Comunicador G16 – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Trikdis G16: conexión al bus de datos o al puerto serie de la central de alarma, programación de la central, SIM y configuración en TrikdisConfig, transmisión a la CRA y la aplicación Protegus 2.



Edición: 2026-11-17
Versión web siempre actualizada: https://trikdis.es/manual-g16

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Centrales de alarma compatibles
1.3 Versiones
1.4 Características principales
1.5 Partes del comunicador
1.6 Bornes
1.7 Indicaciones de los LED
1.8 Datos técnicos

2. Puesta en marcha rápida con TrikdisConfig

2.1 Preparativos
2.2 Modelo de central y control directo
2.3 Conexión con la aplicación Protegus 2
2.4 Conexión con la CRA

3. Instalación y conexión

3.1 Pasos de la instalación
3.2 Ubicación y antena
3.3 Conexión a la central de alarma
3.3.1 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception e Integriti
3.4 Conexión de una zona de llave
3.5 Conexión de las entradas
3.6 Conexión de una salida con relé
3.7 Conexión del expansor iO-8
3.8 Conexión de los módulos W485 y E485
3.9 Encendido y primera comprobación
A TRIKDIS átjelző elindítása

4. Programación de la central de alarma

4.1 DSC
4.2 Paradox
4.3 Texecom
4.4 UTC Interlogix (Caddx)
4.5 Crow y Pyronix
4.6 Honeywell Ademco Vista
4.7 InnerRange Inception e Integriti

5. Control a distancia con Protegus 2

5.1 Cómo añadir el equipo
A rendszer létrehozása a Protegus 2 alkalmazásban

5.2 Control directo con el código de teclado
5.3 Armado con zona de llave
5.4 Armado y desarmado desde la aplicación
5.5 Control con mensajes SMS

6. TrikdisConfig – la configuración en detalle

6.1 La barra de estado
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 SIM card
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Restablecer la configuración de fábrica

7. Programación a distancia

8. Comprobación del comunicador

9. Actualización del firmware

10. Problemas y preguntas frecuentes

11. Instrucciones de seguridad

Ver también

1. Descripción general

El G16 es el **comunicador celular de conexión directa** de Trikdis: no se conecta a la salida de línea telefónica de la central de alarma, sino al **bus de teclados o al puerto serie** de la central. Lee los eventos directamente de la central –junto con el número de zona, partición y usuario– y los transmite por conexión de datos móviles al receptor de la CRA y a la nube de Protegus, a la aplicación del usuario. Funciona con las centrales DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell y Crow compatibles; en los modelos **de control directo**, el usuario arma y desarma desde la aplicación Protegus 2 con su propio código de teclado, sin necesidad de una zona de llave aparte. La aplicación Protegus 2 se puede usar con todas las centrales de alarma compatibles con el G16, sea cual sea el fabricante. Para una central de otra marca que solo tenga salida de línea telefónica, el comunicador adecuado es el G16T (TIP/RING).

1.1 Para qué sirve y cómo funciona

- **Lee la central directamente.** En el bus de la central, cada evento llega al comunicador al instante y con la numeración propia de la central; no hace falta configurar el marcador de la central y tampoco hay marcación Contact ID.
- **Transmite a la CRA.** Envía los eventos por conexión IP al receptor de software o de hardware de Trikdis (protocolo TRK) –que funcionan con cualquier software de CRA– o a cualquier receptor universal (SIA DC-09 2007/2012, SUR-GARD TL150). Al receptor SUR-GARD le entrega los códigos Contact ID recibidos de la central convertidos en códigos SIA. Comprueba la conexión por defecto cada 30 segundos (o con el intervalo que configures) y, si hay un fallo, pasa al canal de respaldo.
- **Avisa al usuario.** La aplicación Protegus 2 muestra lo ocurrido en notificaciones push –con un sonido propio según el evento– y en la lista de eventos; desde la aplicación el usuario puede armar y desarmar y accionar los dispositivos conectados (iluminación, puerta, ventilación, calefacción, riego, etc.). También se le puede avisar por SMS y por llamada telefónica.
- **Funciona con la CRA y con el usuario a la vez o por separado:** se puede usar solo con Protegus 2 (sin CRA), solo con la CRA o con ambos. Si están configurados los dos, el evento se envía primero a la CRA y después al usuario.
- **Respaldo por SMS.** También avisa a la CRA por SMS si la conexión de datos no funciona en la red del operador; puede enviar a dos receptores en paralelo, cada uno con su propio canal de respaldo.
- **Tiene entradas y salidas propias.** Tres bornes de E/S de doble función se pueden usar como entrada (detector, sabotaje) o como salida controlable (zona de llave, relé); las salidas se pueden accionar desde la aplicación Protegus 2 y con comandos SMS. En el bus RS485 de la versión 4G, con el expansor iO-8 se añaden 8 E/S más, y con el módulo W485 o E485 puede comunicarse también por WiFi o por internet por cable; en ese caso la red móvil es la vía de respaldo.

La estructura del sistema se ve en el esquema siguiente: el bus de la central de alarma se conecta al G16, el G16 llega a internet a través de la red móvil, y desde allí al receptor de la CRA y a la nube de Protegus; el usuario ve el sistema en la aplicación Protegus 2.

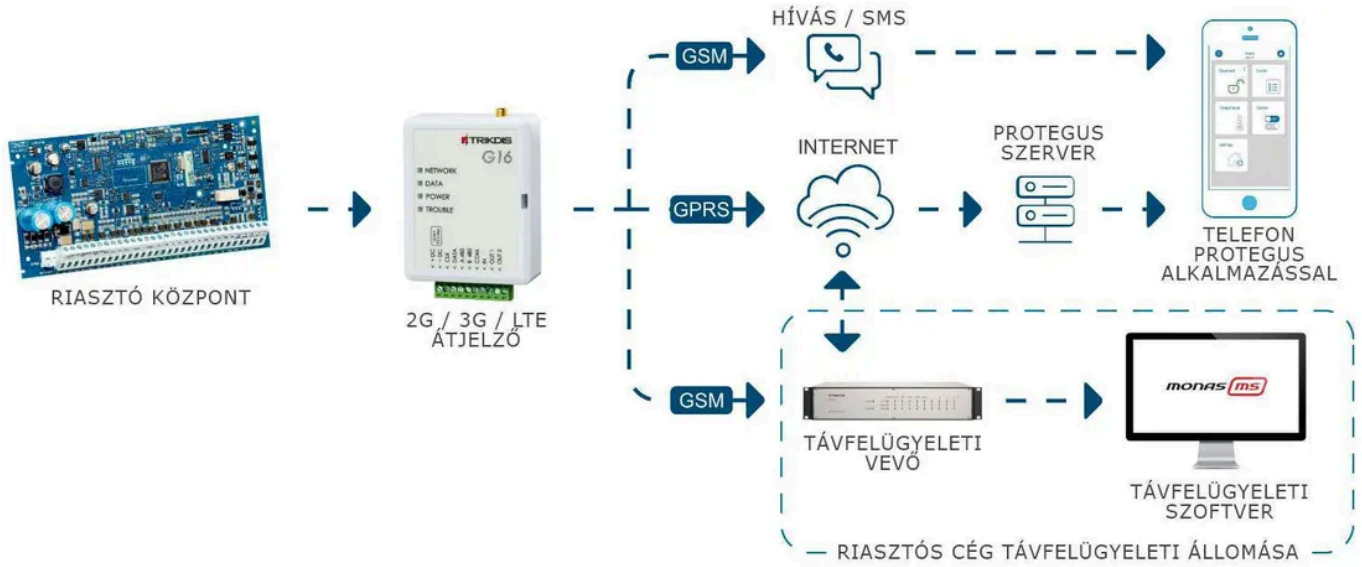


Figura 1. El lugar del G16 en el sistema: central de alarma → G16 → red móvil → receptor de la CRA y nube de Protegus → aplicación Protegus 2. El usuario también puede recibir SMS y llamadas (GSM), y el receptor de la CRA, SMS como respaldo.

- 1 Central de alarma (bus de teclados o puerto serie)
- 2 Comunicador G16 (2G / 4G)
- 3 Llamada y SMS al usuario
- 4 Datos móviles → internet → nube de Protegus
- 5 Teléfono con la aplicación Protegus 2
- 6 Receptor de la CRA
- 7 Software de CRA (la central receptora de la empresa de seguridad)

1.2 Centrales de alarma compatibles

El G16 se puede conectar a las centrales siguientes. En los modelos **de control directo**, el armado y el desarmado se hacen desde la aplicación con el código de teclado; en los demás, con una zona de llave (apartado 3.4). Para el control directo de las centrales Paradox, el firmware de la central debe ser como mínimo **V.4**; en los modelos Paradox más nuevos (SP+, MG5050+, EVOHD+) el puerto serie viene bloqueado de fábrica y hay que desbloquearlo antes de usarlo.

Centrales controlables directamente – el comunicador recibe los eventos por el bus de datos o por el puerto serie, y el armado / desarmado funciona sin cableado adicional:

Fabricante	Conexión	Modelos
Paradox	puerto serie	Spectra SP4000, SP5500, SP5500+*, SP6000, SP6000+*, SP7000, SP7000+*, SP65 Magellan MG5000, MG5050, MG5050+*, MG5075 DIGIPLEX EVO192*, EVOHD*, EVOHD+ (* firmware superior a 7.50)
DSC	bus de datos	PC585, PC1565, PC1616, PC1832, PC1864
Interlogix	bus de datos	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e
Texecom	puerto serie	Premier 24, 48, 88, 168, 640 Premier Elite 12, 24, 48, 64, 88, 168, 640
Honeywell	bus de datos	Ademco Vista-15, Vista-20, Vista-48

En las centrales Paradox más nuevas marcadas con *, el puerto serie viene bloqueado de fábrica; el dispositivo externo solo se comunica con ellas tras el desbloqueo.

Soros port feloldás útmutató

Centrales controlables con interruptor de llave – el comunicador recibe los eventos por el bus de datos o por el puerto serie; para el control hacen falta el cableado y la programación como interruptor de llave (apartado 3.4):

Fabricante	Conexión	Modelos
Paradox	puerto serie	Spectra 1727, 1728, 1738 Magellan MG5050E ESPRIT E55, 728ULT, 738ULT DIGIPLEX EVO48
DSC	bus de datos	PC1404, PC5020
Texecom	puerto serie	Premier 412, 816, 832, 832+
Inner Range	bus de datos	Inception, Integriti
Crow	bus de datos	Runner 4/8, 8/16

La lista cambia de vez en cuando; el estado más actual lo encuentras en el buscador de compatibilidad. Además de estas, también se puede usar con las centrales **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 y MATRIX 816**, **DSC PC5015** y **Paradox DIGIPLEX EVO96 y NE96**. Con las centrales **DSC PowerSeries NEO** el G16 no funciona: el fabricante no permite dispositivos externos en el bus de la NEO; ver DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones.

1.3 Versiones

Este manual está hecho para la **versión de hardware 4** del G16, pero **también sirve para la versión de hardware 3**: la conexión, la configuración y el funcionamiento de las dos versiones son en gran parte iguales. El manual vale por igual para las versiones con módem 2G, 3G y 4G. Las diferencias se resumen en la tabla siguiente; cuando el texto da un dato de la versión 4, en la versión 3 ten en cuenta esta tabla.

	Hardware 3 (v3)	Hardware 4 (v4)
Modelos (en TrikdisConfig)	p. ej. G16_3210 (2G); también hubo versiones con módem 3G y 4G	G16_G410 (2G), G16_54E0 (4G)
Entradas/salidas	1 entrada de tipo seleccionable (IN) + 2 salidas de colector abierto (OUT1, OUT2, máx. 0,15 A)	3 bornes de E/S de doble función (I/O 1, I/O 2, I/O 3); cada uno se puede usar como entrada o como salida de colector abierto (máx. 0,15 A)
Configuración de las entradas/salidas	Página System settings: **Input IN type**, **Output OUT1 & OUT2 mode**	Página **IN/OUT** (apartado 6.6)
Consumo	100 mA; durante el envío, hasta 250 mA	60–100 mA; durante el envío, hasta 500 mA
Bus RS485 (iO-8, W485, E485)	solo en las versiones 3G y 4G	solo en la versión 4G (G16_54E0)

La versión de hardware 4 se fabrica con dos módems:

Modelo	Módem	Frecuencias	RS485 (iO-8, W485, E485)
G16_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	no
G16_54E0	4G (LTE)	bandas LTE según la región	sí

La versión de hardware la encuentras en la barra de estado de TrikdisConfig (**HW**) y en la etiqueta de la parte trasera del equipo. La presentación de la versión 4 tiene un artículo aparte: Llega la versión de hardware v4 de los comunicadores GSM G16 y G16T.

1.4 Características principales

Conexión con la central de alarma

- Con un máximo de 4 cables (+DC, −DC, CLK, DATA) se conecta al bus de teclados de la central (DSC, Caddx, Crow, Pyronix, Honeywell) o a su puerto serie (Paradox, Texecom, InnerRange); para el puerto serie hay cable de fábrica (Paradox: CRP2 / CRP2B, Texecom: CRP4).
- Transmite todos los eventos de la central con la información completa del evento (código, partición, zona o usuario); avisa si se interrumpe la conexión (LED TROUBLE, evento COMMUNICATION).
- Las centrales de control directo se pueden armar y desarmar desde la aplicación con el código de teclado; Protegus 2 también muestra el estado de las zonas.

Comunicación con la CRA

- Conexión IP con los receptores Trikdis (receptor de software IPcom, RL14, RM14) y con receptores universales (SIA DC-09, TL150).
- Canal principal, de respaldo y paralelo; aviso de respaldo por SMS al receptor SMS de Trikdis (RL14, RM14, GM14).
- Cifrado de mensajes AES-128; memoria de 60 eventos.

Funciones para el usuario

- Aplicación móvil y web Protegus 2: notificaciones, lista de eventos, armado y desarmado, accionamiento de salidas.
- Control y configuración básica también con comandos SMS.
- Aviso también por SMS y por llamada telefónica, a un máximo de 4 números de teléfono.
- Permisos de usuario por niveles en la aplicación (administrador, instalador, usuario).

