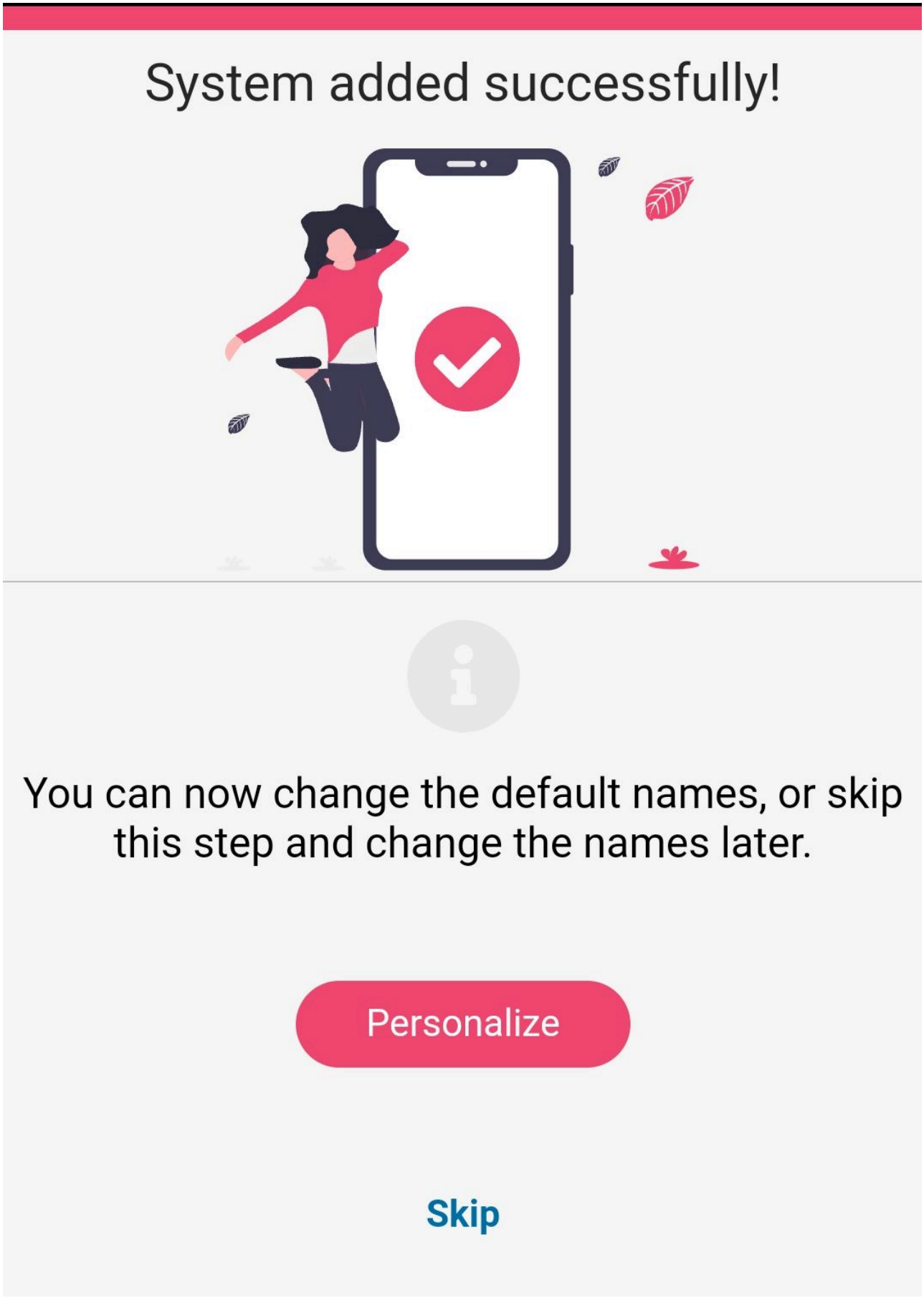
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



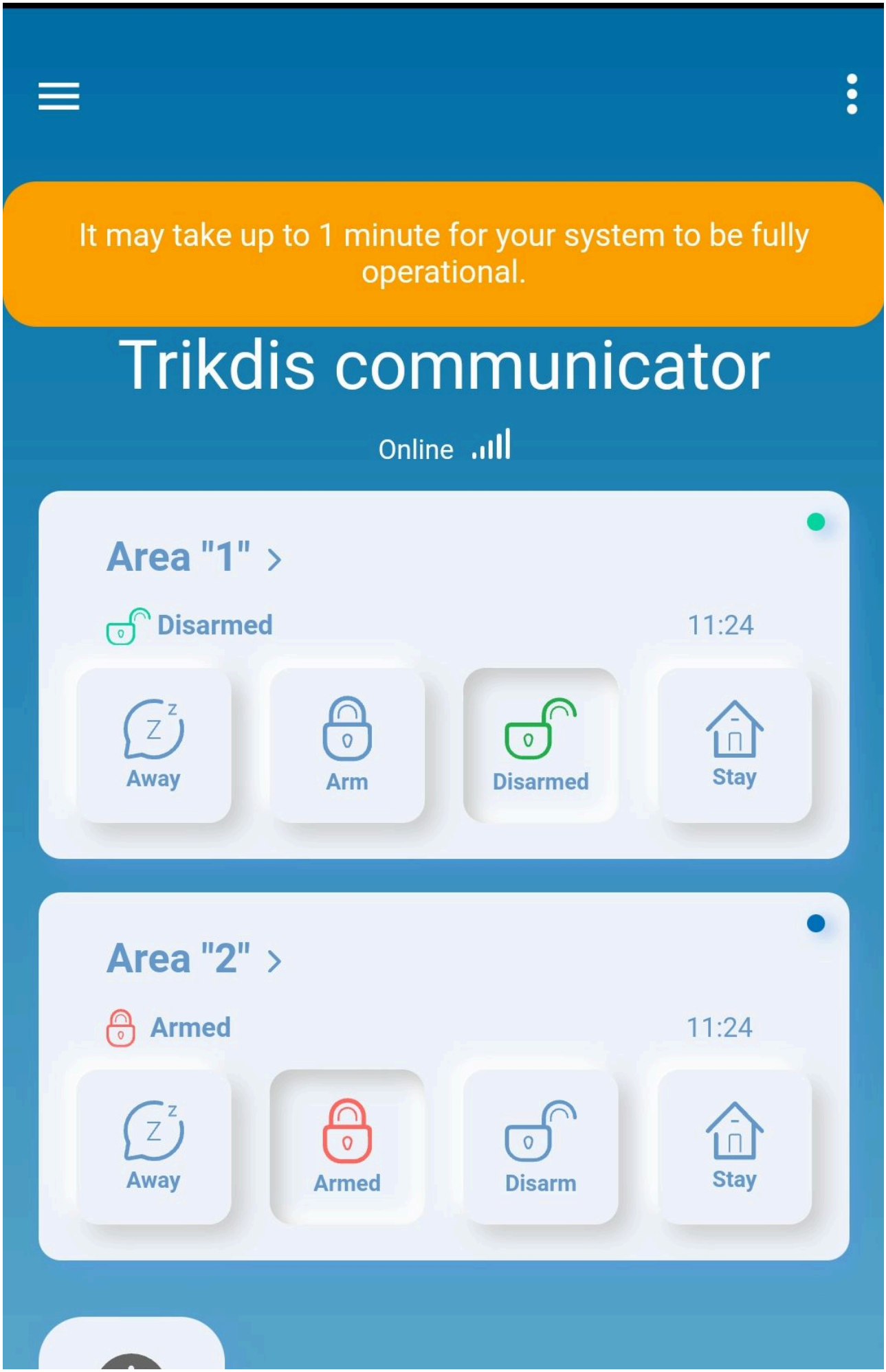
6. Add meg a rendszer nevét és válassz idozónát



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

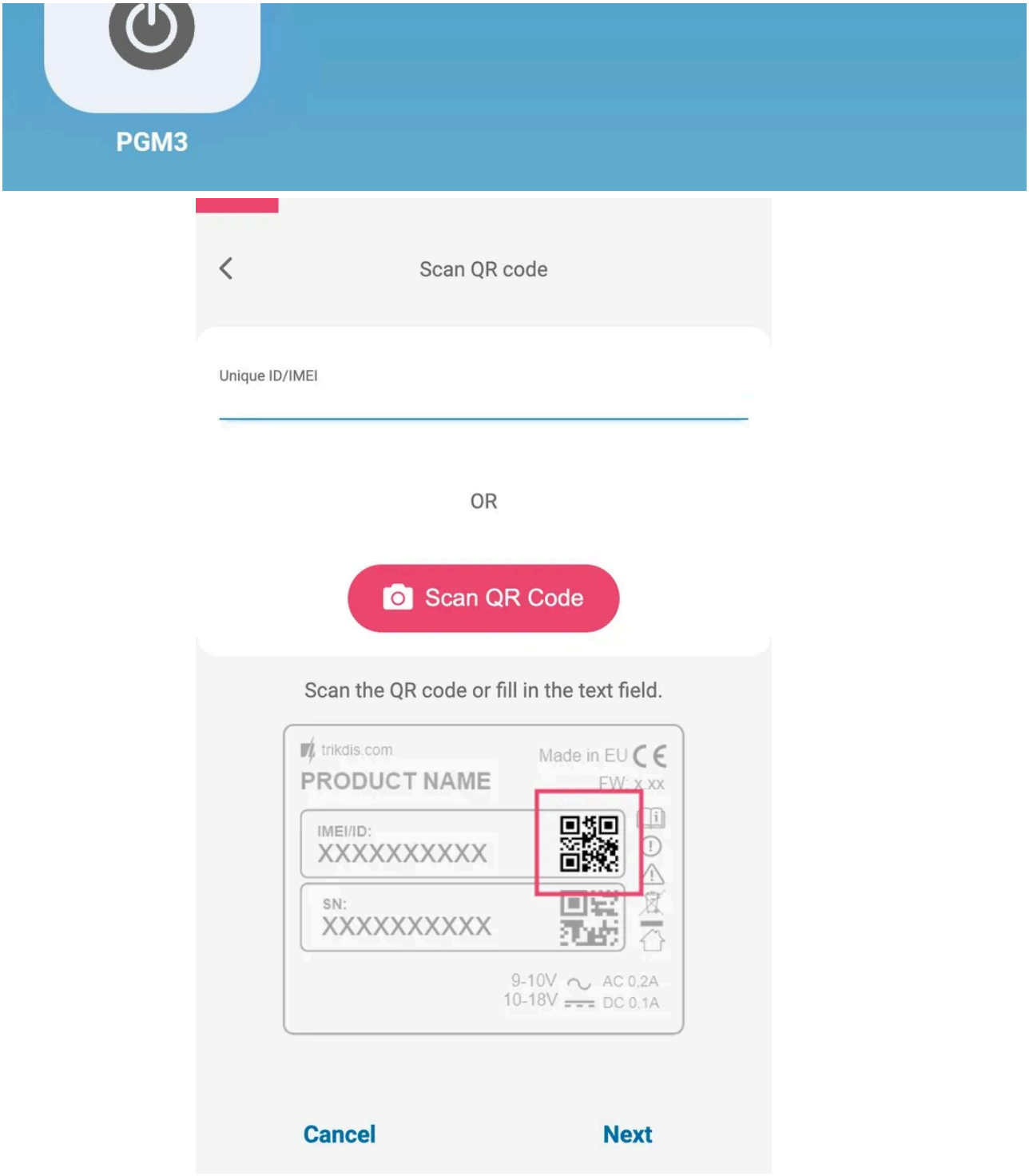


Figura 36. Protegus 2 – añadir un sistema nuevo: escribir el IMEI / Unique ID o escanear el código QR de la etiqueta, y luego Next.

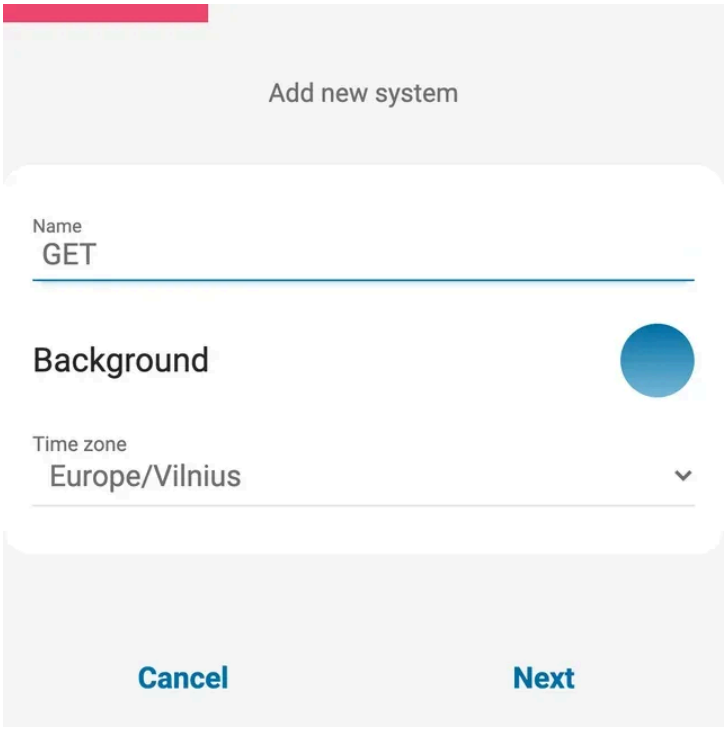


Figura 37. Protegus 2 – introducir el nombre del sistema (Name), y luego Next.

El identificador único del equipo (**IMEI / Unique ID**) se lee 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 añadirlo.

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.

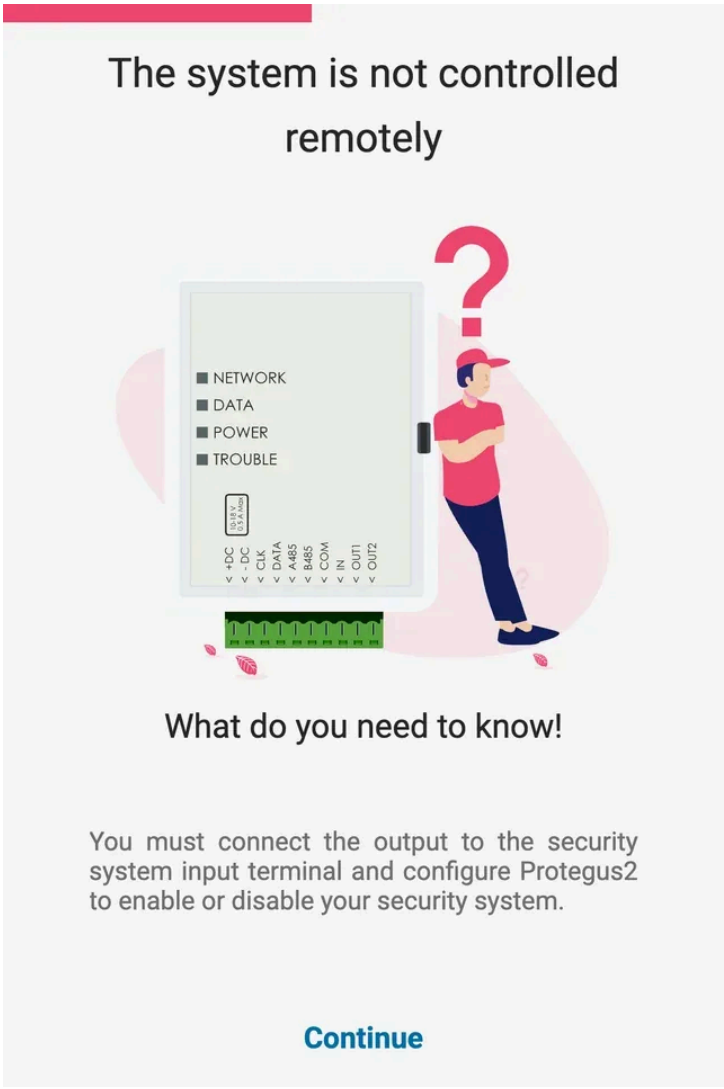


Figura 38. Protegus 2 – la página «El sistema no se controla a distancia» al crear el sistema: con el botón Continue pasas a configurar la partición y la salida PGM.

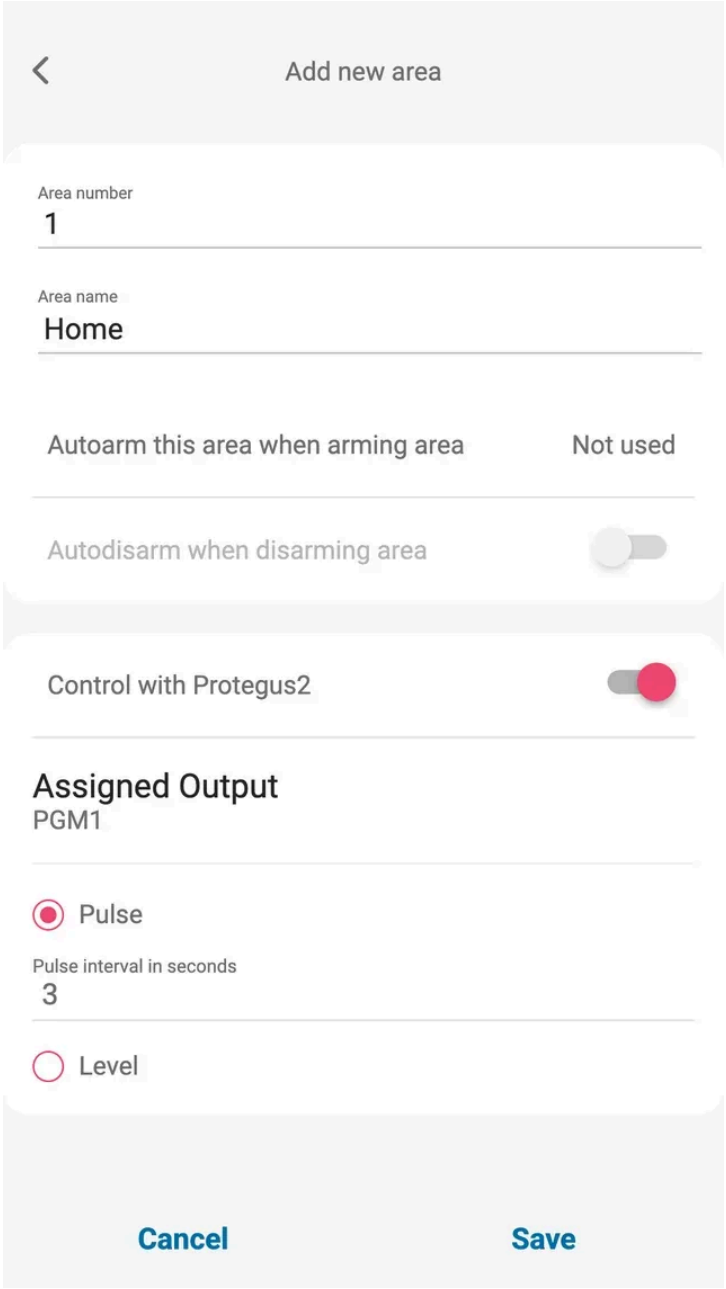


Figura 39. Protegus 2 – añadir una partición (Add new area): Area number, Area name, Control with Protegus2 activado, Assigned Output PGM1, Pulse (3 s) o Level, y luego Save.

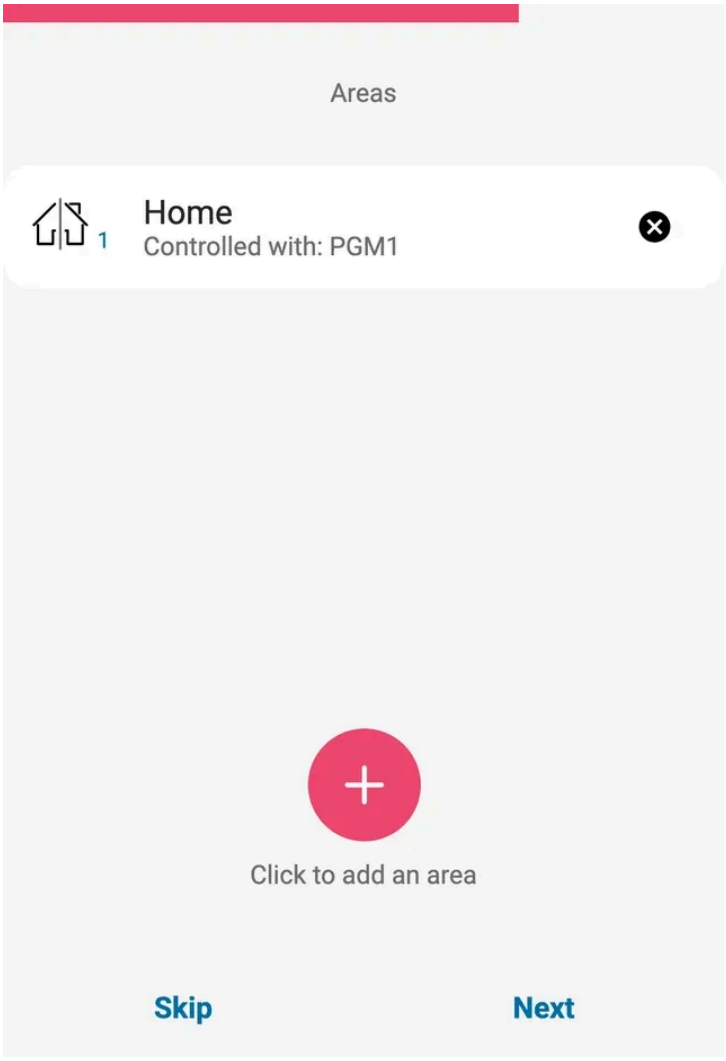


Figura 40. Protegus 2 – la lista de particiones (Areas): la partición Home la controla la PGM1; otra partición se añade con el botón Click to add an area, y el asistente se cierra con el botón Skip.

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.

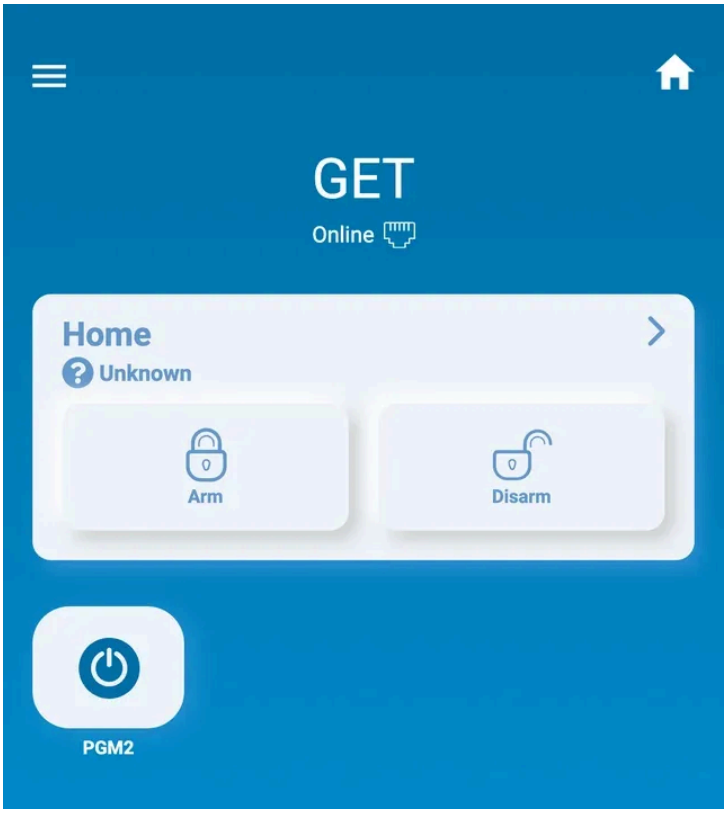


Figura 41. Protegus 2 – la pantalla de inicio del sistema: el estado de la partición, los botones Arm y Disarm y, debajo, la salida PGM que se puede accionar.

6. La configuración en detalle

La mayoría de los ajustes del GET están disponibles tanto en el programa **TrikdisConfig** para Windows como en la aplicación **Protegus 2** (**Settings** → **Advanced settings**, apartado 2.2); cuando algo solo está en una de las dos, lo indicamos. Describimos cada ajuste una sola vez e indicamos en cada apartado dónde lo encuentras en las dos herramientas; entre paréntesis figura el rótulo de la aplicación, si es distinto del de TrikdisConfig. 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, Event summary, Firmware), arriba la barra de botones (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) y abajo la barra de estado.

6.1 Conexión con el comunicador

Aplicación Protegus 2. Abre el sistema y entra en el menú **Settings** → **Advanced settings**. En la parte superior de cada pantalla se ven los datos del equipo conectado: **Unique ID** (IMEI), **Serial** (número de serie), versión de **Firmware** y de **Boot**. Los grupos de ajustes del menú son: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** y **System events**. Después de un cambio, con el botón **Write** escribes la configuración en el equipo; **Read** vuelve a leer del equipo los valores actuales.