Instalación y configuración

- La configuración se puede guardar en un archivo y cargar en otro comunicador.
- Dos niveles de acceso: administrador e instalador.
- Se puede configurar y actualizar a distancia con el software TrikdisConfig.

1.5 Partes del comunicador

El G16 lleva la placa de circuito impreso en una caja de plástico blanca; la tapa frontal se puede quitar y la regleta de bornes es extraíble. En la imagen siguiente se ve la versión 4G; la versión 2G no tiene LED BAND ni bornes A 485 / B 485.

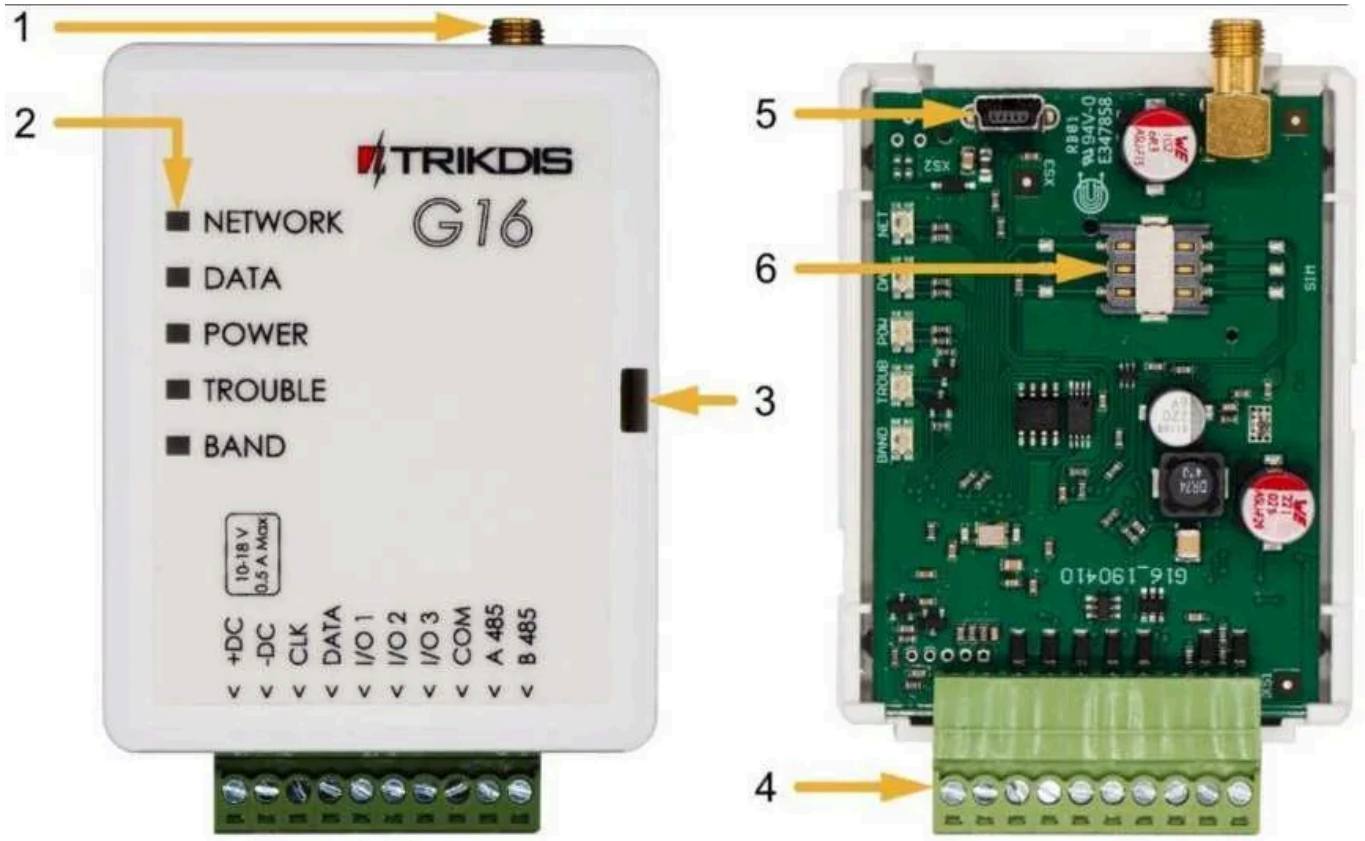


Figura 2. Partes del G16 (versión 4G), de frente y con la caja abierta.

- 1 Conector SMA de la antena GSM
- 2 Indicadores LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Ranura para quitar la tapa frontal
- 4 Regleta de bornes extraíble
- 5 Conector USB Mini-B para la programación
- 6 Ranura de la tarjeta nano-SIM

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 programarlo por USB, se puede llevar el equipo al ordenador.

1.6 Bornes

Borne	Función
+DC	Alimentación, +10–18 V DC
–DC	Alimentación, negativo
CLK	Línea de reloj / serie del bus de la central
DATA	Línea de datos del bus de la central
I/O 1	Entrada/salida 1 (por defecto: sin usar)
I/O 2	Entrada/salida 2 (por defecto: entrada, NO)
I/O 3	Entrada/salida 3 (por defecto: salida)
COM	Punto común (negativo) de las entradas y salidas
A 485	Cable A del bus RS485 (solo versión 4G)
B 485	Cable B del bus RS485 (solo versión 4G)

Los nombres de los bornes también figuran en la tapa frontal, así que no hace falta quitarla para hacer la conexión. A qué borne de la central van CLK y DATA depende del fabricante; los esquemas de conexión están en el apartado 3.3.

1.7 Indicaciones de los LED

Los LED de la tapa frontal son la herramienta más importante para la puesta en marcha y la resolución de problemas. Léelos en conjunto: POWER muestra la alimentación, NETWORK la red, TROUBLE los fallos y BAND (solo 4G) el tipo de red.

NETWORK – conexión de red

Indicación	Significado
apagado	Sin conexión con la red móvil
parpadea en amarillo	Conectándose a la red móvil
verde fijo	Conectado a la red móvil
verde fijo, parpadea en amarillo	Conectado; el número de destellos amarillos es el **nivel de señal**: en 2G, 5 destellos, y en 4G, 3 destellos indican buena señal

DATA – tráfico de datos

Indicación	Significado
apagado	No hay mensajes pendientes de envío
verde fijo	Hay mensajes pendientes de envío en la memoria
parpadea en verde	Se están enviando o recibiendo datos (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	Sin alimentación, o la alimentación está desconectada
verde fijo	Encendido, la tensión de alimentación es correcta
amarillo fijo	Tensión de alimentación insuficiente (11,5 V o menos)
verde fijo, parpadea en amarillo	Listo para programar (cable USB conectado)
amarillo fijo (durante la programación)	Sin conexión con el ordenador

TROUBLE – fallo

Indicación	Significado
apagado	Sin fallos
1 destello rojo	No hay tarjeta SIM
2 destellos rojos	Error de PIN de la SIM (código PIN incorrecto)
3 destellos rojos	Error de programación (falta el APN)
4 destellos rojos	No puede registrarse en la red móvil (error de registro)
5 destellos rojos	No puede conectarse a la red de datos (GPRS/UMTS/LTE)
6 destellos rojos	Sin conexión con el receptor de la CRA y/o con el servidor de Protegus (la causa también puede ser un fallo de la conexión a internet)
7 destellos rojos	Se ha interrumpido la conexión con la central de alarma (bus o conexión serie)
parpadea en rojo (durante la programación)	Error de memoria
rojo fijo (durante la programación)	Firmware dañado

BAND – tipo de red (solo versión 4G)

Destellos verdes	Red
1	ninguna
2	GSM
3	GPRS
4	EDGE
5	3G (HSDPA, HSUPA, HSPA+, WCDMA)
6	4G (LTE TDD, LTE FDD)

1.8 Datos técnicos

Parámetro	Valor
Conexión con la central de alarma	bus de teclados o puerto serie, según el modelo de central (máximo 4 cables: +DC, −DC, CLK, DATA; en el bus de Caddx y de Pyronix no se usa CLK)
Entradas/salidas	3 E/S de doble función (I/O 1, I/O 2, I/O 3): 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
Ampliación	en el bus RS485 (solo versión 4G): expansor iO-8 (+8 E/S) y otros expansores de la serie iO; módulo WiFi W485, módulo Ethernet E485
Módem 2G	850 / 900 / 1800 / 1900 MHz
Módem 4G	bandas LTE según la región
Tensión de alimentación	10–18 V DC
Consumo	60–100 mA nominal; hasta 500 mA durante el envío
Protocolos de transmisión	TRK, DC-09_2007, DC-09_2012, TL150

Parámetro	Valor
Memoria de eventos	60 mensajes
Cifrado	AES-128
Programación	TrikdisConfig (Windows) por cable USB Mini-B o a distancia; comandos SMS
Condiciones de funcionamiento	−10 … +50 °C, humedad relativa máx. 80 % (a +20 °C)
Dimensiones	92 × 65 × 26 mm
Peso	80 g

2. Puesta en marcha rápida con TrikdisConfig

Toda la configuración del G16 se hace con el programa **TrikdisConfig**, que funciona en Windows, por cable USB o a distancia. En este capítulo describimos el camino más corto: configuras el equipo en la mesa, antes de conectarlo, y después en la instalación solo queda conectarlo. La explicación detallada de los ajustes está en el capítulo 6.

2.1 Preparativos

Qué vas a necesitar

Cable USB Mini-B · cable de al menos 4 hilos para el bus de la central – para el puerto serie de Paradox, cable **CRP2** o **CRP2B**; para el puerto serie de Texecom, cable **CRP4** · destornillador plano de 2,5 mm · antena móvil de ganancia adecuada (en lugares con poca cobertura, una antena de mayor ganancia) · tarjeta nano-SIM activa con servicio de datos móviles (la petición de PIN se puede desactivar) · el manual de instalación de la central de alarma. Los accesorios necesarios se piden por separado al distribuidor.

1. Descarga e instala el software TrikdisConfig. En la web de Trikdis (www.trikdis.com), escribe en el 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 tapa frontal del G16. Introduce un destornillador plano en la ranura del borde superior de la tapa y, haciendo palanca hacia abajo, suelta la tapa frontal con cuidado. El esquema siguiente muestra la apertura y la posición del conector USB.

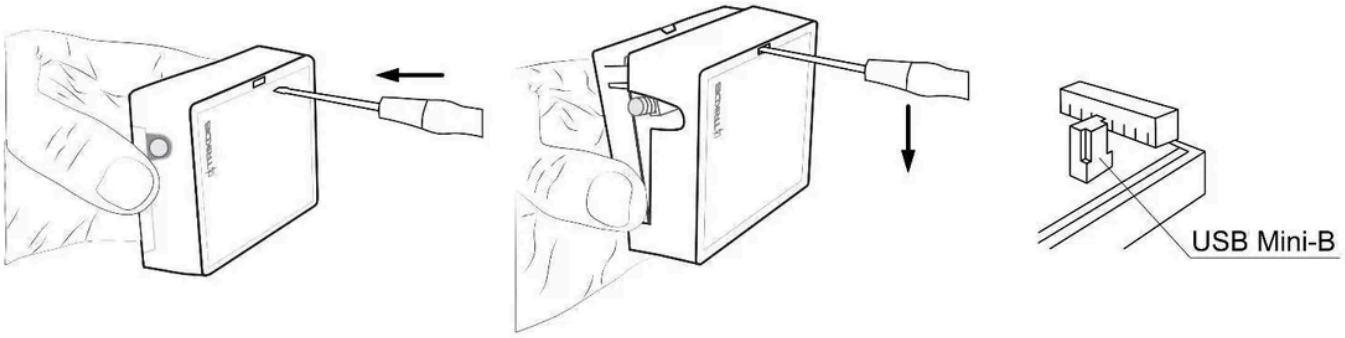


Figura 3. Cómo soltar la tapa frontal con un destornillador plano (izquierda, centro) y posición del conector USB Mini-B en la placa de circuito impreso (derecha).

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

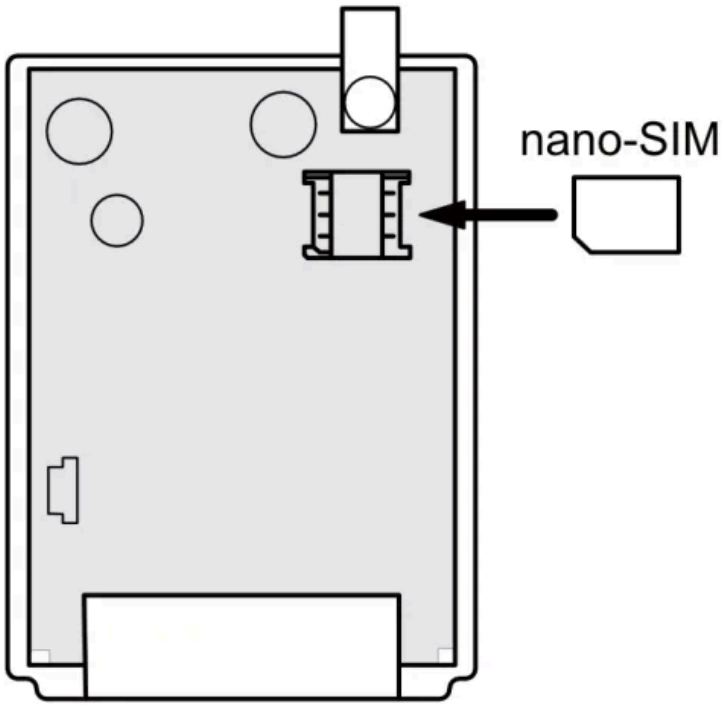


Figura 4. Posición de la tarjeta nano-SIM en la placa de circuito impreso.

4. Conecta el G16 al ordenador con un cable USB Mini-B. El USB da suficiente alimentación para la programación; no hace falta alimentación aparte.

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. Inicia 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 te pide contraseña, introduce el código de 6 dígitos de administrador (por defecto `123456`) o de instalador (por defecto `654321`).