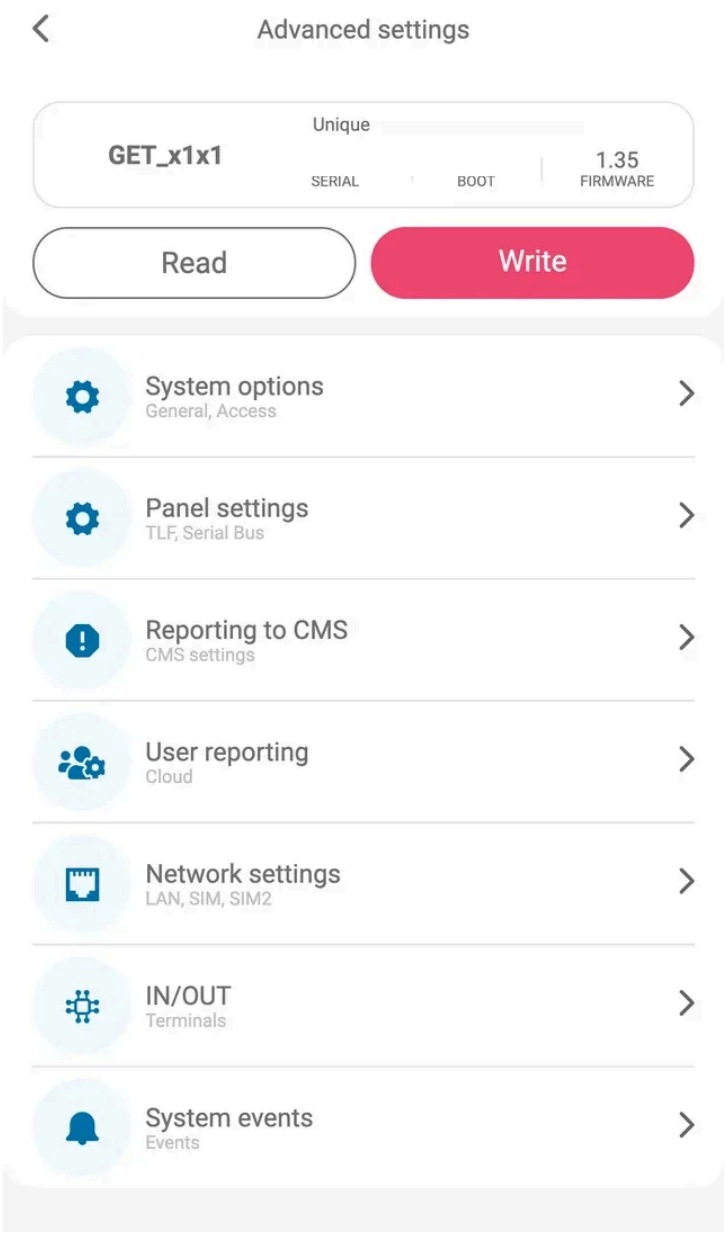


Figura 42. Protegus 2 – menú Advanced settings: arriba, los datos del equipo (modelo, Unique ID, número de serie, versión de boot y de firmware), los botones Read y Write y, debajo, los grupos de ajustes.

TrikdisConfig. Después de conectar el comunicador y pulsar **Read [F4]**, el programa muestra los datos del equipo en 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.

Rótulo	Significado
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 43. La barra de estado de TrikdisConfig con un GET leído: identificador, estado, modelo (Device: GET_S170), número de serie, versión de BL (bootloader), FW y HW, modo de conexión y nivel de acceso.

En el campo **Device** debe figurar un modelo GET (en la imagen, GET_S170; el sufijo de letras y números indica la versión de hardware); **BL** es la versión del bootloader. 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 (System options)

En la aplicación: Advanced settings → System options → System general (identificadores, sincronización horaria) y **System options → Access** (códigos y permisos del instalador). Dónde están **Account No.** y **Device account No.** depende de la versión de hardware y del firmware: en el hardware **x1x1**, con firmware **1.31** o posterior, los encuentras en la página **Reporting to CMS → CMS settings → Primary channel** (**Primary Account no.**; en el canal paralelo, **Parallel Account no.**) y en la página **Reporting to CMS → Settings** (**Device account No.**), y en la página System general solo queda **Time set**; en los demás casos, los dos están en la página System general.

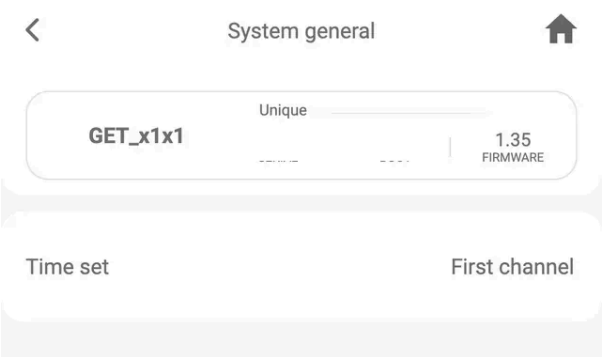


Figura 44. Protegus 2 – System options → System general en el hardware x1x1 (firmware 1.35): solo se ve Time set; los identificadores están entre los ajustes de la CRA.

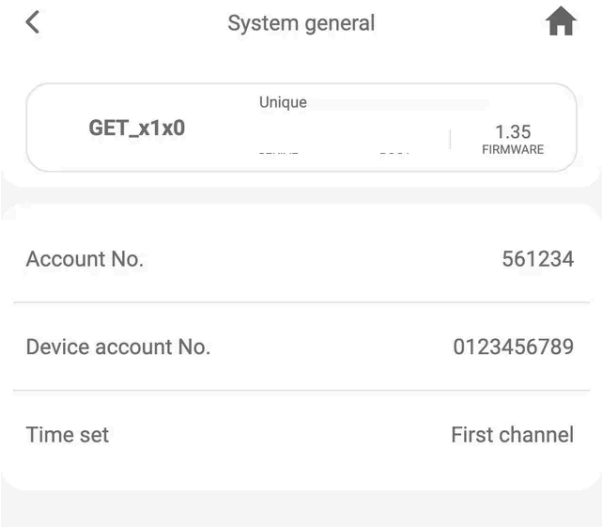


Figura 45. Protegus 2 – System options → System general en el hardware x1x0: Account No., Device account No. y Time set.

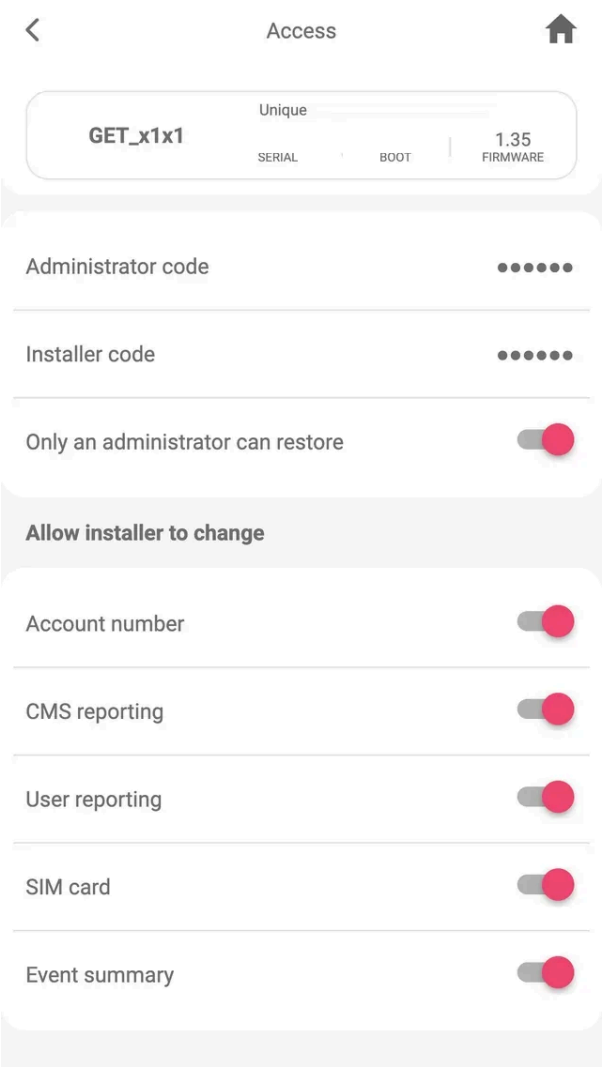


Figura 46. Protegus 2 – System options → Access: Administrator code, Installer code, Only an administrator can restore y la lista Allow installer to change (Account number, CMS reporting, User reporting, SIM card, Event summary).

En TrikdisConfig: la página **System settings** consta de dos grupos: en el grupo **General** configuras los identificadores del equipo y en el grupo **Access** los niveles de acceso.

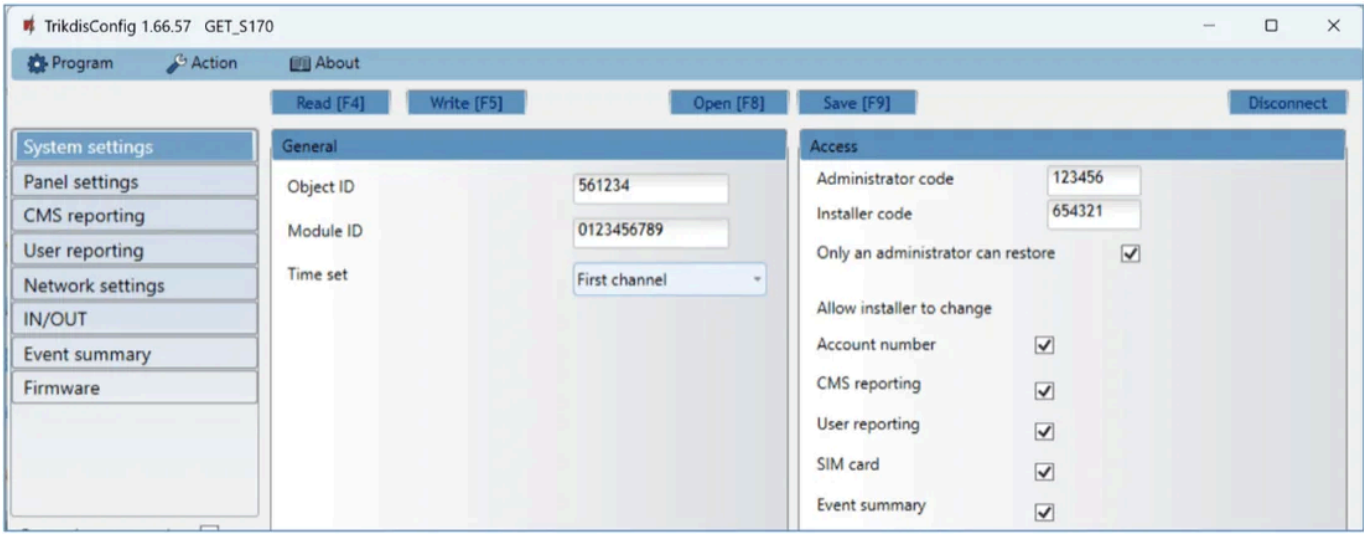


Figura 47. TrikdisConfig – página System settings: grupo General (Object ID, Module ID, Time set) y grupo Access (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.): el número de abonado recibido de la CRA (6 caracteres hexadecimales: 0–9, A–F; `FFFE` y `FFFF` no se pueden usar). Es obligatorio si el equipo también transmite a una CRA.
- **Module ID** (Device account No.): 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.

Acceso de instalador en la aplicación. Si abres el comunicador con el código de instalador, Protegus 2 oculta los campos **Administrator code** y **Only an administrator can restore**, y muestra solo como lectura los ajustes que el administrador no ha permitido. En la aplicación, el permiso **SIM card** también se aplica a los ajustes de LAN; donde los identificadores están entre los ajustes de la CRA (ver arriba), se les aplica el permiso **CMS reporting**.

6.3 Panel settings

En esta página indicas cómo está conectado el comunicador a la central de alarma: el grupo **TLC** (en la aplicación, **TLF**) contiene los ajustes de la conexión por línea telefónica (TIP/RING), y el grupo **Serial bus** (**Serial Bus**), los de la conexión al bus de datos o serie. En la aplicación: **Advanced settings → Panel settings → TLF** o **Panel settings → Serial Bus**.

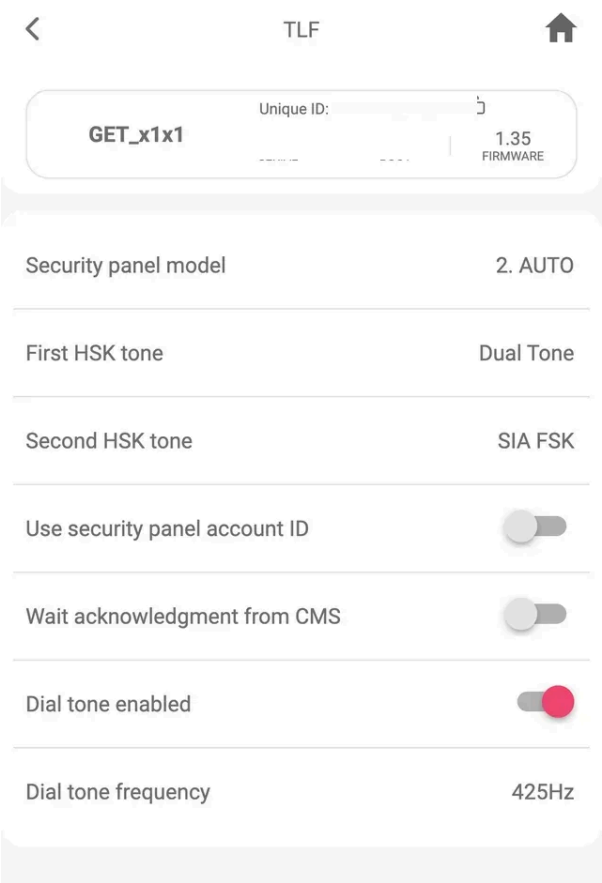


Figura 48. Protegus 2 – Panel settings → TLF: Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.

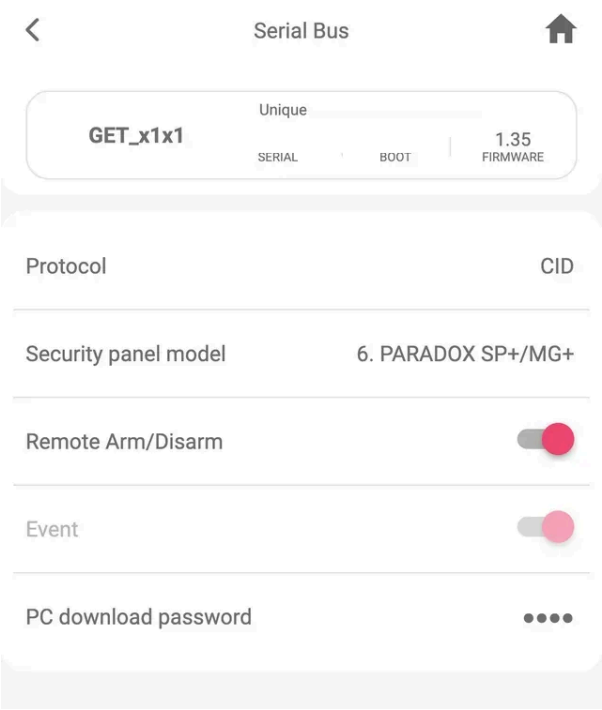


Figura 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm activado, Event (solo lectura), PC download password.

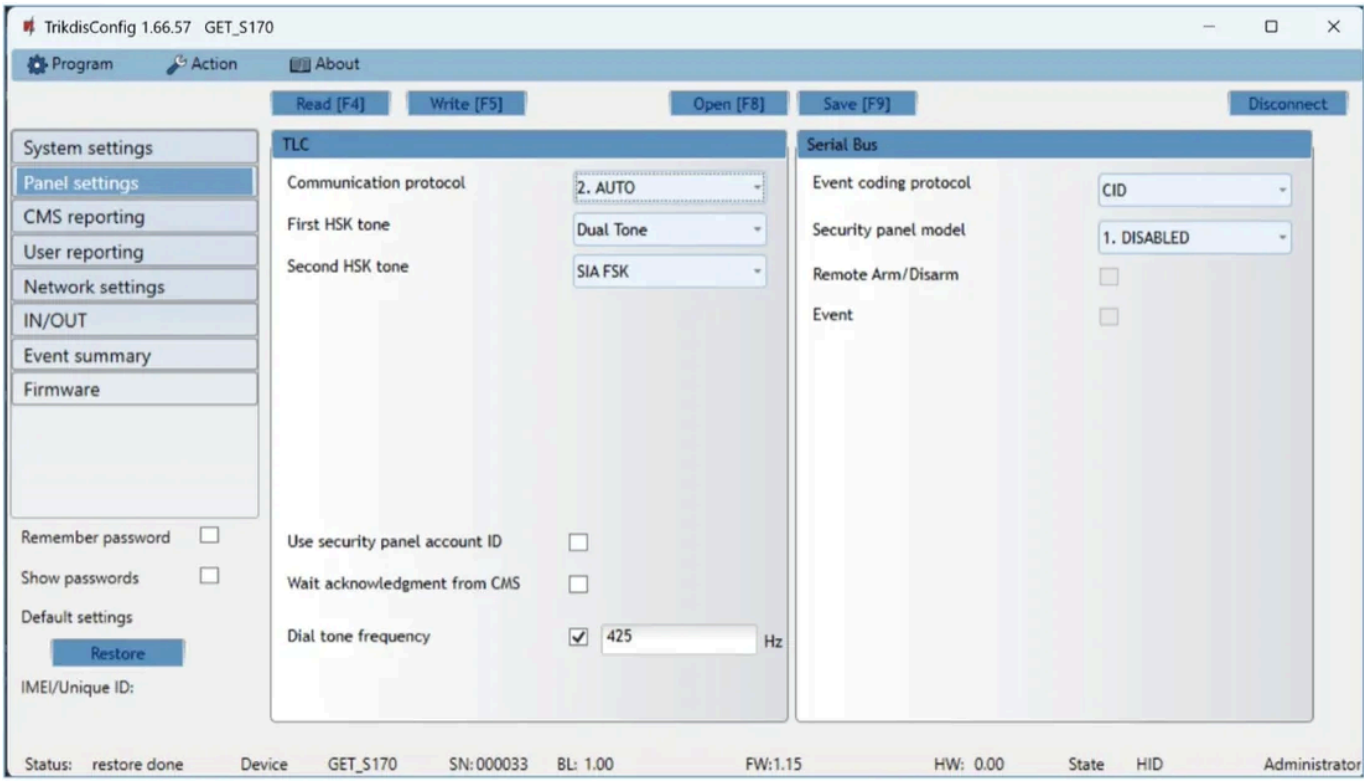


Figura 50. TrikdisConfig – Panel settings en la conexión TIP/RING: en el grupo TLC, Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; el grupo Serial bus aparece entonces en gris.

Grupo TLC: si el comunicador está conectado a los bornes TIP/RING del comunicador telefónico de la central:

- **Communication protocol** (Security panel model): activa (**2. AUTO**) o desactiva (**1. DISABLED**) la interfaz telefónica DTMF del comunicador. En la conexión TIP/RING, elige el valor AUTO.

- **First HSK tone**, **Second HSK tone**: el tono de saludo (handshake) de la central con el que el comunicador atiende al marcador de la central (en la imagen, Dual Tone y SIA FSK).
- **Use security panel account ID**: marcado, el comunicador no envía el valor de su propio campo **Object ID**, sino el número de abonado configurado en la central y enviado por ella.
- **Wait acknowledgment from CMS**: marcado, después de enviar cada evento el comunicador espera la confirmación del receptor IP de que el mensaje ha llegado; si la confirmación no llega, no da la señal de «kiss-off» a la central, y el comunicador telefónico de la central repite el mensaje.
- **Dial tone frequency**: la frecuencia del tono de invitación a marcar con la que el comunicador se comunica con el marcador de la central (por defecto, 425 Hz, que es también el tono de invitación a marcar en España y en la mayoría de los países europeos). En la página TLF de la aplicación hay además el interruptor **Dial tone enabled**: activa o desactiva el tono de invitación a marcar; la frecuencia solo se puede cambiar con el tono activado.

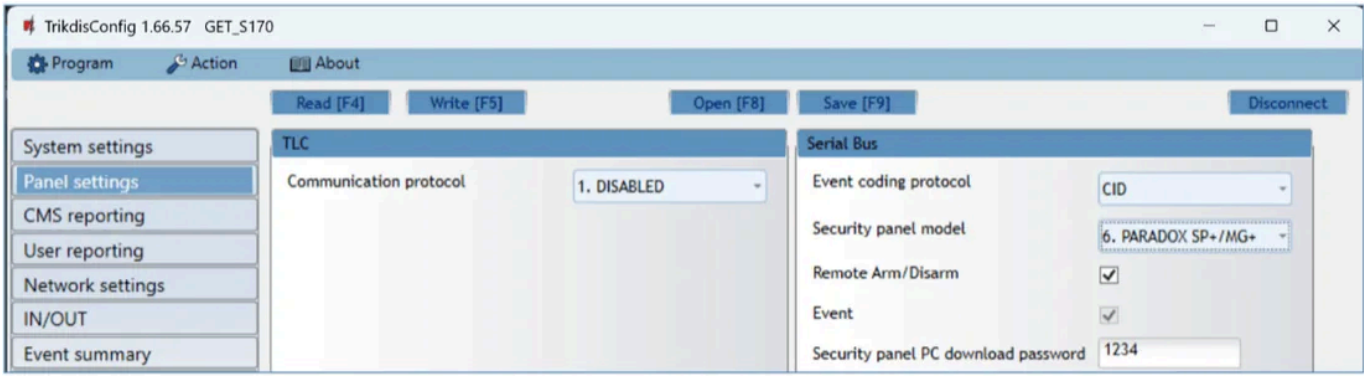


Figura 51. TrikdisConfig – Panel settings en la conexión al bus de datos o serie: Communication protocol 1. DISABLED; en el grupo Serial bus, Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm y Event marcados, Security panel PC download password introducida.

Grupo Serial bus: si el comunicador está conectado al bus de datos o al puerto serie de la central:

- **Event coding protocol** (Protocol): el protocolo de transmisión de eventos: **CID** o **SIA**.
- **Security panel model**: el modelo de la central de alarma conectada, elegido de la lista (para la conexión Keybus + TIP/RING de Paradox SP / SP+ / MG / MG+, elige el elemento **Paradox SP+/MG+ series KeyBus**, apartado 3.3.3).
- **Remote Arm/Disarm**: marcado, el comunicador controla la central directamente (armado y desarmado desde Protegus 2). Solo se ve en las centrales de control directo. Para el control directo también hay que configurar la central según el apartado 4.1.
- **Event**: marcado, el comunicador envía los eventos de la central a la CRA y a Protegus 2. La aplicación muestra este interruptor, pero allí no se puede cambiar.
- **Security panel PC download password** (PC download password; en Texecom, el UDL passcode): para el control directo de una central Paradox o Texecom, la contraseña PC o UDL; debe coincidir con la contraseña configurada en la central, cuya introducción se describe en el apartado 4.1.

6.4 CMS reporting (Reporting to CMS)

El comunicador envía los eventos a la CRA por conexión IP, por la red cableada (LAN) o por la red móvil (SIM1, SIM2), en el orden configurado en el apartado 6.4.2. 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 el canal correspondiente se interrumpe. La comunicación está cifrada y protegida con contraseña. Los protocolos TRK necesitan un receptor Trikdis que reciba los eventos y los

transmita al software de la CRA: para la conexión IP, el receptor por software IPcom (Windows o Linux), el receptor IP/SMS RL14 o el receptor multicanal RM14; los protocolos DC-09 y TL150 son para los receptores universales y SUR-GARD, respectivamente (ver abajo, **Protocol**).

6.4.1 Canales del receptor (CMS settings)

En la aplicación: Advanced settings → Reporting to CMS → CMS settings y luego **Primary channel**, **Backup channel** o **Parallel channel** (dentro de este, **Parallel primary channel** y **Parallel backup channel**). Al activar el interruptor **Enabled** aparecen los ajustes del canal.

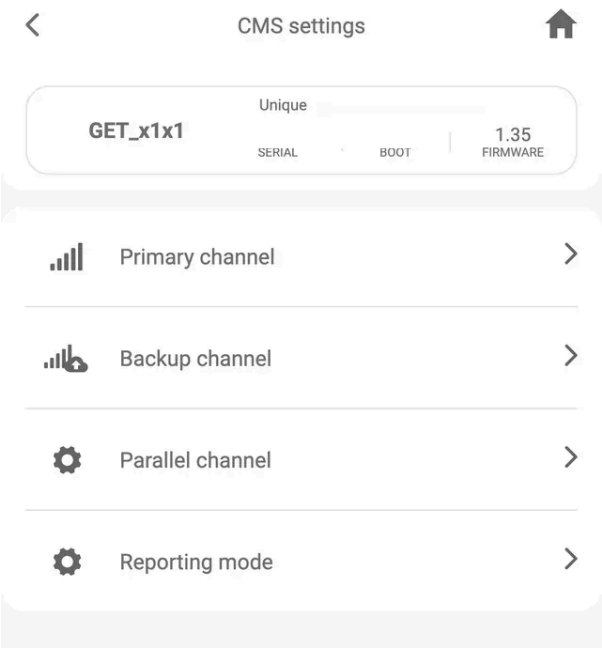


Figura 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel y Reporting mode.

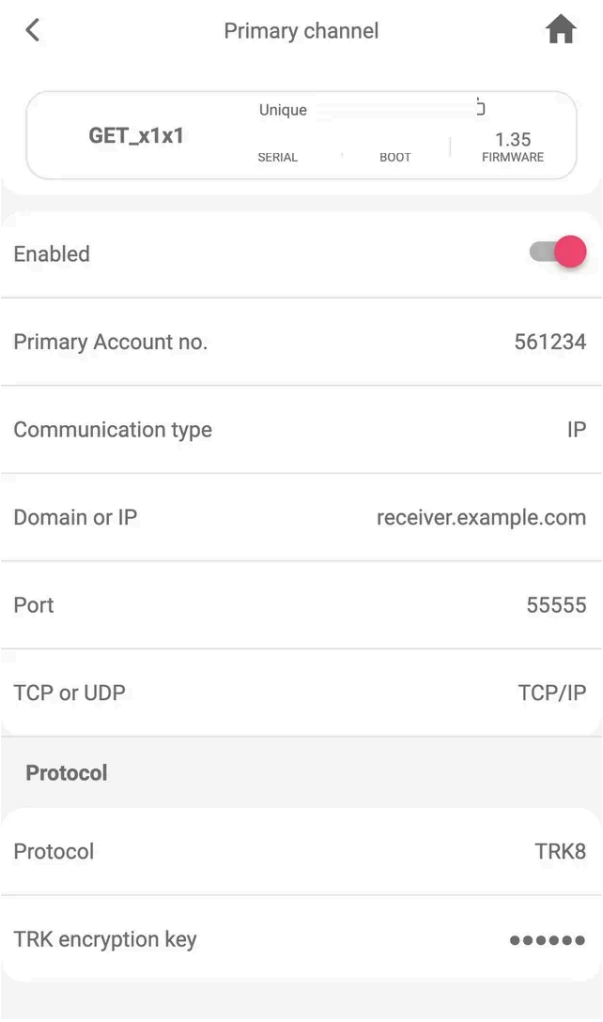


Figura 53. Protegus 2 – Primary channel en el hardware x1x1: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 y la TRK encryption key.