2.2 Modelo de central y control directo

Uses el modo que uses, primero indica en la página **System settings** a qué central va conectado el comunicador.

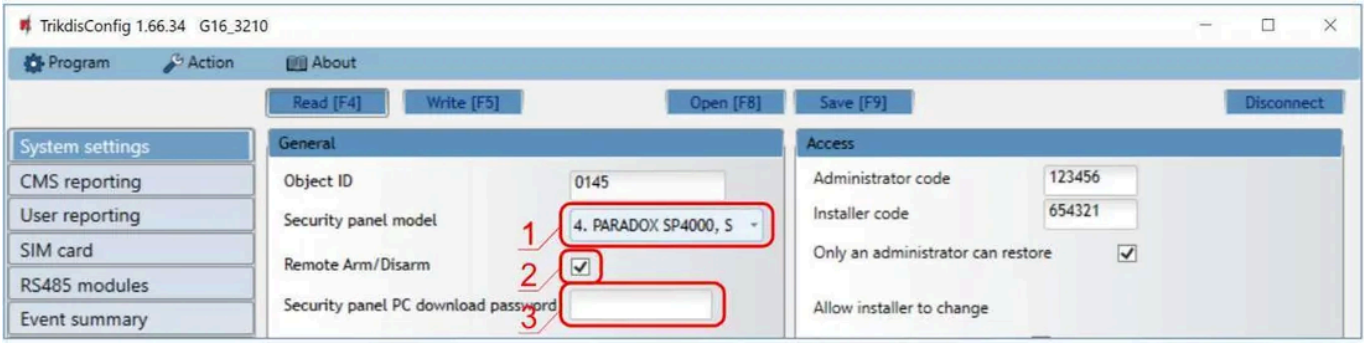


Figura 5. TrikdisConfig – página System settings, grupo General.

- 1 **Security panel model** – el modelo de la central de alarma conectada, elegido de la lista; de él depende cómo lee el comunicador el bus.
- 2 **Remote Arm/Disarm** – márcalo si el usuario quiere armar y desarmar la central desde la aplicación Protegus 2 con su propio código de teclado. Solo aparece en los modelos de control directo; en las demás centrales el armado se resuelve con una zona de llave (apartado 3.4); en ese caso déjalo sin marcar.
- 3 **Security panel PC download password** – en las centrales Paradox y Texecom, la contraseña de PC o de UDL de la central (4 caracteres); debe coincidir con la configurada en la central. El campo aparece después de marcar Remote Arm/Disarm.

En varias centrales también hay que configurar algo en la propia central: en las centrales Caddx, Honeywell e InnerRange ya para leer los eventos (habilitar el bus o el puerto serie), y en las centrales Paradox y Texecom para el control directo (contraseña de PC o de UDL). El capítulo 4 lo describe por fabricante, incluido el cambio de contraseña.

2.3 Conexión con la aplicación Protegus 2

Si el usuario quiere ver y controlar el sistema desde la aplicación Protegus 2, configura lo siguiente en la página **User reporting**, pestaña **PROTEGUS Cloud**.



Figura 6. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- 4 **Enable connection** – márcalo: habilita la conexión con la nube de Protegus.
- 5 **Protegus Cloud access code** – cambia la contraseña de fábrica `123456`. Es la que habrá que introducir en la aplicación al crear el sistema; **una vez creado el sistema ya no se puede cambiar.**

Después, en la página **SIM card**, introduce los datos de la tarjeta.

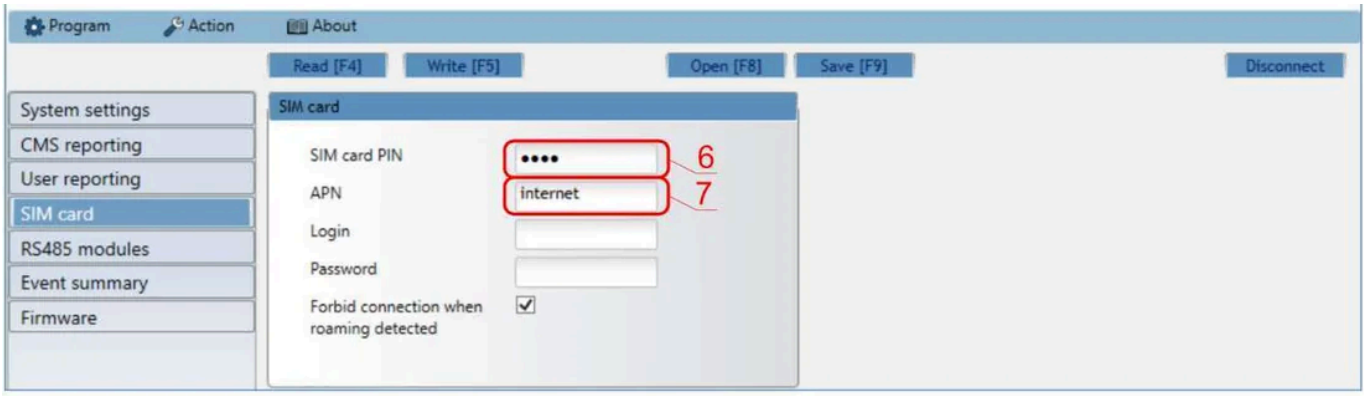


Figura 7. TrikdisConfig – página SIM card.

- 6 **SIM card PIN** – el código PIN de la tarjeta (si la petición de PIN está desactivada, puede quedarse el valor de fábrica).
- 7 **APN** – el punto de acceso de datos del operador (ver más abajo).

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

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.

2.4 Conexión con la CRA

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

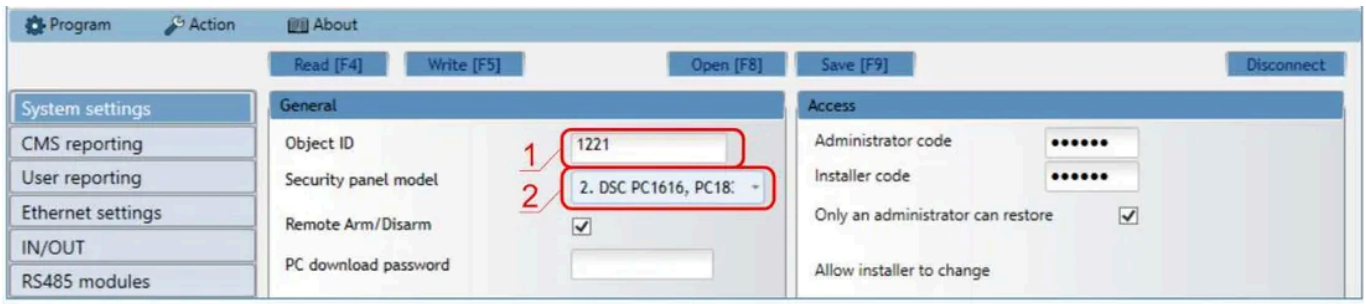


Figura 8. TrikdisConfig – página System settings, grupo General.

- 1 **Object ID** – el identificador de abonado que te da la CRA (4 caracteres hexadecimales, 0–9, A–F). No se pueden usar `FFFE` ni `FFFF`.
- 2 **Security panel model** – el modelo de la central de alarma conectada (si aún no lo has configurado en el apartado 2.2).

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

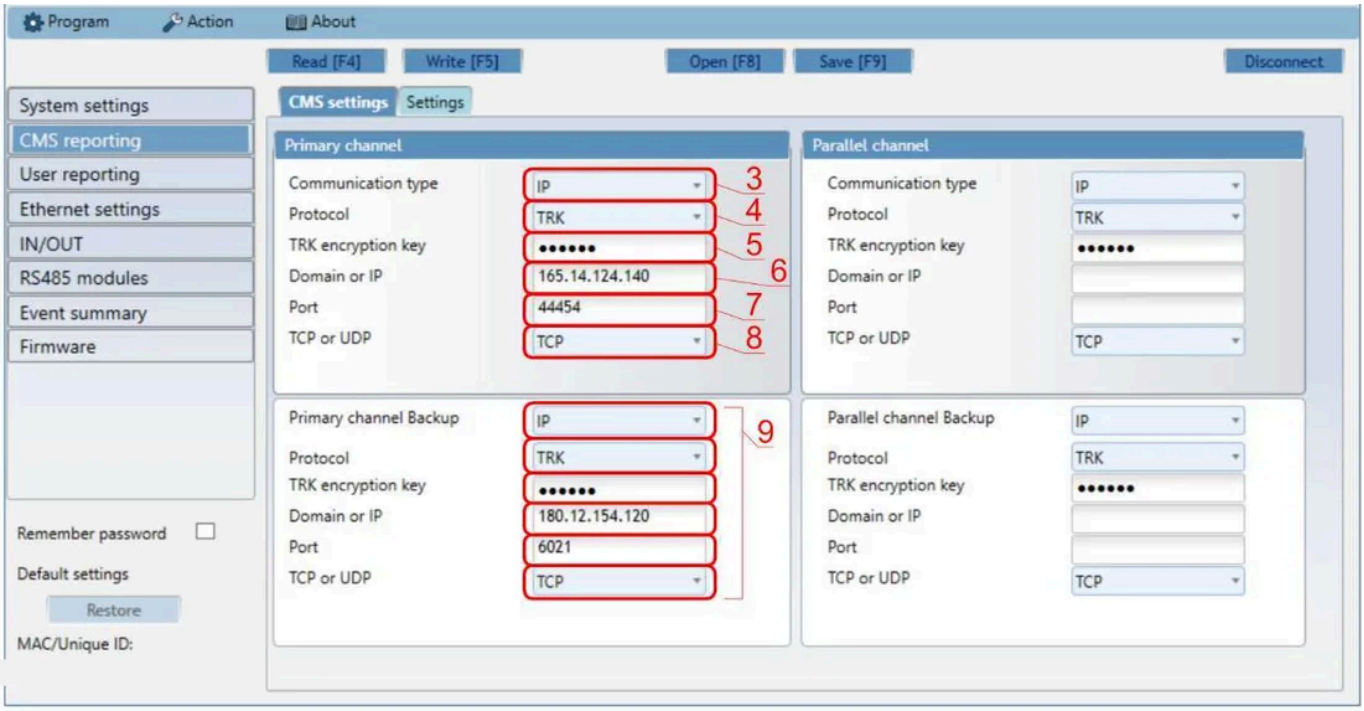


Figura 9. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 3 **Communication type** – elige la conexión **IP** (no se recomienda SMS como canal principal).
- 4 **Protocol** – **TRK** para receptor Trikdis, **DC-09_2007** o **DC-09_2012** para receptor universal, **TL150** para receptor SURGARD.
- 5 **TRK encryption key** – la clave de cifrado de 6 dígitos configurada en el receptor.
- 6 **Domain or IP** – el nombre de dominio o la dirección IP del receptor.
- 7 **Port** – el número de puerto del receptor.
- 8 **TCP or UDP** – el protocolo de transmisión; se ajusta a la configuración del receptor.
- 9 **Primary channel Backup** – canal de respaldo para cuando falle el principal; rellénalo igual, se recomienda configurarlo.

También se recomienda configurar el **Parallel channel** (canal paralelo) y su canal de respaldo si los eventos los tienen que recibir dos receptores; y en el campo **Backup SMS reporting number** –también recomendado– puedes escribir el número de teléfono del receptor SMS de Trikdis: el equipo envía aquí un SMS justo después del primer arranque, y después transmite por SMS cuando no funciona ninguno de los canales IP.

Por último, en la página **SIM card**, introduce los datos de la tarjeta si no lo has hecho ya en el apartado 2.3.

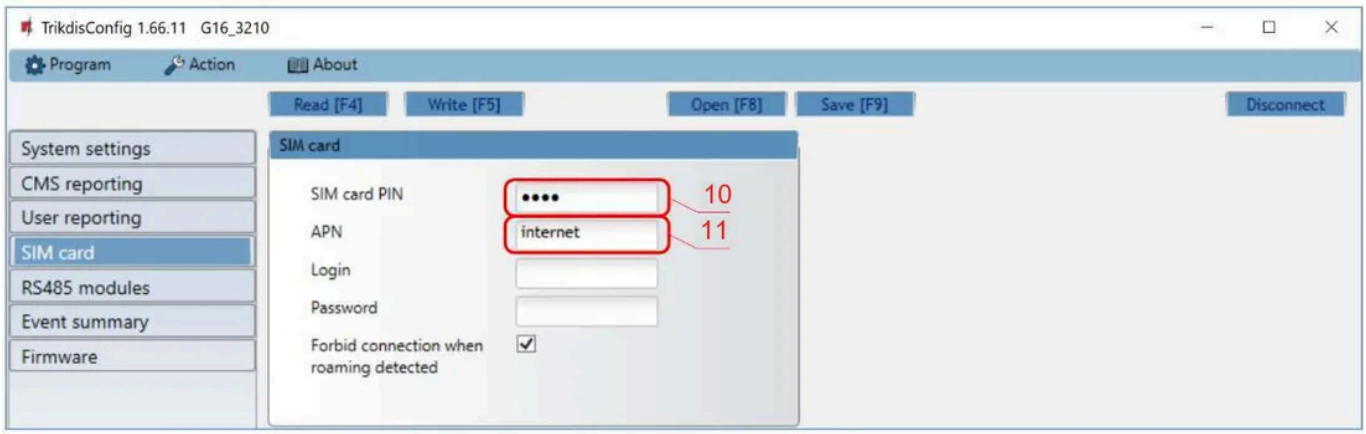


Figura 10. TrikdisConfig – página SIM card.

- 10 **SIM card PIN** – el código PIN de la tarjeta.
- 11 **APN** – el punto de acceso del operador (ver el apartado 2.3).

La **transmisión por SMS** a la CRA solo funciona con receptor Trikdis (receptor IP/SMS RL14, receptor multicanal RM14 o receptor SMS GM14); en ese caso solo hacen falta la clave de cifrado y el número de teléfono. Con el protocolo **DC-09**, indica también en la pestaña **Settings** el número de abonado, de línea y de receptor DC-09.

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 conectarlo.