En TrikdisConfig: la pestaña **CMS settings** de la página **CMS reporting**.

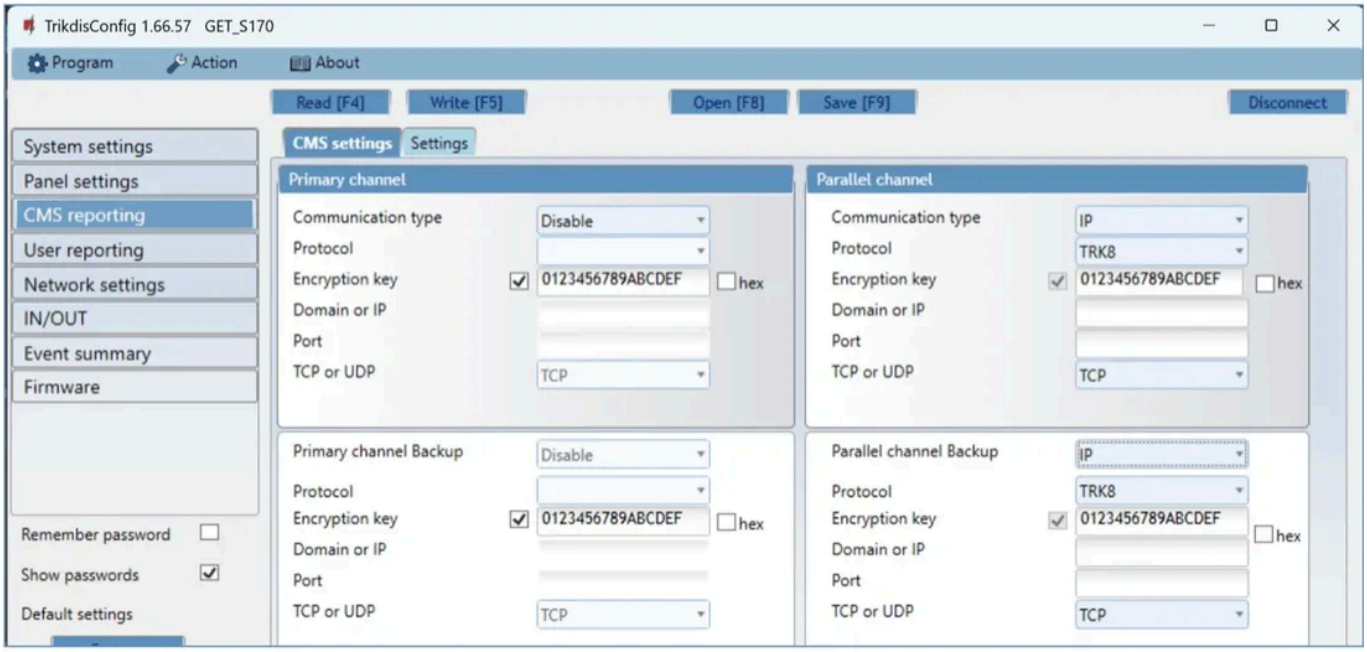


Figura 54. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal y su respaldo, canal paralelo y su respaldo (en la imagen, el canal paralelo con la configuración IP / TRK8 / TCP).

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** (TRK encryption key; con los protocolos DC-09, **Enable encryption key** y **DC-09 encryption key**, con el interruptor **HEX** para una clave hexadecimal): la clave de cifrado de los mensajes; debe ser la misma en el comunicador y en el receptor. En la aplicación, la TRK encryption key tiene como máximo 6 caracteres y la DC-09 encryption key como máximo 16 (32 en HEX).
- **Domain or IP**, **Port**: el nombre de dominio o la dirección IP del receptor y su puerto de red.
- **TCP or UDP**: el protocolo de transmisión.

Primary channel Backup – canal de respaldo. Activado, toma el relevo de la comunicación si el canal principal no funciona; sus ajustes son iguales que los anteriores.

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.

6.4.2 Test, PING y orden de las conexiones

En la aplicación: Advanced settings → Reporting to CMS → Settings (test, PING, tiempos del canal de respaldo, número de receptor y de línea) y **Reporting to CMS → CMS settings → Reporting mode** (orden de las vías de conexión). En la aplicación, junto a cada intervalo hay un interruptor: **Enable test** para Test period, **Enable ping** para IP ping period y **Test enabled** para Communication path test; en la página Reporting mode, los tipos de conexión figuran con los nombres **LAN**, **SIM** (la SIM1) y **SIM2**.

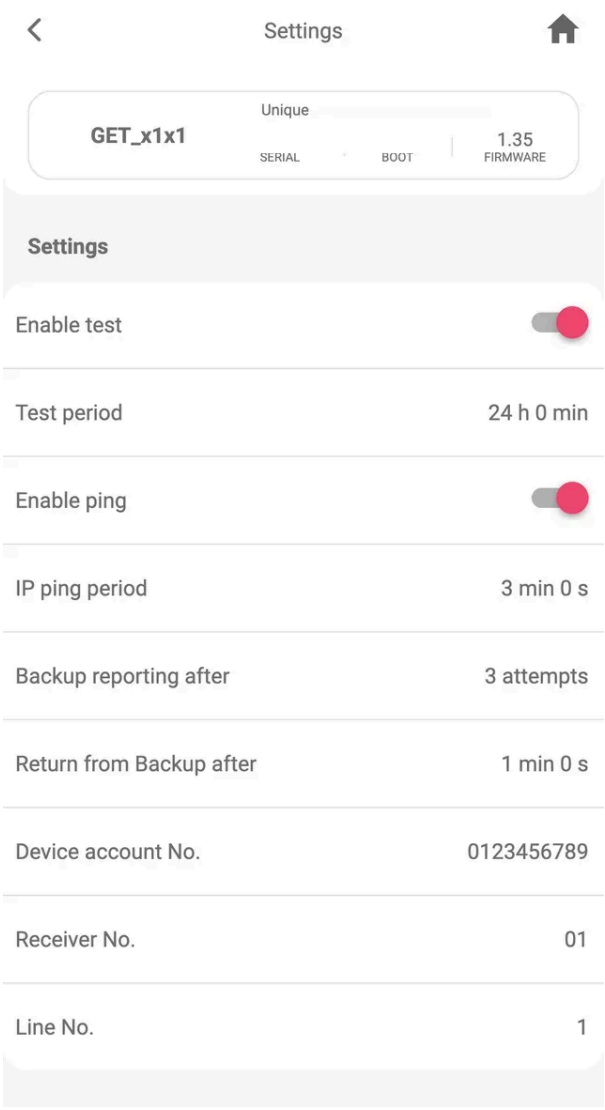


Figura 55. Protegus 2 – Reporting to CMS → Settings en el hardware x1x1: Enable test y Test period, Enable ping e IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.

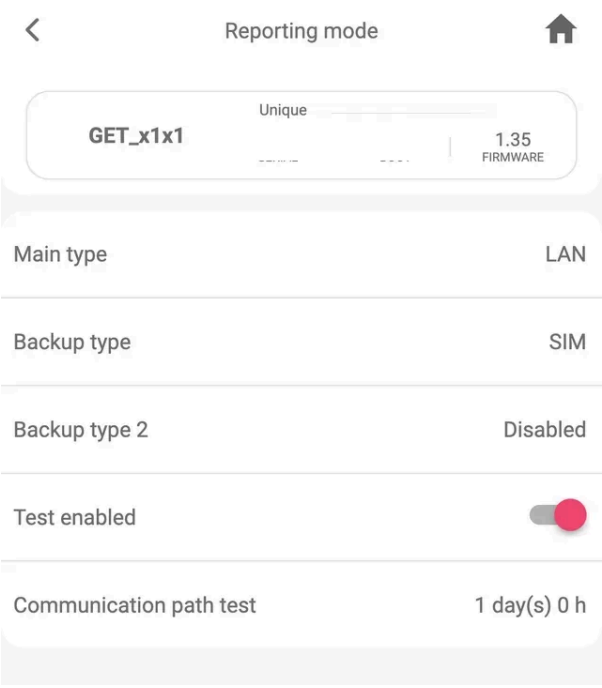


Figura 56. Protegus 2 – CMS settings → Reporting mode: Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled y Communication path test.

En TrikdisConfig: la pestaña **Settings** de la página **CMS reporting**.

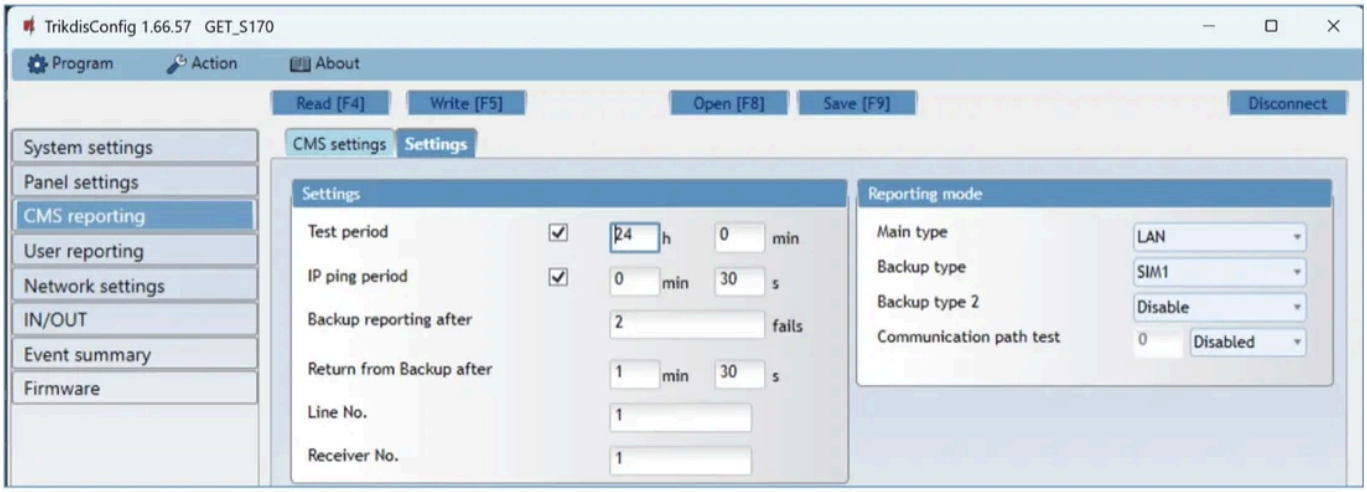


Figura 57. TrikdisConfig – CMS reporting, pestaña Settings: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; en el grupo Reporting mode, Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **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 GET también están aquí los campos **Line No.** (número de línea del receptor) y **Receiver No.** (número de receptor); el GET no tiene un campo aparte «Object ID in DC-09».

Grupo Reporting mode: aquí indicas por qué vía se comunica el comunicador con los canales de la CRA y con Protegus 2. Los tipos de conexión se indican por orden: si la conexión según **Main type** no se establece, el comunicador pasa a la de **Backup type**, y así sucesivamente; si el mensaje se ha podido enviar por la vía de respaldo, pasado el tiempo indicado (Return from backup after) vuelve a intentar la vía principal.

- **Main type**: el tipo de la conexión principal con el receptor y con Protegus 2: **LAN**, **SIM1** o **SIM2**.
- **Backup type**: el tipo de la conexión de respaldo (LAN, SIM1, SIM2).
- **Backup type 2**: el tipo de la segunda conexión de respaldo (LAN, SIM1, SIM2).
- **Communication path test**: con qué intervalo prueba el comunicador los tipos de conexión elegidos (LAN, SIM1, SIM2).

6.5 User reporting (Protegus Cloud)

Con el servicio Protegus 2, el usuario supervisa y controla a distancia el comunicador y el sistema conectado a él; detalles: web.protegus.app. En la aplicación: **Advanced settings** → **User reporting** → **Cloud**; en TrikdisConfig, la pestaña **PROTEGUS Cloud** de la página **User reporting**.

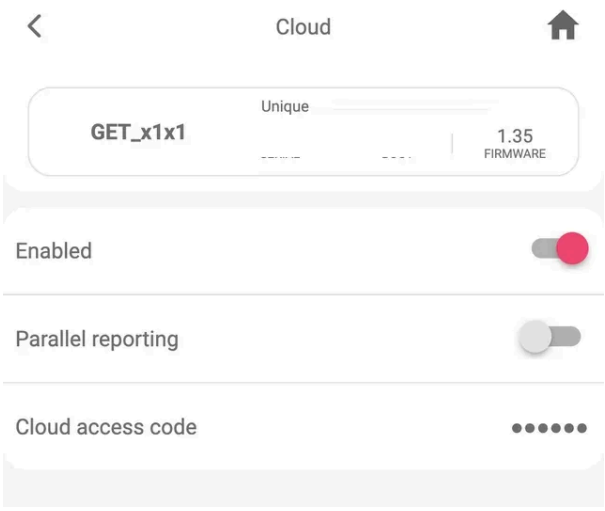


Figura 58. Protegus 2 – User reporting → Cloud: Enabled, Parallel reporting, Cloud access code.