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 si no lo hiciste durante la puesta en marcha.
3. Saca la placa de circuito impreso de la base: abre el pestillo de la esquina (ver la imagen).
4. Fija la base con tornillos en el lugar elegido.
5. Vuelve a colocar la placa de circuito impreso en la base y enchufa de nuevo la regleta de bornes.
6. Enrosca la antena GSM.
7. Vuelve a colocar la tapa frontal.

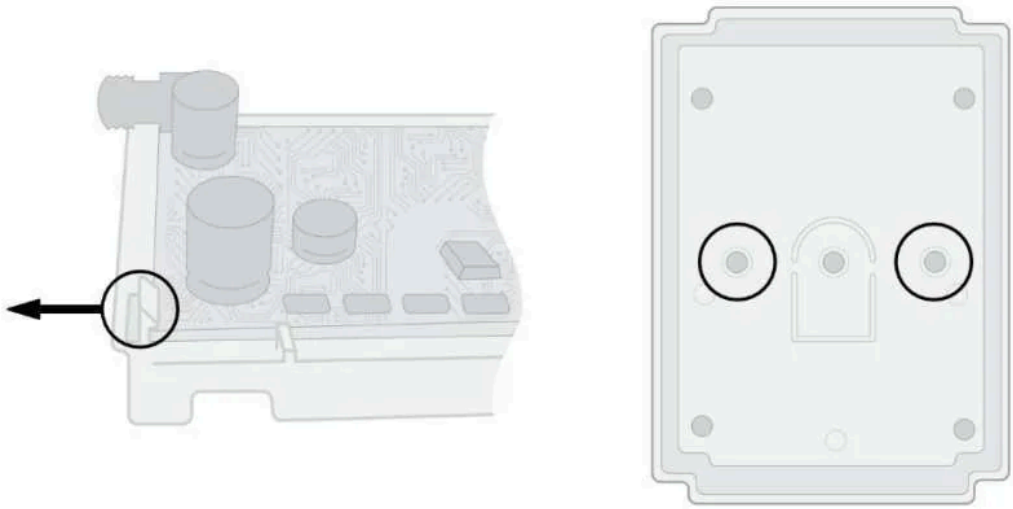


Figura 11. Cómo sacar la placa de circuito impreso: apertura del pestillo de la esquina (izquierda) y orificios de fijación de la base (derecha, marcados con un círculo).

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

3.2 Ubicación y antena

- Coloca el comunicador en un lugar **seco y en interior**, a ser posible cerca de la caja de la central de alarma, para que el cable del bus sea corto.
- **Dentro de una caja metálica** la señal móvil se debilita mucho. Si el comunicador va dentro de la caja metálica de la central, saca la antena fuera de la caja o usa una antena con cable más largo.
- Antes de la fijación definitiva, **comprueba el nivel de señal**: el número de destellos amarillos del LED NETWORK debe ser al menos 5 en 2G y al menos 3 en 4G (ver el apartado 1.7). Si son menos, busca un lugar mejor o cambia a una antena más sensible que se pueda colocar más lejos.
- Mantén la antena y el comunicador alejados del transformador de la central y de los cables de red eléctrica.



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

3.3 Conexión a la central de alarma

El G16 se conecta a la central con **un máximo de cuatro cables** (en el bus de Caddx y de Pyronix no se usa CLK): a los bornes **+DC** y **–DC** va la alimentación auxiliar de 12 V (AUX) de la central, y a los bornes **CLK** y **DATA**, los dos cables de datos del bus de teclados o del puerto serie de la central. Qué borne de la central es cada uno depende del fabricante; conecta según los esquemas siguientes. Para las centrales con puerto serie (Paradox, Texecom) hay cable de fábrica: un extremo encaja en el conector de la central y el otro se conecta a la regleta de bornes del G16.

El G16 puede consumir hasta 500 mA durante el envío. Comprueba que la salida AUX de la central lo soporte junto con los demás equipos conectados. Como la alimentación la da la central, durante un corte de corriente la batería de la central también alimenta al comunicador. La mayoría de las centrales no se dañan si se intercambian los cables de un equipo conectado al bus, pero intercambiar **+DC y –DC** puede estropear el comunicador; comprueba la polaridad antes de conectar.

Después de la conexión, en el campo **System settings** → **Security panel model** de TrikdisConfig hay que elegir el modelo de la central conectada (apartado 2.2); en algunos fabricantes también hay que configurar la central (capítulo 4).

3.3.1 DSC PowerSeries

Los cuatro bornes del Keybus: **RED** → +DC, **BLK** → –DC, **YEL** → CLK, **GRN** → DATA.

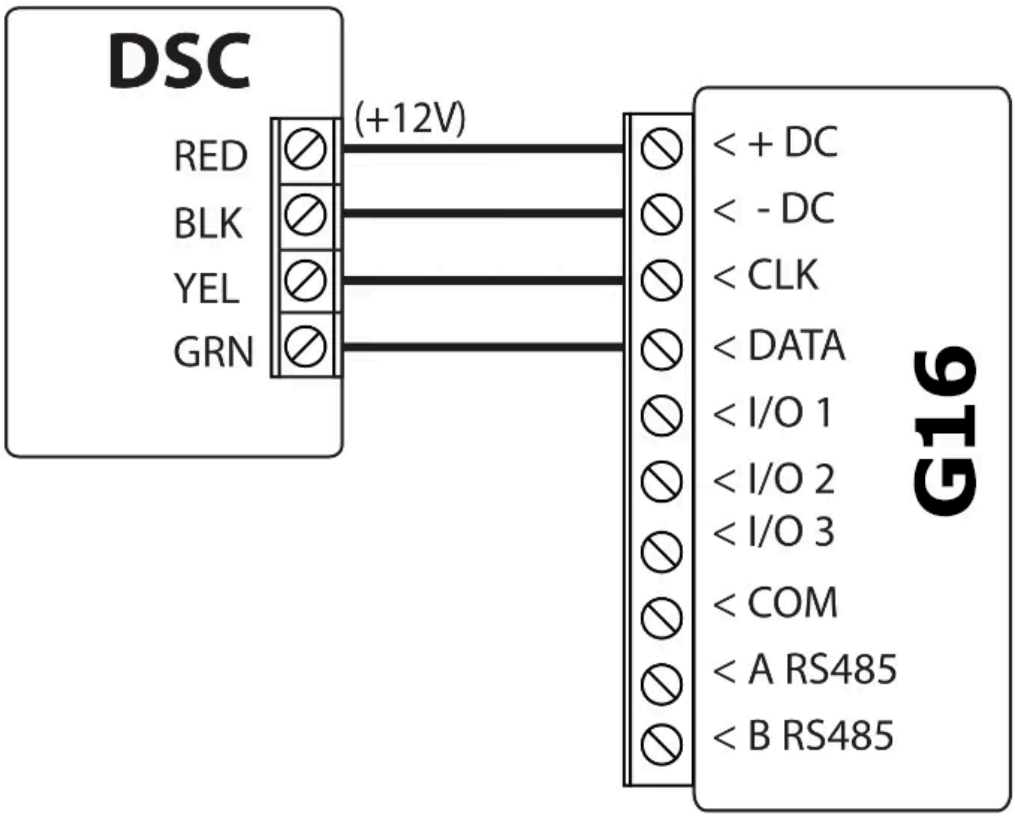


Figura 12. Conexión al Keybus de una central DSC PowerSeries (bus de teclados, «Keypad bus»): RED → +DC (+12 V), BLK → –DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

El comunicador se conecta al **puerto serie** (SERIAL) de las centrales Paradox con el cable de fábrica **CRP2** o **CRP2B**; el extremo del cable del lado de la central encaja en el conector serie, y el otro extremo lo conectas a la regleta de bornes del G16. Los 4 pines del conector: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Los colores de los hilos de los dos cables son distintos; el esquema muestra la asignación de colores de ambos cables. Marcado del conector serie de Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

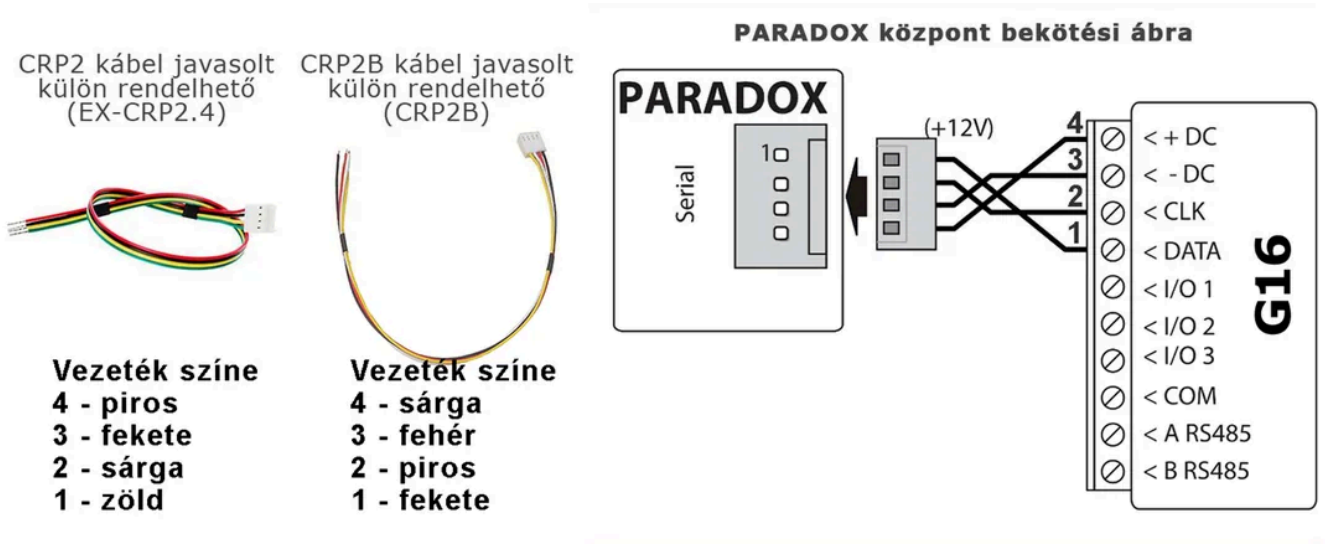


Figura 13. Conexión al puerto serie de una central Paradox con el cable CRP2 (EX-CRP2.4) o CRP2B. CRP2: 4 rojo → +DC, 3 negro → −DC, 2 amarillo → CLK, 1 verde → DATA. CRP2B: 4 amarillo → +DC, 3 blanco → −DC, 2 rojo → CLK, 1 negro → DATA.

En las centrales Paradox más nuevas, el puerto serie puede venir bloqueado de fábrica; cómo desbloquearlo se explica en el apartado 4.2 y en el artículo Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox.

3.3.3 UTC Interlogix (Caddx) NetworX

Los tres bornes del bus de teclados: **POS** → +DC, **COM** → −DC, **DATA** → DATA. El borne **CLK** no se usa.

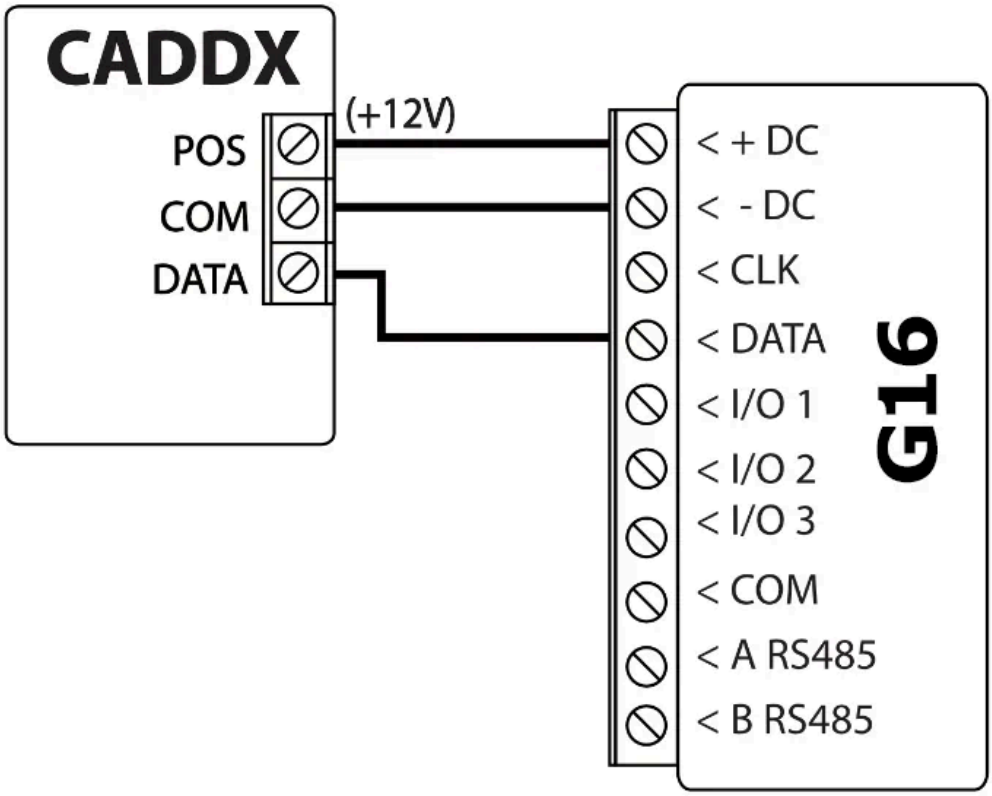


Figura 14. Conexión al bus de teclados de una central Caddx NetworX («Keypad bus»): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK queda libre.

3.3.4 Texecom Premier / Premier Elite

El comunicador se conecta al puerto serie de la central con el cable de fábrica **CRP4**: **rojo (R)** → +DC, **negro (B)** → −DC, **azul (BL)** → CLK, **blanco (W)** → DATA.

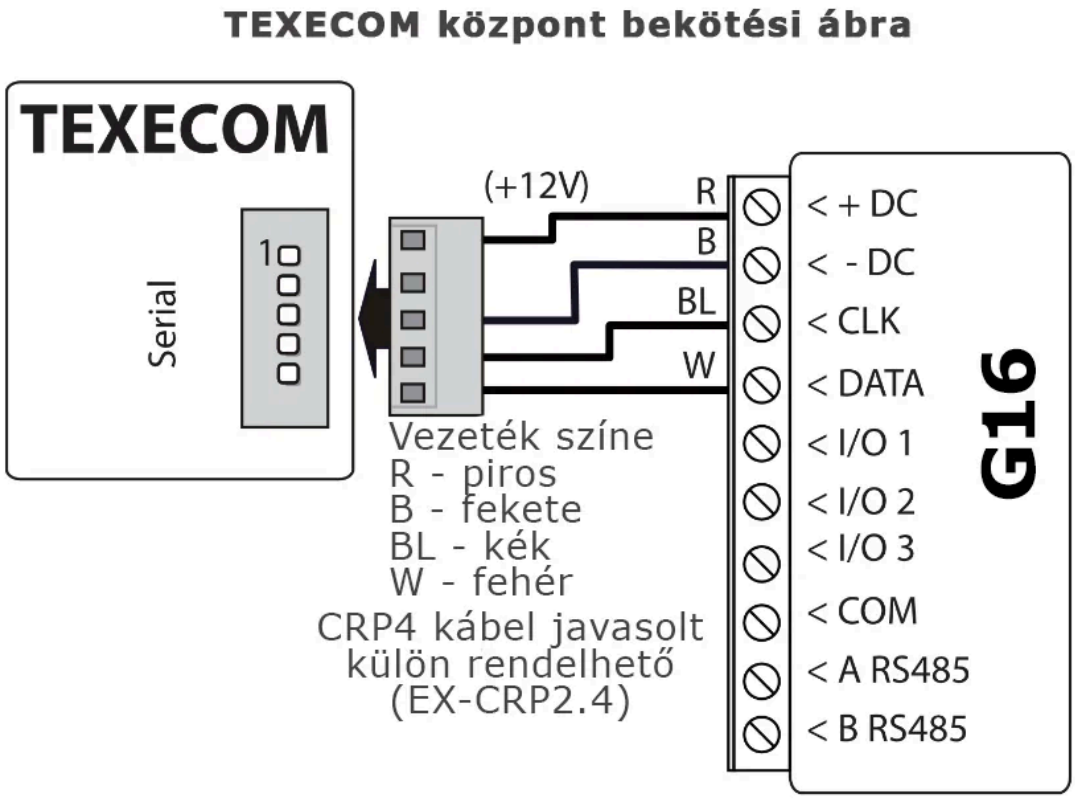


Figura 15. Conexión al puerto serie de una central Texecom con el cable CRP4: rojo → +DC, negro → −DC, azul → CLK, blanco → DATA.

3.3.5 Crow Runner

Bus de teclados de las Crow Runner 4/8 y Runner 8/16: **POS** → +DC, **NEG** → −DC, **CLK** → CLK, **DATA** → DATA.

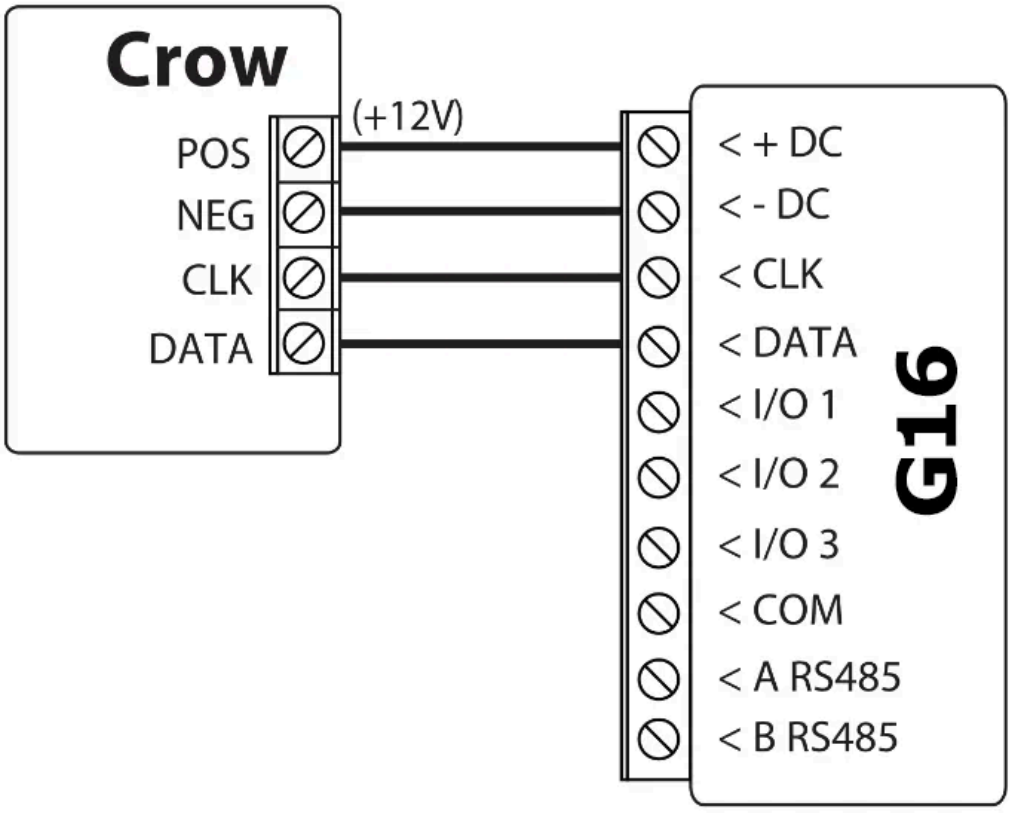


Figura 16. Conexión al bus de teclados de una central Crow Runner 4/8 y Runner 8/16 («Keypad bus»): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Bus de teclados de las centrales Pyronix: **+AUX** → +DC, **–AUX** → –DC, **KD** → DATA. El borne **CLK** no se usa. Después de la conexión y de configurar el comunicador, deja la central sin alimentación y reiníciala para que acepte el comunicador (apartado 4.5).

3.3.7 Honeywell Ademco Vista

Bornes numerados del bus de teclados de las centrales Vista-15, Vista-20 y Vista-48: **5** (AUX +) → +DC, **4** (AUX –) → –DC, **7** (salida de datos, amarillo) → CLK, **6** (entrada de datos, verde) → DATA.

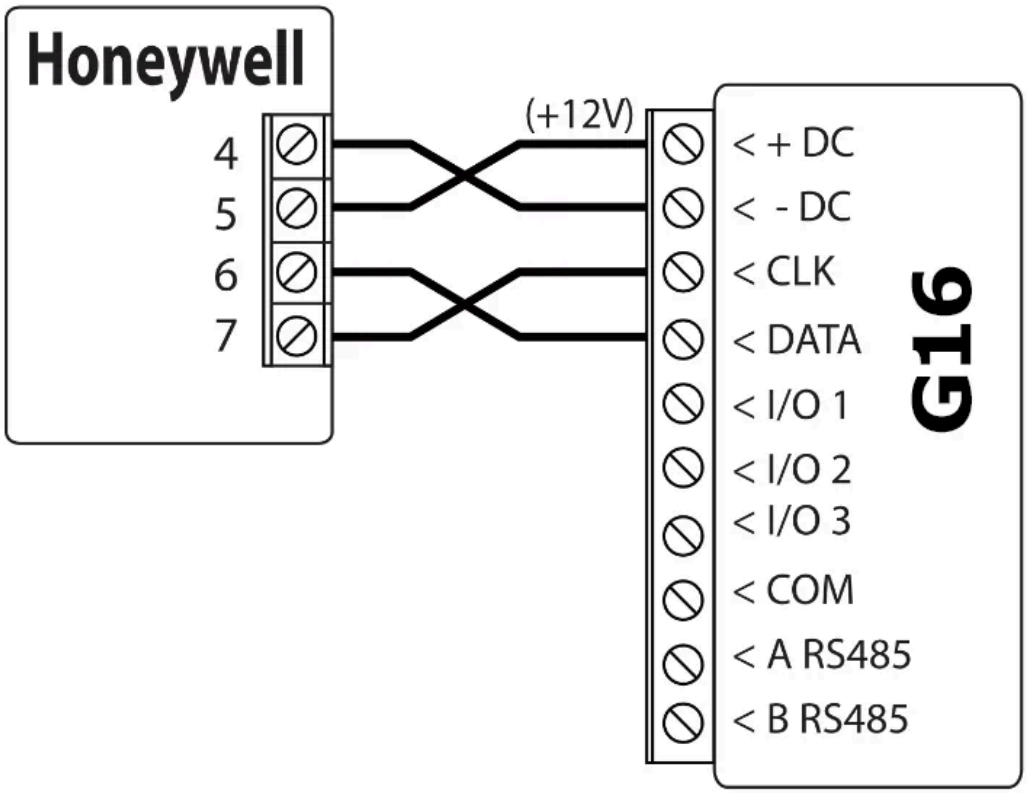


Figura 17. Conexión al bus de teclados de una central Honeywell Vista-20 / Vista-48 («Keypad bus»): 5 → +DC (+12 V), 4 → –DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception e Integriti

El comunicador toma la alimentación de los bornes de alimentación de la central **Inception** (**VOUT +** → +DC, **0V** → –DC), y la conexión de datos se hace desde el puerto USB de la central con el cable 993030USB de InnerRange: **negro** → 0V (–DC), **verde** → CLK, **blanco** → DATA. En la central hay que habilitar el uso del puerto serie (apartado 4.7).

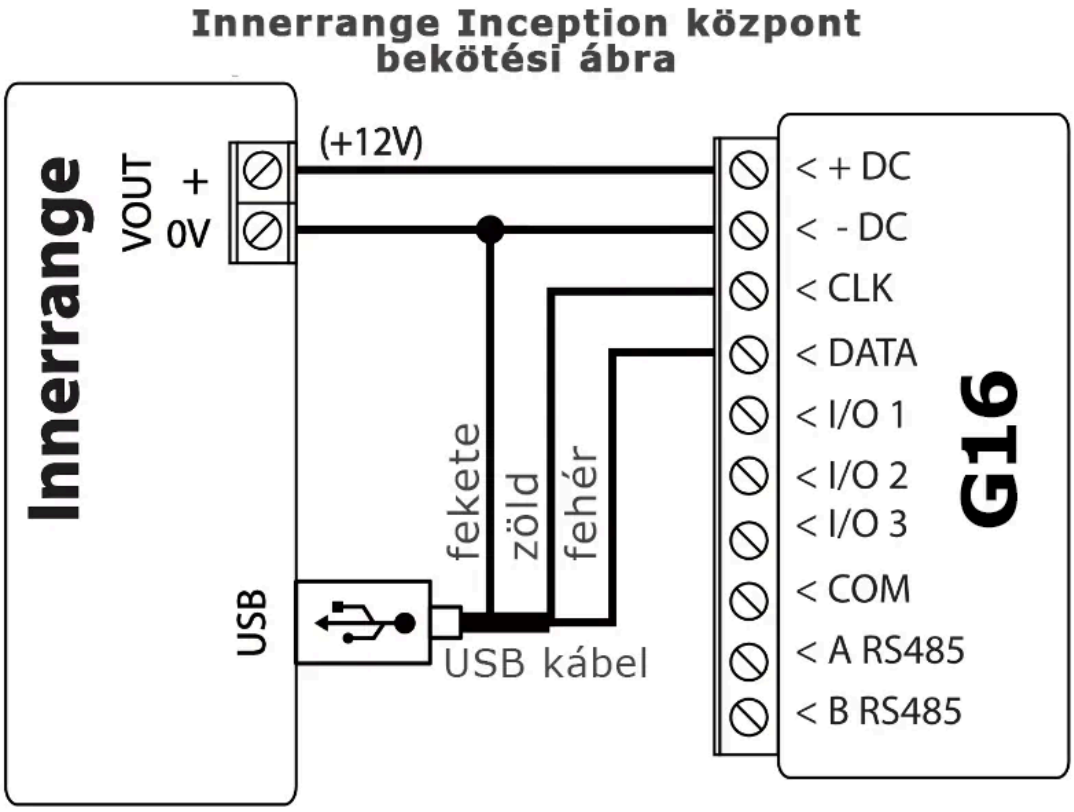


Figura 18. Conexión a una central InnerRange Inception: alimentación desde los bornes VOUT + y 0V, datos desde el puerto USB con el cable 993030USB (negro → 0V, verde → CLK, blanco → DATA).

A la central **Integriti** se conecta en el puerto 0 (Port 0) con el cable INTG-996795: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA.

3.4 Conexión de una zona de llave

Si la central no es de los modelos de control directo, o no quieres usar el control directo, el armado y desarmado a distancia se puede resolver con una **zona de llave**: configuras uno de los bornes de E/S del comunicador como **salida** (página IN/OUT, apartado 6.6) y lo conectas a una zona de llave de la central. Al activarse, la salida lleva la zona a COM (negativo); conecta la resistencia de fin de línea de la zona según el tipo de zona de la central. Como el G16 tiene tres bornes de E/S, se pueden controlar hasta tres particiones, cada una con su propia salida.