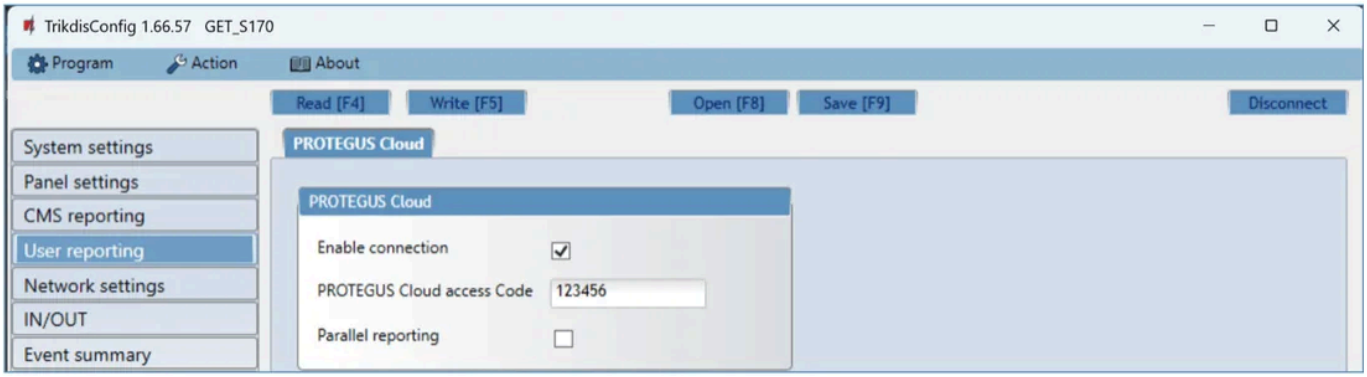


Figura 59. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled): habilita el servicio Protegus 2: el equipo intercambia datos con la aplicación Protegus 2, y TrikdisConfig también puede acceder a él a distancia.
- **PROTEGUS Cloud access Code** (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** (en la aplicación solo se ve si el firmware lo admite): marcado, los mensajes van a la vez por el canal principal (a la CRA) y a Protegus 2; Protegus 2 y los usuarios reciben el mensaje solo después de que se haya enviado a la CRA.

6.6 Network settings

6.6.1 LAN (Ethernet)

Estos ajustes hay que introducirlos si el comunicador está conectado a la red local cableada (LAN). En la aplicación: **Advanced settings → Network settings → LAN**; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** y **DNS2** solo se pueden cambiar con **Use DHCP** desactivado. En TrikdisConfig, la pestaña **LAN** de la página **Network settings**, grupo **Ethernet settings**.

¿Qué necesita la red? El propio comunicador inicia la conexión saliente hacia el receptor de la CRA y hacia la nube Protegus, por lo que en el router **no hace falta abrir ni redirigir puertos**, ni tampoco una IP pública fija o un DNS dinámico. Lo que sí hace falta:

- un puerto Ethernet libre en el router o switch;
- DHCP (ajuste de fábrica), o bien la IP fija, la máscara de subred, la puerta de enlace y el DNS que te dé el administrador de red;
- permitir el tráfico saliente hacia la dirección y el puerto del receptor (TCP o UDP, según la configuración del receptor), así como hacia la nube Protegus.

En una red filtrada –de empresa o institucional– acuérdalo antes con el administrador de red: en los routers domésticos todas las conexiones salientes están permitidas por defecto, pero en una red protegida por cortafuegos puede hacer falta una regla específica.

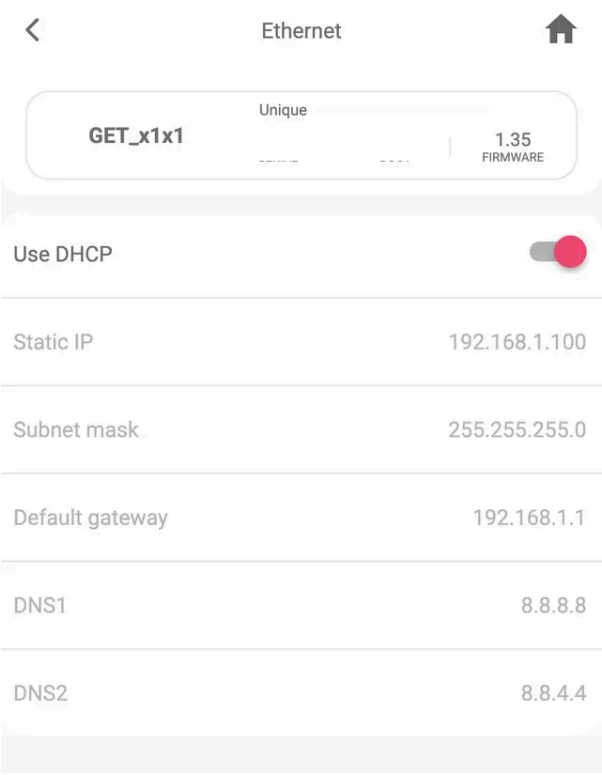


Figura 60. Protegus 2 – Network settings → LAN: Use DHCP activado; los campos Static IP, Subnet mask, Default gateway, DNS1 y DNS2 aparecen entonces en gris.



Figura 61. TrikdisConfig – Network settings, pestaña LAN, grupo Ethernet settings: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

- **Use DHCP**: marcado, el comunicador se conecta automáticamente a la red (recibe la dirección del servidor DHCP del router). Si la conexión automática no funciona, las direcciones hay que introducirlas a mano:
- **Static IP**: la dirección IP fija del comunicador en la configuración manual.
- **Subnet mask**: la máscara de subred en la configuración manual.
- **Default gateway**: la dirección de la puerta de enlace (router) en la configuración manual.
- **DNS1, DNS2**: servidores de nombres (DNS, Domain Name System: da la dirección IP que corresponde a un nombre de dominio); hacen falta si has indicado el receptor en el campo **Domain or IP** del canal con un nombre de dominio y no con una dirección IP. Por defecto, el DNS público de Google. Independientemente de la configuración IP, comprueba que las direcciones DNS funcionan con tu proveedor de internet.

6.6.2 SIM1 y SIM2

Estos ajustes hay que introducirlos por separado para cada tarjeta SIM colocada; los ajustes de las ranuras SIM1 y SIM2 son iguales.

Antes de usarla, asegúrate de que la tarjeta SIM está activa y funciona, y de que la tarjeta tiene habilitado también el servicio de datos móviles.

En la aplicación: **Advanced settings** → **Network settings** → **SIM** (la SIM1) o **SIM2**. En TrikdisConfig, la pestaña **SIM1** o **SIM2** de la página **Network settings**, grupo **SIM card**.

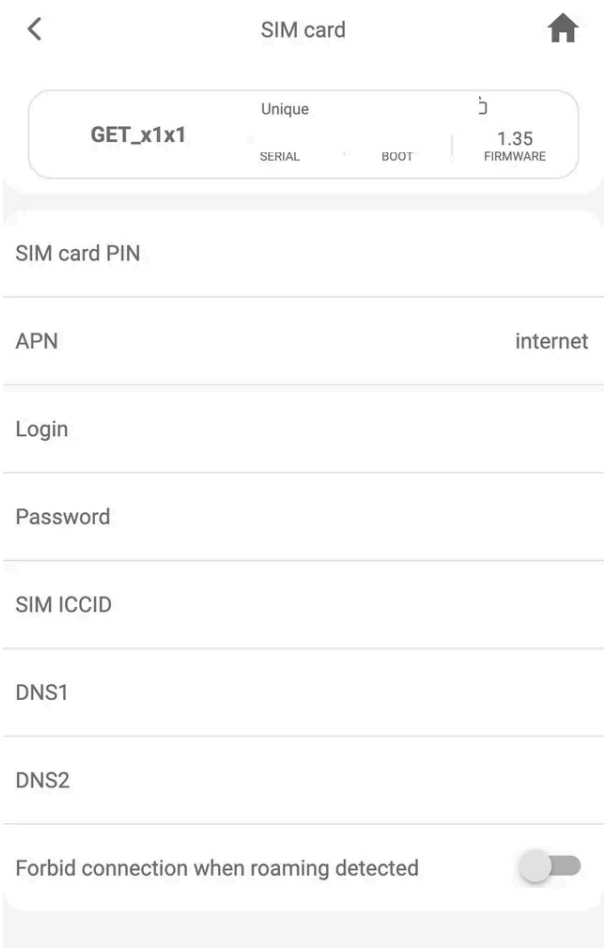


Figura 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 y el interruptor Forbid connection when roaming detected.

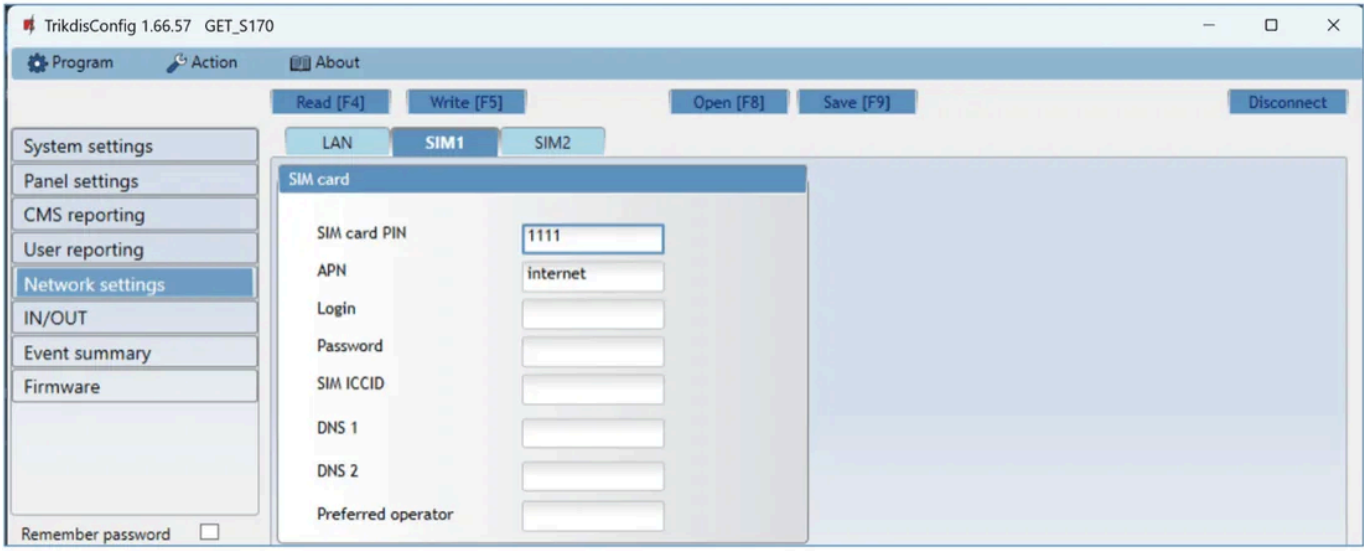


Figura 63. TrikdisConfig – Network settings, pestaña SIM1, grupo SIM card: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (la pestaña SIM2 es igual).

- **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 puede quedar el valor de fábrica del campo.
- **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 2.3).
- **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 esa tarjeta.
- **DNS1, DNS2**: servidores de nombres; hacen falta si has indicado el receptor en el campo **Domain or IP** del canal con un nombre de dominio. Por defecto, el DNS público de Google; comprueba que las direcciones DNS funcionan con tu operador.
- **Preferred operator**: el código del operador móvil (MCC + MNC); si lo indicas, el equipo solo se conecta a la red del operador elegido. **Solo está en TrikdisConfig**.

En la página SIM de la aplicación, en lugar de Preferred operator está el interruptor **Forbid connection when roaming detected**: activado, el comunicador no se conecta si detecta itinerancia (roaming). En la versión de hardware **M15**, con firmware **1.17** o posterior, en la página SIM aparecen también los ajustes **Generation** y **Bands**: con ellos puedes limitar qué tecnología de red móvil y qué bandas de frecuencia usa el comunicador.

6.7 IN/OUT

Aquí indicas la función de los dos bornes I/O de doble función del comunicador: **Disabled** (no se usa), **IN** (entrada) u **OUT** (salida; en el GET, esta es la configuración de fábrica). 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). A las entradas se pueden conectar otros detectores: cuando se activa el detector, el comunicador envía un evento propio, con el código Contact ID (SIA) asignado a la entrada, a la CRA y a Protegus 2.

En la aplicación: **Advanced settings** → **IN/OUT** y luego el borne **1** o **2**: **Function** (Disabled, IN, OUT) y, en una entrada, **Type**; en las partes **Alarm** y **Tamper**, los mensajes de evento y de restauración que se envían cuando se activa la entrada. En TrikdisConfig, la página **IN/OUT**.