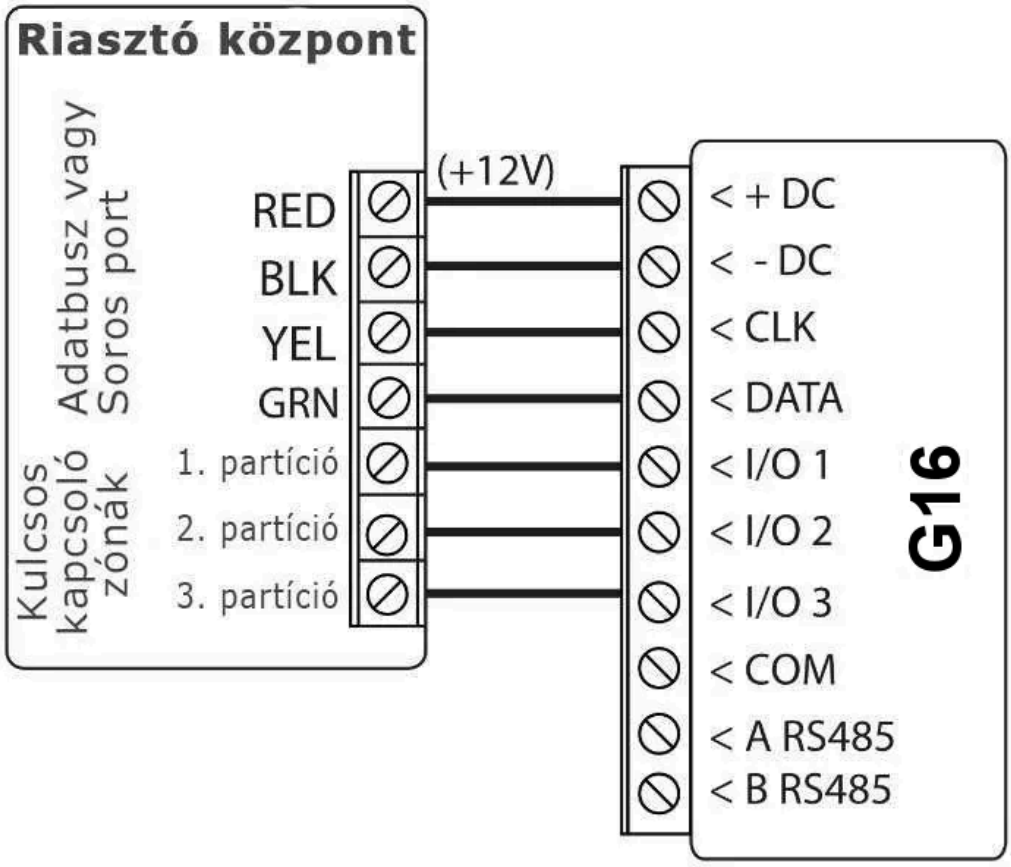


Figura 19. Armado y desarmado con zona de llave: el comunicador lee los eventos del bus de la central, y las salidas I/O 1–3 accionan la zona de llave de las particiones 1–3 de la central.

- En la página **System settings** de TrikdisConfig, deja **Remote Arm/Disarm sin marcar**: no se pueden usar los dos a la vez.
- La zona de llave puede ser de impulso o biestable; en la aplicación Protegus 2 hay que configurar el mismo modo (apartado 5.3).
- En la **versión de hardware 3**, las dos salidas (OUT1, OUT2) pueden controlar dos particiones; el campo **System settings → Output OUT1 & OUT2 mode** debe estar en **Remote control** (valor de fábrica).

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 las entradas

Los bornes de E/S del comunicador, como entradas, también sirven para recibir otros detectores (p. ej. un interruptor de sabotaje, un pulsador de pánico, un termostato), independientemente de la central de alarma. La entrada se conecta entre la E/S elegida y el borne COM.

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	–

Tipo	Estado de reposo	Alarma	Sabotaje
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: tipos NO, NC, NC/EOL, NO/EOL, NO/DEOL y NC/DEOL con resistencia de fin de línea de 2,2 kΩ; en los tipos DEOL también está conectado el circuito de sabotaje.

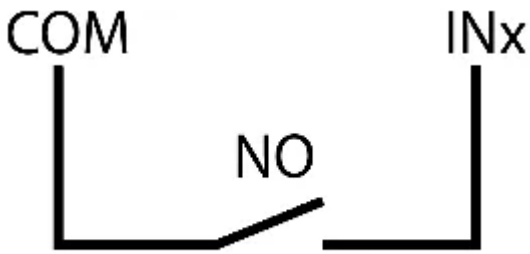


Figura 20. NO – circuito normalmente abierto: cerrado – alarma, abierto – reposo.

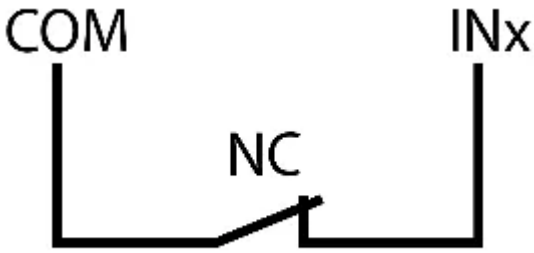


Figura 21. NC – circuito normalmente cerrado: abierto – alarma, cerrado – reposo.

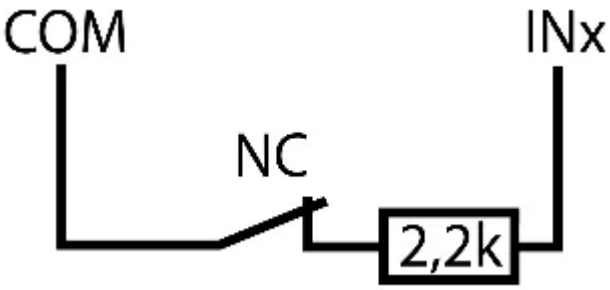


Figura 22. NC/EOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

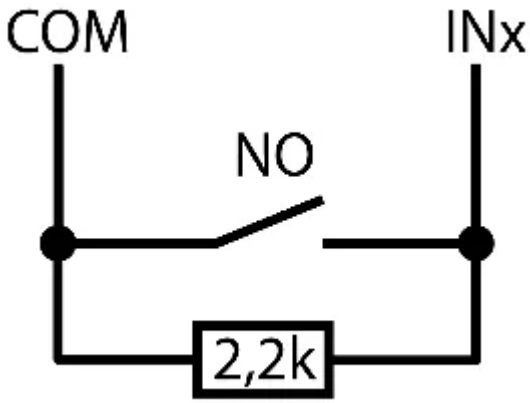


Figura 23. NO/EOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

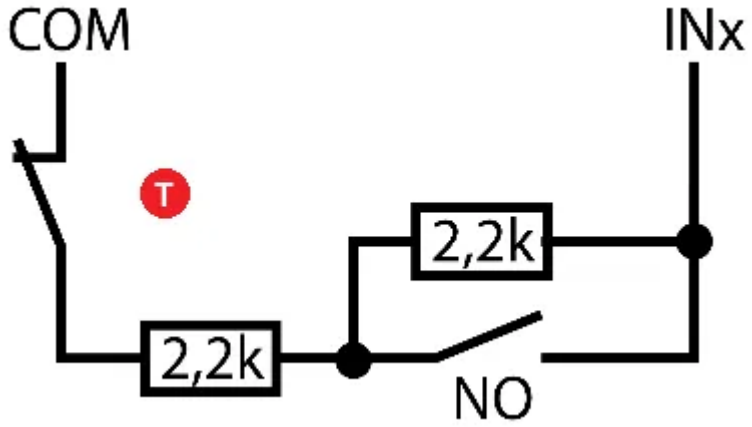


Figura 24. NO/DEOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o corte – sabotaje, 2,2 kΩ – alarma, 3,3–5,5 kΩ – reposo.

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

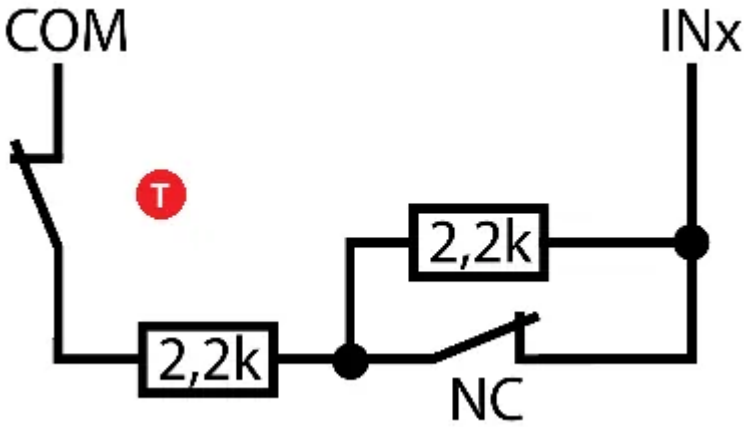


Figura 25. NC/DEOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o corte – sabotaje, 2,2 kΩ – reposo, 3,3–5,5 kΩ – alarma.

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

En la **versión de hardware 3** hay una sola entrada (IN); su tipo se configura en el campo **System settings → Input IN type**.

3.6 Conexión de una salida con relé

Como salidas, los bornes de E/S son salidas de colector abierto (OC): en estado activo llevan la carga conectada al negativo, con un máximo de 0,15 A y hasta 30 V DC. Un consumo mayor o un equipo de tensión de red acciónalo **a través de un relé**: un extremo de la bobina del relé va a +DC y el otro al borne de E/S. Con los contactos del relé se pueden encender y apagar distintos equipos eléctricos. Para ello, el borne de E/S se configura como salida (**OUT**) en la página **IN/OUT** de TrikdisConfig (apartado 6.6).

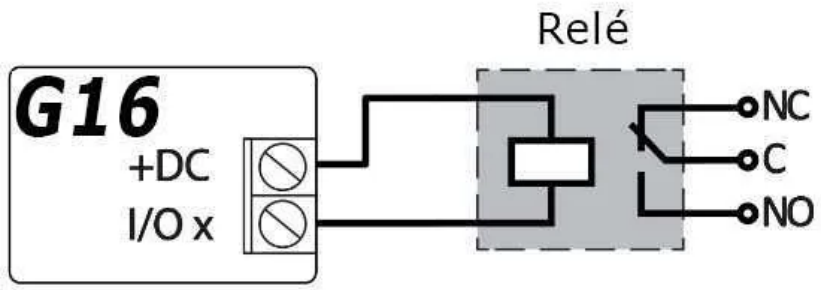


Figura 26. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne I/O x, y los contactos (NC, C, NO) accionan la carga.

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

3.7 Conexión del expansor iO-8

Si hacen falta más entradas o salidas, al bus RS485 de la **versión 4G** se pueden conectar hasta cuatro expansores **iO-8**; cada uno añade 8 E/S de doble función. Une los bornes A 485 y B 485 con los bornes A y B del módulo, y toma la alimentación del módulo de la salida AUX de 12 V de la central. La forma de conectarlo también la describe el manual propio del iO-8. El módulo se añade en la página **RS485 modules** de TrikdisConfig (apartado 6.7); los eventos de las entradas van a la CRA y a Protegus 2, y las salidas se pueden accionar desde la aplicación.

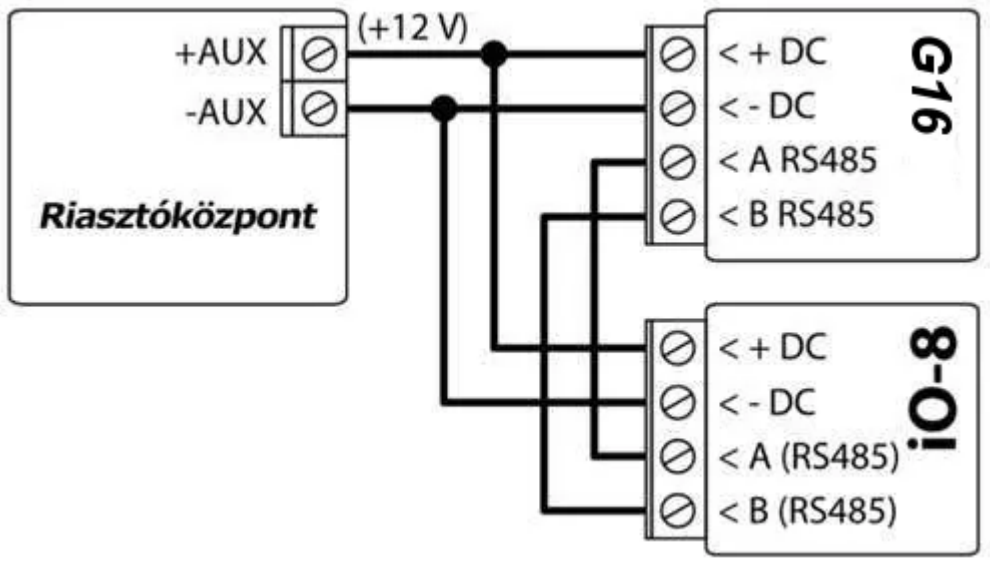


Figura 27. Conexión del expansor iO-8 al bus RS485 del G16 (A 485 → A, B 485 → B); los dos equipos se alimentan de la salida AUX de la central de alarma (+12 V).

El G16 con módem 2G (G16_G410) no tiene bus RS485, por lo que no se le pueden conectar los módulos iO-8, W485 ni E485.

3.8 Conexión de los módulos W485 y E485

Ampliación Ethernet o Wi-Fi – W485 y E485. El comunicador se puede complementar con el módulo Wi-Fi W485 o el módulo Ethernet E485: los eventos llegan a la CRA y a la aplicación Protegus 2 por Internet cableado o por Wi-Fi.

- **Conexión:** por el bus RS485, con alimentación común con el comunicador (entrada de alimentación del módulo 9–28 V DC); no hace falta una fuente de alimentación aparte.
- **Internet es el canal principal:** mientras funciona, todo va por él. Si se interrumpe, el comunicador pasa por sí solo a la red móvil y, en cuanto vuelve Internet, regresa a IP.
- **No solo transmisión de alarmas:** la aplicación Protegus 2 (notificaciones, control remoto) también funciona por este canal.
- **E485** – Ethernet cableado (RJ45). **W485** – Wi-Fi 2,4 GHz (WPA / WPA2), donde no hay cable UTP tendido.
- Si se necesita, también se puede usar sin tarjeta SIM. Configuración: con el software TrikdisConfig, por USB.

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

Mientras la conexión WiFi o Ethernet está activa, el G16 se comunica a través de ella y no usa la conexión de datos móviles; si la conexión se interrumpe, pasa a los datos móviles y, cuando la conexión se restablece, vuelve al módulo. Para que el módulo funcione, **el G16 tiene que tener una tarjeta SIM**.