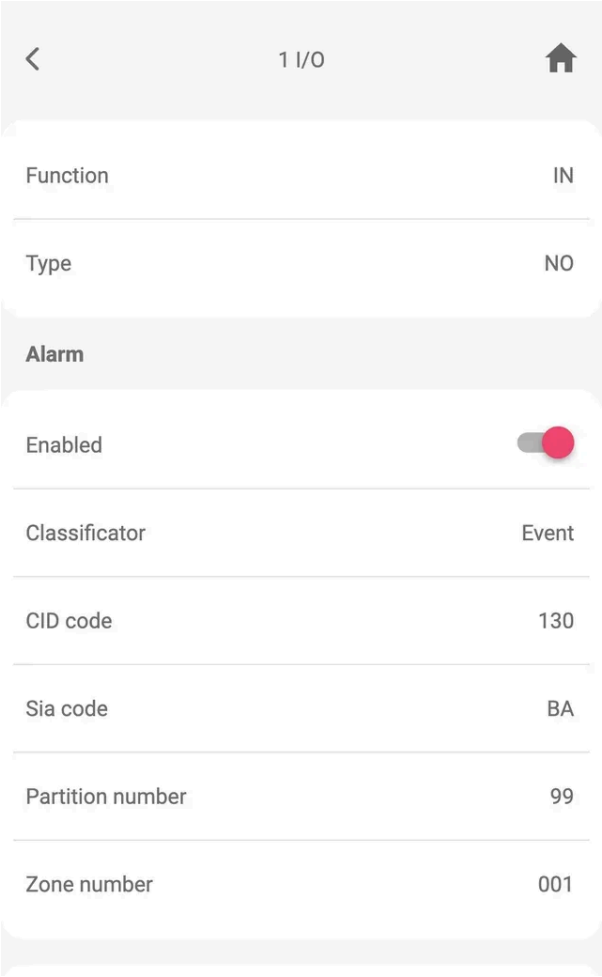


Figura 64. Protegus 2 – IN/OUT, borne 1: Function IN, Type NO; el evento Alarm Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.

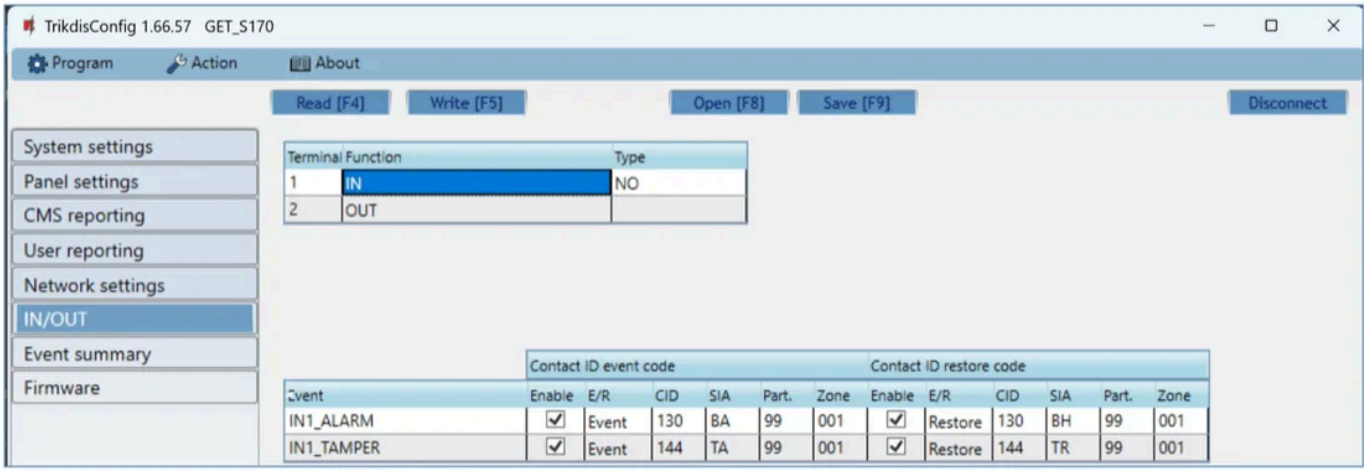


Figura 65. TrikdisConfig – página IN/OUT: el borne 1 es entrada (IN, NO), el 2 salida (OUT); debajo, los eventos de alarma y de sabotaje de la entrada 1 con código CID y SIA.

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

- **Enable** (Enabled): habilita el envío del mensaje a la CRA y a Protegus 2.

- **E/R** (Classificator): el tipo de mensaje: Event (evento) o Restore (restauración).
- **CID** (CID code): el código Contact ID (se puede cambiar o dejar el de fábrica); cuando se activa la entrada, el mensaje va con este código a Protegus 2 y a la CRA.
- **SIA** (Sia code): el código SIA (se puede cambiar o dejar el de fábrica).
- **Part.** (Partition number): el número de partición en el mensaje (tanto en el evento como en la restauración).
- **Zone** (Zone number): el número de zona en el mensaje.

6.8 Event summary (System events)

Aquí puedes habilitar, deshabilitar y modificar los mensajes internos propios del equipo. Un mensaje deshabilitado aquí no se envía, sea cual sea cualquier otro ajuste. En la aplicación: **Advanced settings** → **System events**; los mensajes están en las listas **Event** y **Restore**; para modificar uno, selecciónalo. En TrikdisConfig, la página **Event summary**.

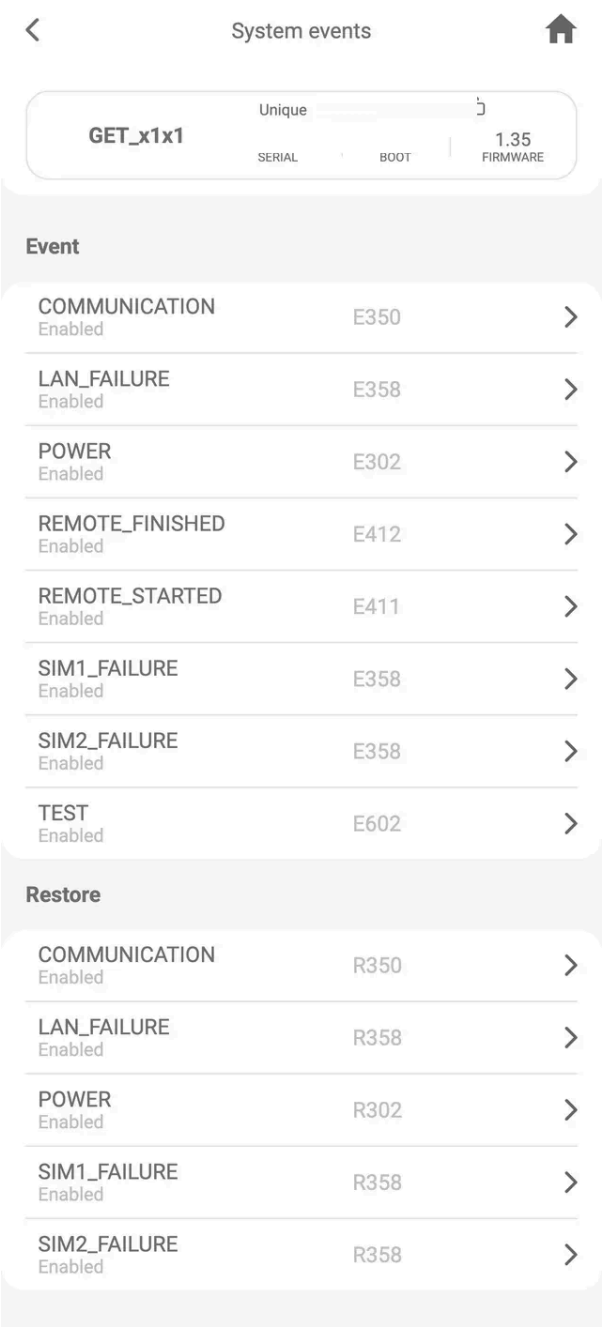


Figura 66. Protegus 2 – System events: la lista Event (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) y la lista Restore.

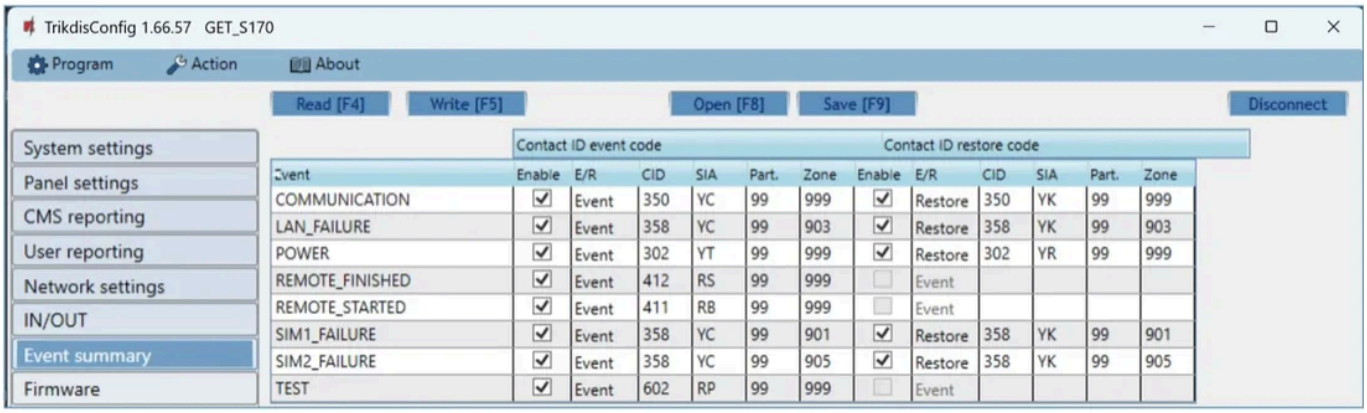


Figura 67. TrikdisConfig – página Event summary: los mensajes internos del equipo con código CID y SIA, con la partición 99.

Los mensajes internos del GET (entre paréntesis, el código Contact ID y la zona de fábrica):

- **COMMUNICATION** (350, zona 999): fallo de la conexión entre la central y el comunicador; su restauración es un mensaje aparte.
- **LAN_FAILURE** (358, zona 903): fallo de la conexión de red cableada (LAN); su restauración es un mensaje aparte.
- **POWER** (302, zona 999): tensión de alimentación baja; su restauración es un mensaje aparte.
- **REMOTE_FINISHED** (412): fin de la programación a distancia con TrikdisConfig (desconexión).
- **REMOTE_STARTED** (411): conexión a distancia para programar el GET con TrikdisConfig.
- **SIM1_FAILURE** (358, zona 901): fallo de la conexión a la red móvil en la SIM1; su restauración es un mensaje aparte.
- **SIM2_FAILURE** (358, zona 905): fallo de la conexión a la red móvil en la SIM2; su restauración es un mensaje aparte.
- **TEST** (602): informe de test periódico.

La activación y el intervalo del mensaje periódico TEST se configuran en el campo **Test period** (apartado 6.4.2).

- **Enable** (Enabled): marcado, el envío del mensaje está habilitado.
- En cada mensaje se pueden modificar el código Contact ID (SIA) y los números de zona y de partición.

6.9 Restablecer la configuración de fábrica

Desde la aplicación Protegus 2 **no** se puede restablecer la configuración de fábrica: hace falta el botón **Restore** de TrikdisConfig o el botón **RESET** del equipo.

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 68. TrikdisConfig – el botón Restore del grupo Default settings.

La configuración de fábrica también se puede restablecer en el propio equipo, sin ordenador: con la alimentación encendida, pulsa y mantén pulsado el botón **RESET** del circuito impreso (apartado 1.4) durante **10 segundos**, hasta que se apaguen los LED NETWORK, POWER y TROUBLE y luego se encienda el LED POWER. Entonces suelta el botón: la configuración de fábrica se ha 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.

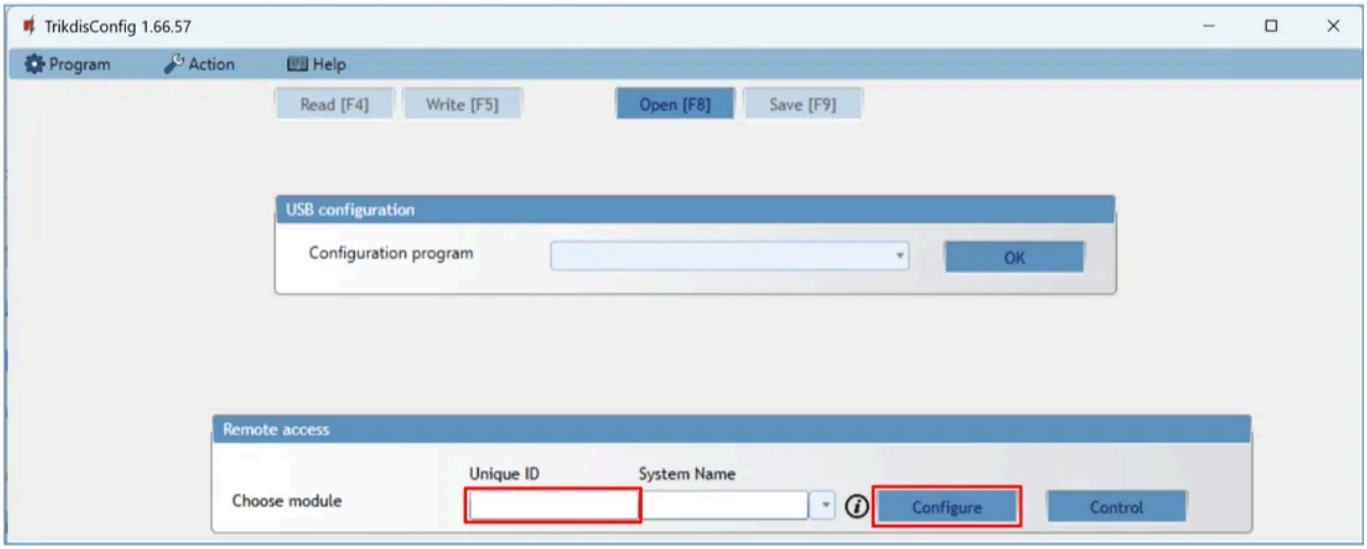


Figura 69. TrikdisConfig – el grupo Remote access: el campo Unique ID, la lista System name y el botón Configure.

El identificador único del GET es el **IMEI / Unique ID**; se lee en la etiqueta del equipo y en la pegatina de la caja. El acceso a distancia solo funciona si la tarjeta SIM está activa y su código PIN está introducido o la petición de PIN está desactivada –**o bien** el comunicador está conectado con un cable de red (LAN)–; si en la página **User reporting** → **PROTEGUS Cloud** está marcada la opción **Enable connection** (apartado 6.5); si el LED **POWER** está verde fijo; y si el LED **NETWORK LTE** está verde fijo y parpadea en amarillo (si solo hay conexión cableada, el LED **NETWORK LAN** está verde fijo). El comunicador informa del inicio y del final de la programación a distancia con los mensajes REMOTE_STARTED y REMOTE_FINISHED (apartado 6.8).

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.

Si el comunicador transmite tanto por la red cableada como por la red móvil (apartado 6.4.2, Reporting mode), conviene hacer la prueba por las dos vías: desconecta el cable LAN, provoca un evento y comprueba que también llega a la CRA a través de la tarjeta SIM; después vuelve a conectar el cable.

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.

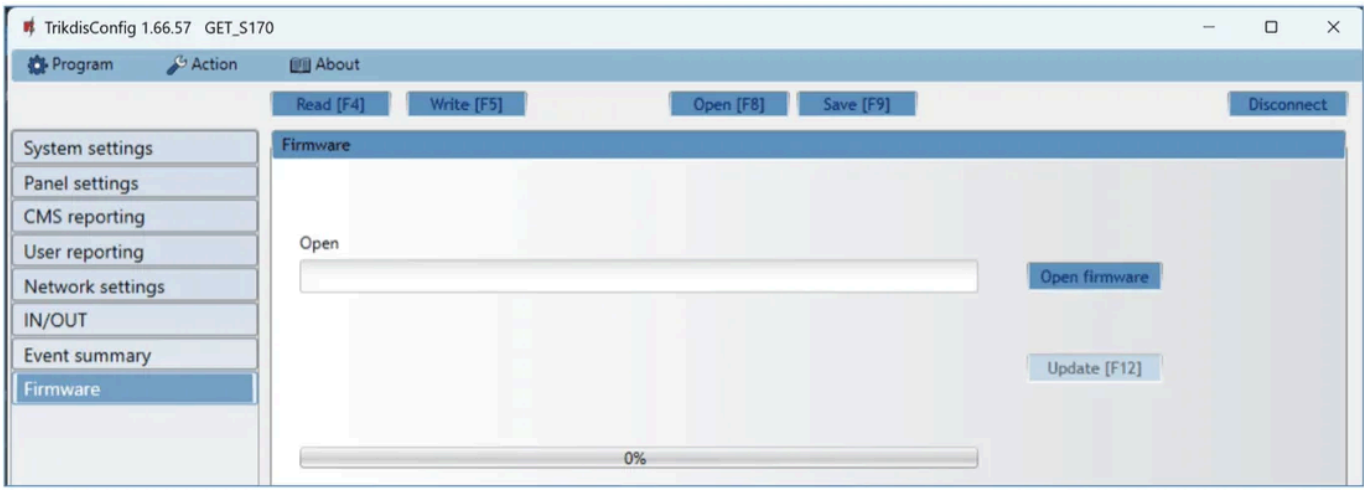


Figura 70. TrikdisConfig – página Firmware: el botón Open firmware, el botón Update [F12] y la barra de progreso.

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 cambiar la configuración del antivirus.

Algunas funciones del GET necesitan una versión de firmware determinada:

- **1.08** o posterior: configuración desde la aplicación Protegus 2 (Advanced settings, apartado 2.2 y capítulo 6);
- **1.17** o posterior, en la versión de hardware **M15**: los ajustes **Generation** y **Bands** en la página SIM de la aplicación (apartado 6.6.2);
- **1.21** o posterior: la conexión Keybus + TIP/RING de Paradox SP / SP+ / MG / MG+ (apartado 3.3.3);
- **1.31** o posterior, en la versión de hardware **x1x1**: en la aplicación, los identificadores (Account No., Device account No.) están entre los ajustes de la CRA (apartado 6.2).

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 LTE no se enciende: no hay red móvil

1. Mira los destellos del LED **TROUBLE**: 2 = fallo de la tarjeta SIM1, 3 = fallo de la tarjeta SIM2 (apartado 1.6).
2. Comprueba que la tarjeta SIM está activa, tiene servicio de datos y está bien colocada en la ranura (la SIM1 en el centro de la placa, la SIM2 en el borde izquierdo; apartado 3.1).
3. Si la petición de PIN está activada en la tarjeta, introduce el PIN en la pestaña **Network settings** → **SIM1** (o **SIM2**), o desactiva la petición de PIN en un teléfono.
4. Comprueba el APN (apartado 2.3): 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 LTE da como mínimo 3 destellos amarillos; apartados 1.6 y 3.2).
6. Si el comunicador transmite por la red cableada, la falta de red móvil por sí sola no lo detiene: envía por la siguiente vía disponible según el orden del **Reporting mode** (apartado 6.4.2); pero así falta la vía de respaldo, así que conviene arreglarlo.

El LED NETWORK LAN no se enciende: no hay red cableada

1. 1 destello del LED **TROUBLE** indica un fallo en la conexión física de la red cableada: comprueba el cable LAN en sus dos extremos y que el puerto del router o del switch está activo (apartado 1.6).
2. Si el cable está bien, mira la pestaña **Network settings** → **LAN**: con DHCP, el router debe dar una dirección; con dirección fija, Static IP, Subnet mask y Default gateway deben corresponder a la red local (apartado 6.6.1).
3. Si has indicado el receptor con un nombre de dominio, las direcciones DNS también deben funcionar en la red (DNS1, DNS2).

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. Comprueba la dirección y el puerto del receptor, el ajuste TCP/UDP, el protocolo y la clave de cifrado (**CMS reporting** → **CMS settings**, apartado 6.4.1); la clave debe ser la misma en el comunicador y en el receptor.
2. Mira el ajuste **Reporting mode** (apartado 6.4.2): **Main type** debe ser una vía que de verdad esté disponible en la instalación (hay cable LAN, o hay tarjeta SIM en la ranura indicada), y también debe haber una vía de respaldo.
3. Si el receptor está indicado con un nombre de dominio, comprueba la configuración DNS en la vía por la que transmite el comunicador (**Network settings** → **LAN** o **SIM1 / SIM2** → **DNS1, DNS2**).

4. En la red móvil, comprueba que el plan de datos de la tarjeta SIM no bloquea el puerto necesario (algunas tarjetas M2M solo permiten determinadas direcciones); en la red cableada, el cortafuegos local debe permitir la salida hacia el puerto del receptor.
5. Si la central no envía eventos (el LED DATA no se enciende), la causa está en la central: ver el punto siguiente.

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

1. En 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 elegido 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. En 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 **Communication protocol** debe ser **2. AUTO** (apartado 6.3).

¿Por qué vía va el evento: por LAN o por SIM?

Por la que indica el orden del **Reporting mode** (apartado 6.4.2): por la vía de **Main type**; si esta no funciona, por la de **Backup type** y luego por la de **Backup type 2**. Si el mensaje ha salido por la vía de respaldo, el comunicador vuelve a intentar la vía principal pasado el tiempo **Return from backup after**, y con el intervalo de **Communication path test** prueba todas las vías. La conexión de Protegus 2 también usa esta misma vía. En la red cableada no se consume tráfico de datos móviles.

¿Para qué sirven las dos ranuras SIM?

Con tarjetas de dos operadores distintos, la red móvil también tiene dos vías: en Reporting mode, la SIM1 y la SIM2 son tipos de conexión distintos, y cualquiera de ellas puede ser la vía principal o la de respaldo (apartado 6.4.2). Las dos tarjetas hay que configurarlas por separado (**Network settings** → **SIM1**, **SIM2**: PIN, APN; apartado 6.6.2); el fallo de la SIM2 lo indican 3 destellos del LED TROUBLE y el mensaje SIM2_FAILURE (apartados 1.6 y 6.8). El comunicador también funciona con una sola tarjeta.

DSC: todas las alarmas llegan como alarma general 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). La conexión simultánea del Keybus y de TIP/RING no existe en el GET (es una función del GT+). Si la CRA espera el código que corresponde al tipo de zona (por ejemplo, incendio: E110), conecta el GET solo a los bornes TIP/RING de la central y programa el marcador (apartados 3.3.9 y 4.2): así se envían los códigos Contact ID propios de la central, pero no hay control directo; 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 3.3.3), que no necesita desbloqueo, pero el firmware del comunicador debe ser como mínimo 1.21 (capítulo 9).

No puedo armar desde Protegus 2

1. En el control directo, **Panel settings** → **Remote Arm/Disarm** debe estar marcado, y la central debe estar configurada según el apartado 4.1 (Paradox: contraseña PC, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: los ajustes descritos). Comprueba en la tabla del apartado 1.3 si la central admite el control directo.
2. En el armado con zona de llave (apartado 3.4), el borne debe estar en **OUT** en la página **IN/OUT** (la configuración de fábrica del GET), 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 biestable; 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** (apartado 6.5).
2. Al añadirlo, hay que introducir el **PROTEGUS Cloud access Code** configurado en el equipo; si has cambiado el código en TrikdisConfig, cámbialo también en la aplicación.
3. Escribe el IMEI exactamente, tomándolo de la etiqueta del equipo o de la pegatina de la caja (o escanea el código QR).
4. Debe haber internet funcionando al menos por una vía: el LED NETWORK LTE está verde y parpadea en amarillo (tarjeta SIM con servicio de datos y APN correcto), o el LED NETWORK LAN está verde (cable LAN). Después de un evento, el LED DATA debe apagarse.

No puedo entrar a distancia con TrikdisConfig

1. El equipo debe estar en línea (NETWORK LTE verde y parpadeando en amarillo, o NETWORK LAN verde), y la conexión con Protegus debe estar habilitada (**Enable connection**).
2. **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.

¿Puedo configurar el comunicador desde la aplicación?

Sí: con firmware 1.08 o posterior, la mayoría de los ajustes están disponibles en el menú **Settings** → **Advanced settings** de Protegus 2 (apartado 2.2 y capítulo 6). Lo que solo está en TrikdisConfig: el restablecimiento de la configuración de fábrica (apartado 6.9), **Preferred operator** (apartado 6.6.2) y la actualización manual del firmware (capítulo 9); el interruptor **Event** de Serial bus la aplicación lo muestra, pero no lo cambia. Si entras con el código de instalador, solo puedes modificar los grupos que el administrador ha permitido (apartado 6.2).

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 6.9): con la alimentación conectada, mantenlo pulsado 10 segundos. Se borran todos los ajustes. Desde la aplicación no se puede iniciar el restablecimiento.

¿Cuánto tráfico de datos consume el equipo?

Los mensajes de evento y los PING son muy pequeños; el tráfico depende sobre todo del periodo de PING y de la frecuencia de los informes de test. En un sistema doméstico medio, el tráfico mensual suele quedar por debajo de 10 MB. El valor exacto depende de la configuración y de la unidad de facturación del operador, así

que con una tarjeta con límite de datos conviene comprobar el tráfico del primer mes. Mientras el comunicador transmite por la red cableada, no se consume el tráfico de datos de la tarjeta SIM.

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 / WEEE) que lleva el equipo indica que hay que entregarlo por separado, como residuo electrónico.

Ver también

- Buscador de compatibilidad: qué comunicador Trikdis y qué conexión van con tu central de alarma.
- Comunicador Trikdis + central de alarma DSC: guía rápida de instalación: los pasos de la conexión DSC, en breve.
- Comunicador Trikdis + central de alarma Paradox: guía rápida de instalación: los pasos de la conexión Paradox, en breve.
- 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 – GET: aquí está también la tabla de conversión de códigos Contact ID → SIA (anexo).

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

Productos relacionados

Trikdis GET Ethernet + 4G comunicador inteligente

Trikdis CRP2 cable de conexión puerto serie para paneles de alarma Paradox

Trikdis ANT04 antena GSM adhesiva con cable de 2,5m

Trikdis ME301M antena GSM magnética con cable de 2,5m

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-get