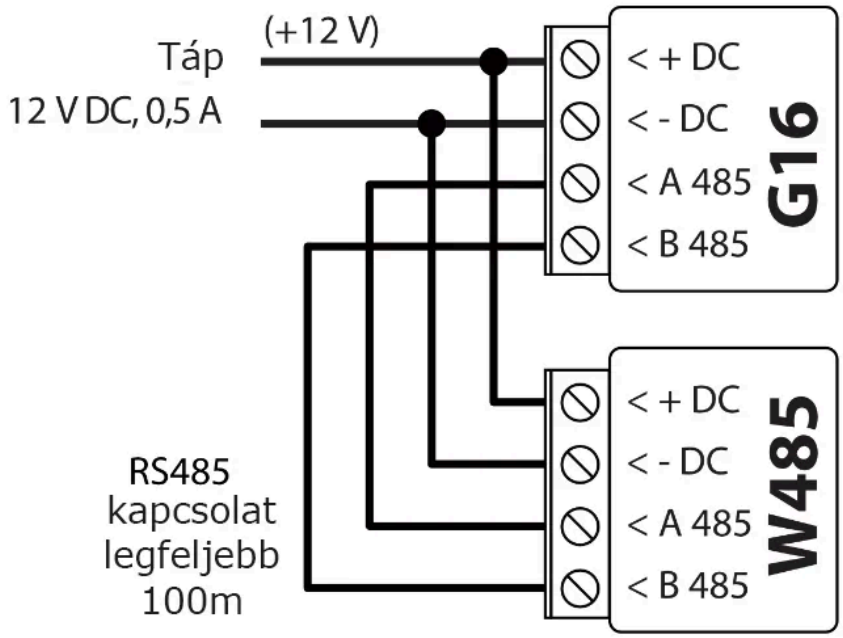


Figura 28. Conexión del módulo WiFi W485 al G16 por el bus RS485. Los dos equipos se alimentan de una fuente común de 12 V DC (de al menos 0,5 A) (entrada de alimentación del módulo: 9–28 V DC); el cable RS485 puede tener como máximo 100 m.

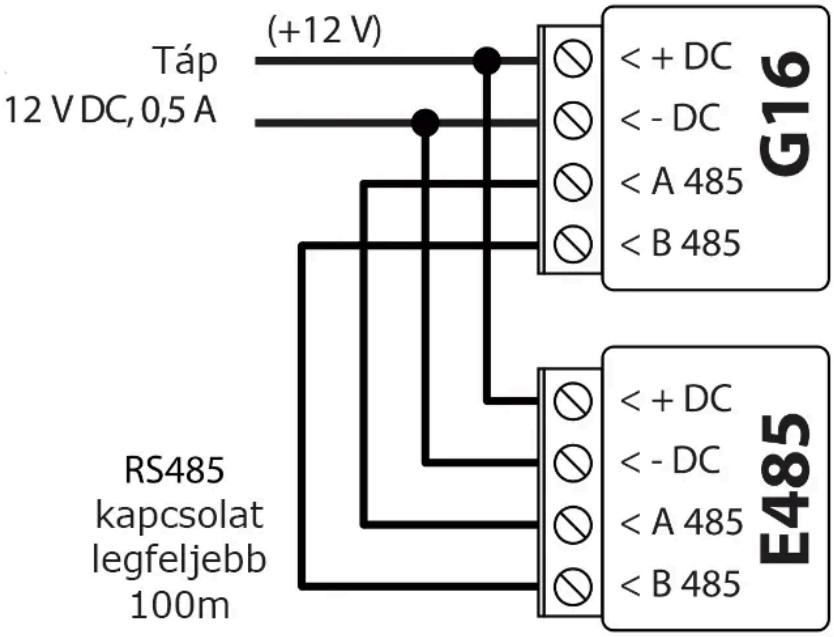


Figura 29. Conexión del módulo Ethernet E485 al G16 por el bus RS485. Los dos equipos se alimentan de una fuente común de 12 V DC (de al menos 0,5 A) (entrada de alimentación del módulo: 9–28 V DC); el cable RS485 puede tener como máximo 100 m.

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

La configuración de red de los módulos se hace en la página **RS485 modules** de TrikdisConfig (apartado 6.7).

3.9 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 central de alarma también arranca el comunicador. En la tapa frontal debes ver esto:

- **POWER** verde fijo: la alimentación es correcta;
- **NETWORK** verde fijo y parpadeando en amarillo: se ha conectado a la red; el número de destellos es el nivel de señal (en 2G, 5, y en 4G, 3 es bueno);
- **TROUBLE** apagado.

Si el LED NETWORK da menos destellos amarillos, el nivel de señal no es suficiente: busca otro lugar para el comunicador o usa una antena más sensible (apartado 3.2). Cualquier otra indicación de los LED señala algún fallo; identifícalo con las tablas del apartado 1.7. Si TROUBLE parpadea, el número de destellos indica la causa (apartado 1.7). **7 destellos** indican que falta la conexión con la central: comprueba los cables CLK y DATA, el modelo de central elegido y, donde haga falta, la programación de la central (capítulo 4). Si no se enciende ningún LED, comprueba la alimentación y el cableado.

4. Programación de la central de alarma

Este capítulo describe, por fabricante, qué hay que configurar en la central de alarma para que el G16 lea los eventos y, donde es posible, controle la central a distancia. En la mayoría de las centrales no hay que programar nada para leer los eventos; para el **control directo**, marca la opción **Remote Arm/Disarm** en la página **System settings** de TrikdisConfig y, en las centrales Paradox y Texecom, introduce también la contraseña de PC o de UDL de la central en el campo **Security panel PC download password** (apartados 2.2 y 6.2).

Si no controlas la central directamente, sino a través de una zona de llave (apartado 3.4), deja **Remote Arm/Disarm** sin marcar; en ese caso este capítulo solo se refiere a la configuración necesaria para leer los eventos.

4.1 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.

4.2 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.

4.3 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]**.

4.4 UTC Interlogix (Caddx)

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

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

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

Posición (location)	Segmento	Ajuste
105	3	12345678
108	3	12345678

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

4.5 Crow y Pyronix

Las centrales **Crow Runner 4/8** y **Runner 8/16** no requieren ningún ajuste especial.

Las centrales **Pyronix** tampoco requieren programación, pero después de configurar y conectar el comunicador, **deja la central sin alimentación** (red y batería) y vuelve a arrancarla: la central acepta el comunicador conectado a su bus al arrancar.

4.6 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]**.

4.7 InnerRange Inception e Integriti

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.

Las centrales Inception e Integriti transmiten los eventos al comunicador; para armar y desarmar hace falta una zona de llave (apartados 1.2 y 3.4).

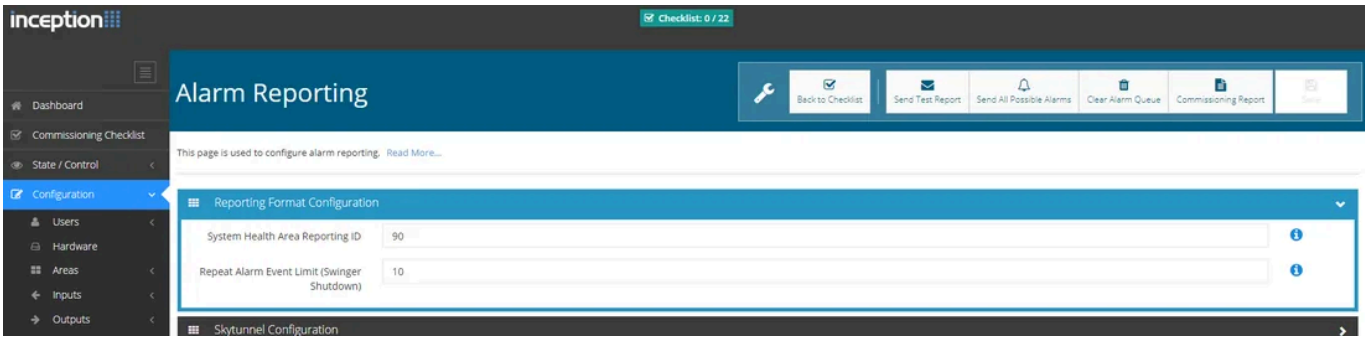


Figura 30. Interfaz web de Inception – Configuration → General → Alarm Reporting.



Figura 31. Inception – 3rd Party Device Configuration.

- 1 **Enable 3rd Party Device Reporting** – marcado.
- 2 **3rd Party Device Type** – Trikdis.
- 3 **Serial Port** – Serial Port 1 (Plugged In, In Use By 3rd Party Device).

5. Control a distancia con Protegus 2

Con la aplicación móvil y web Protegus 2, el usuario ve a distancia el estado del sistema, recibe avisos de los eventos, puede armar y desarmar y accionar las salidas del comunicador. Con el G16, el armado se puede hacer de dos maneras: en las centrales **de control directo**, el usuario lo hace con su propio **código de teclado**; en las centrales conectadas con zona de llave, mediante una **salida** del comunicador.

5.1 Cómo añadir el equipo

Antes de añadir el equipo, comprueba lo siguiente:

1. La tarjeta SIM está activa y tiene la conexión de datos móviles operativa; su código PIN está escrito en el equipo o la petición de PIN está desactivada.
2. En la pestaña **User reporting** → **PROTEGUS Cloud** de TrikdisConfig está marcado **Enable connection** y está configurado el **Protegus Cloud access code** (una vez creado el sistema ya no se puede cambiar).
3. El LED **POWER** está verde fijo y el LED **NETWORK** está verde fijo y parpadea en amarillo.

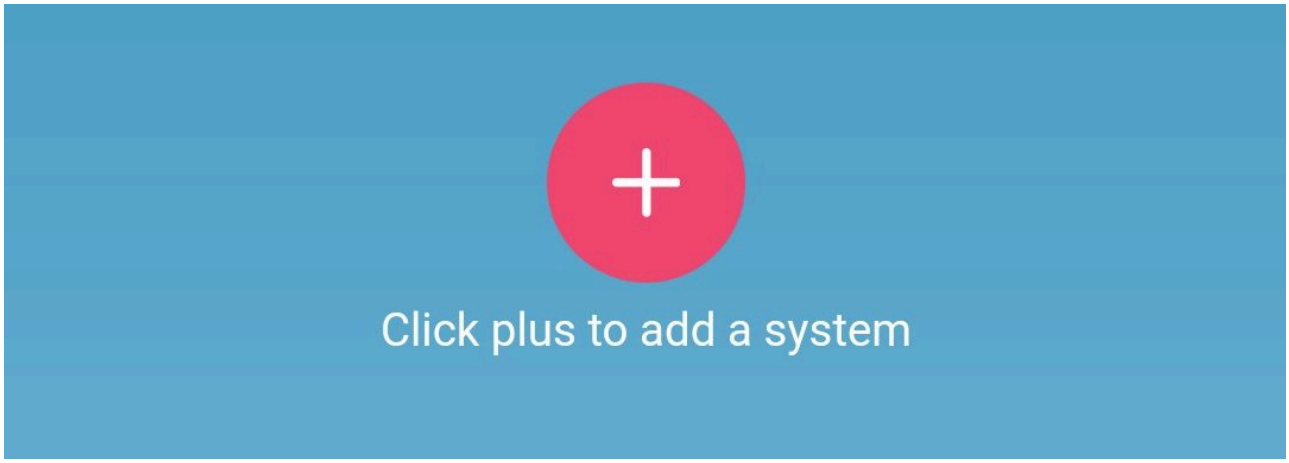
El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del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



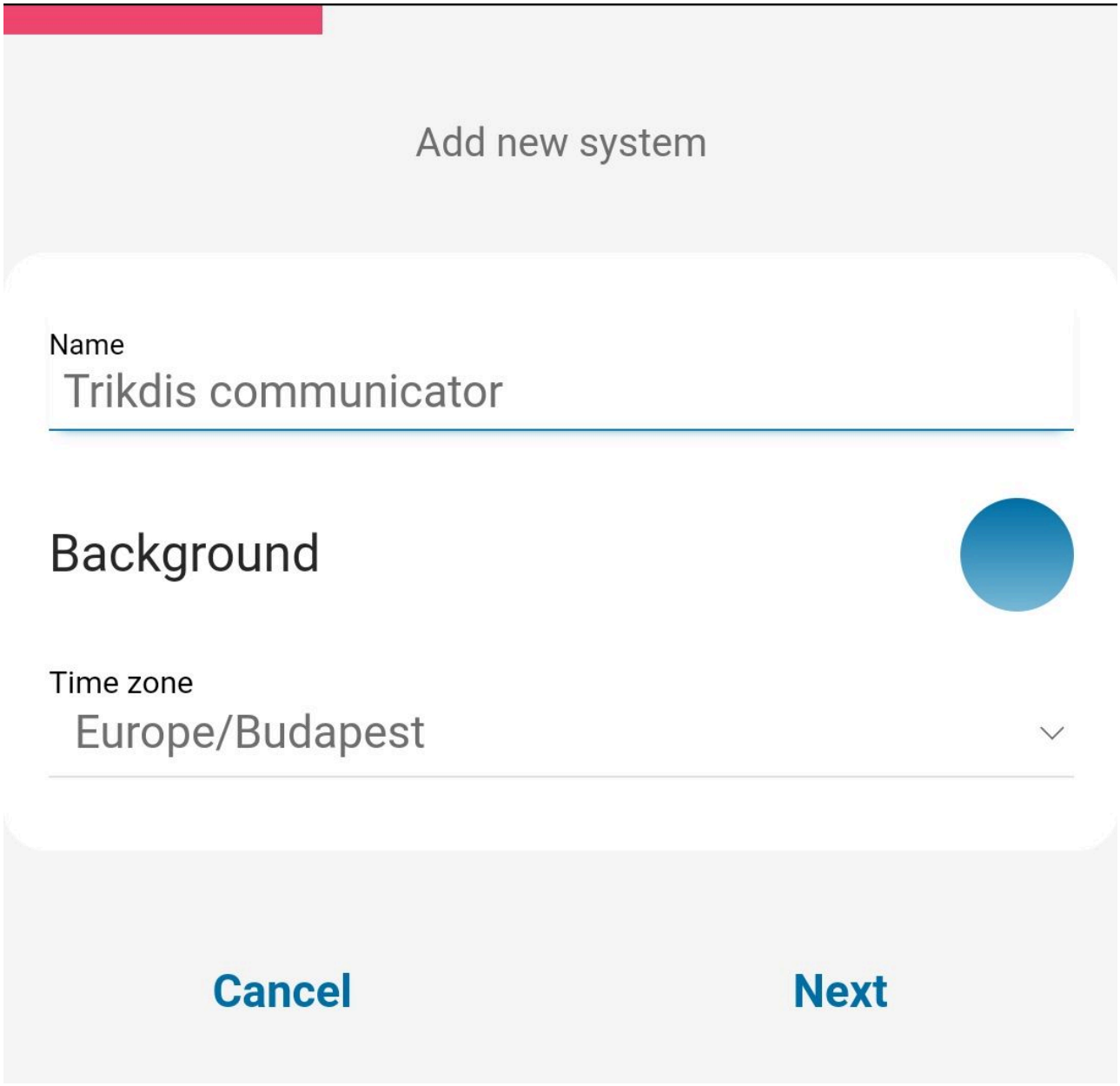
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



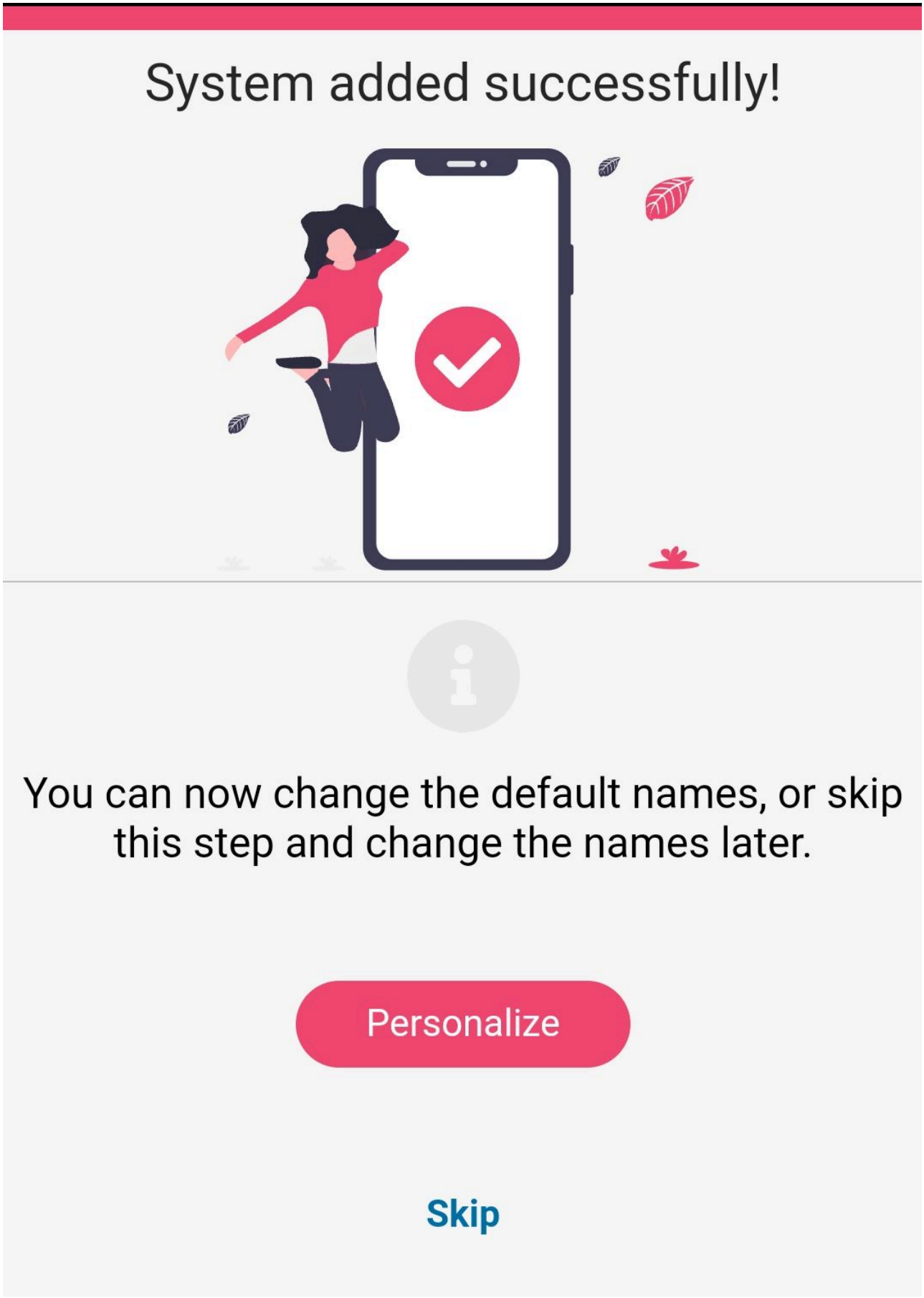
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



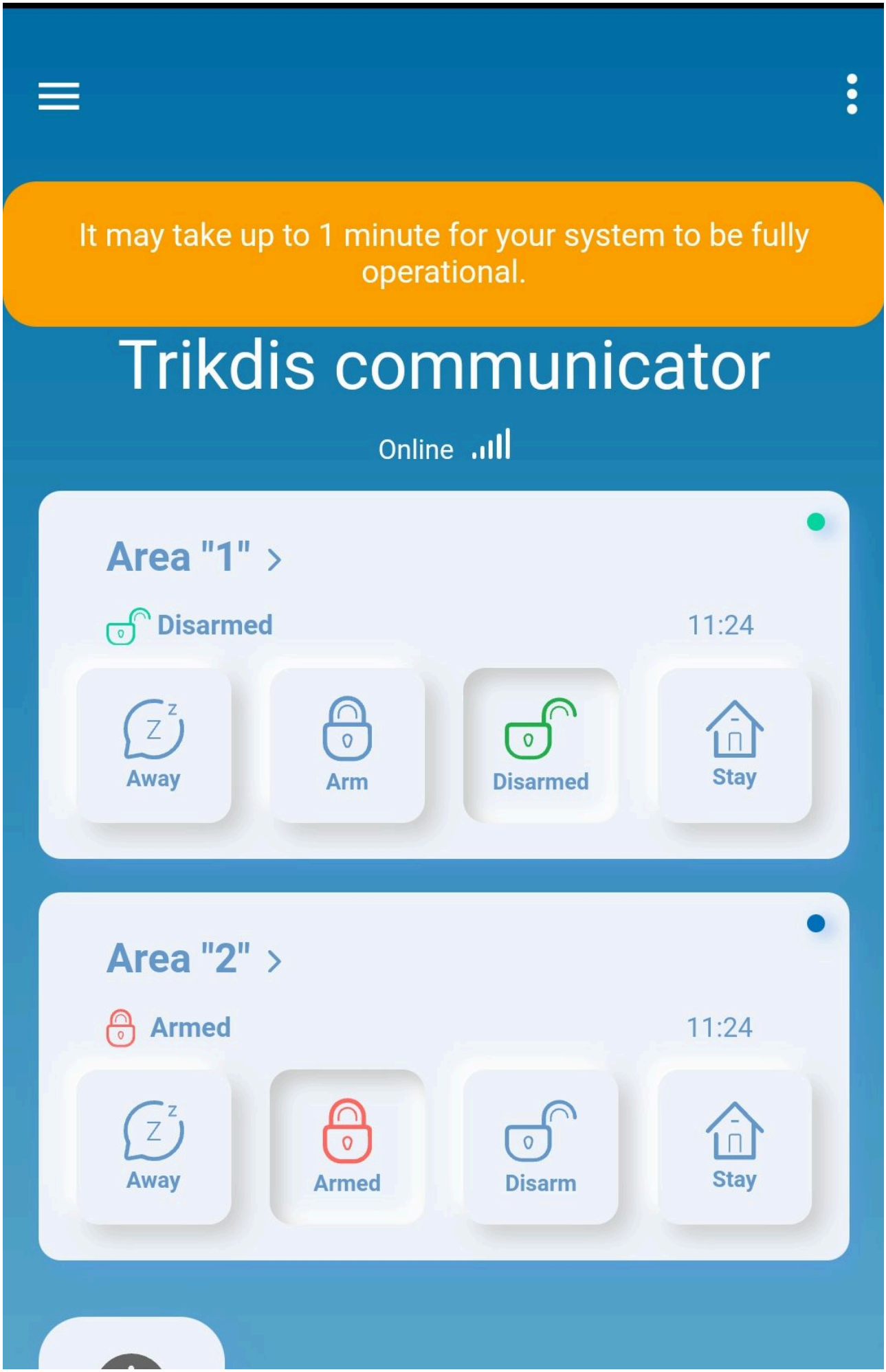
6. Add meg a rendszer nevét és válassz idozónát



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



El identificador único del equipo (**IMEI**) se puede leer en la caja y en la parte trasera del equipo, y también lo muestra la barra de estado de TrikdisConfig.

5.2 Control directo con el código de teclado

Si la central es de los modelos de control directo (apartado 1.2) y en la página **System settings** de TrikdisConfig está marcado **Remote Arm/Disarm**, Protegus 2 muestra las particiones de la central con el estado leído del bus, y para armar / desarmar el usuario introduce en la aplicación **el código de teclado de la central**, el mismo que usa en el teclado. No hace falta una salida aparte ni una zona de llave.

- Para ello, según el fabricante, hay que configurar la central (Paradox: contraseña de PC; Texecom: contraseña de UDL; en las centrales Caddx, Honeywell e InnerRange, habilitar el bus o el puerto serie, ya necesario para leer los eventos); ver el capítulo 4.
- El código de teclado lo comprueba la central, y el registro de eventos de la central anota al usuario, no al comunicador.
- En las centrales Paradox, el código del usuario **no puede ser el código maestro**; después de cambiar un código, reinicia el comunicador (apartado 4.2).
- En las centrales DSC PowerSeries, la aplicación también muestra el estado de las zonas y permite anular zonas; más detalles en el artículo sobre el control directo de DSC.

Al crear el sistema, Protegus 2 pregunta si el armado lo controla una salida del comunicador. Con el control directo **no** asignes ninguna salida a la partición (**Control with Protegus2** desactivado): la partición la gestiona la central y el estado llega del bus.

5.3 Armado con zona de llave

Si la central no se puede controlar directamente, o no quieres usarla así, conectas una salida del comunicador a la zona de llave de la central (apartado 3.4), en TrikdisConfig dejas **Remote Arm/Disarm** sin marcar y en Protegus 2 asignas la salida a la partición.

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.

5.4 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.

Con el control directo, la aplicación pide el código de teclado de la central; con el armado por zona de llave –si está activada– pide la contraseña de Protegus 2.

5.5 Control con mensajes SMS

El comunicador también se puede controlar y programar con mensajes SMS. Estructura del mensaje:

`CONTRASEÑA espacio COMANDO espacio DATOS` – por ejemplo `123456 OUTPUT1 ON`

Con la contraseña de **administrador** se pueden usar todos los comandos; con la contraseña de **instalador**, los comandos INFO, RESET y OUTPUTx. La `x` es el número de salida: el borne I/O configurado como salida (1, 2 o 3) que quieres conmutar.

Comando	Datos	Qué hace	Ejemplo
`INFO`	–	Pide información sobre el dispositivo: tipo, IMEI, número de serie, versión de firmware	`123456 INFO`
`RESET`	–	Reinicia el dispositivo	`123456 RESET`
`OUTPUTx`	`ON`	Activa la salida x	`123456 OUTPUT1 ON`
`OUTPUTx`	`OFF`	Desactiva la salida x	`123456 OUTPUT1 OFF`
`OUTPUTx`	`PULSE=tttt`	Da un impulso en la salida x; `tttt` = duración del impulso en segundos, con cuatro dígitos	`123456 OUTPUT2 PULSE=0002`

Comando	Datos	Qué hace	Ejemplo
`CONNECT`	`PROTEGUS=ON` / `PROTEGUS=OFF`	Habilita o deshabilita la conexión con Protegus	`123456 CONNECT PROTEGUS=ON`
`CONNECT`	`IP=dirección:puerto`	Dirección IP y puerto del canal principal	`123456 CONNECT IP=192.120.120.255:8000`
`CONNECT`	`ENC=clave`	Clave de cifrado TRK	`123456 CONNECT ENC=123456`
`CONNECT`	`APN=nombre`	APN de la tarjeta SIM	`123456 CONNECT APN=internet`
`CONNECT`	`USER=nombre`	Nombre de usuario del APN (si el operador lo pide)	`123456 CONNECT USER=user`
`CONNECT`	`PASS=contraseña`	Contraseña del APN (si el operador la pide)	`123456 CONNECT PASS=password`
`CONNECT`	`CP=n`	Selección del tipo de central de alarma por el número de orden en la lista **Security panel model** de TrikdisConfig	`123456 CONNECT CP=4`
`CONNECT`	`DIR=jjjj` / `DIR=OFF`	Contraseña de 4 dígitos del control directo (la contraseña de PC o UDL de la central); `DIR=OFF` lo desactiva	`123456 CONNECT DIR=1122`

Puedes limitar desde qué números de teléfono acepta comandos el dispositivo: TrikdisConfig → página **User reporting** → **Control by SMS**. Si no hay ningún número indicado, ejecuta los comandos con la contraseña correcta que lleguen desde cualquier número.

6. TrikdisConfig – la configuración en detalle

En la parte izquierda de la ventana de TrikdisConfig está la lista de páginas (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware), arriba la fila de botones (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) y abajo la barra de estado. Este capítulo repasa página por página la configuración del G16.

6.1 La barra de estado

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

Rótulo	Significado
IMEI / Unique ID, en un dispositivo Ethernet **MAC / Unique ID**	Identificador único del dispositivo: en un dispositivo con tarjeta SIM, el IMEI; en un dispositivo Ethernet, la dirección MAC. El mismo figura en la caja y en la parte trasera del dispositivo.
Status	Estado de funcionamiento actual.
Device	Tipo de dispositivo (modelo). Comprueba que aquí figura el modelo de tu dispositivo.
SN	Número de serie.
BL	Versión del bootloader.
FW	Versión del firmware.

Rótulo	Significado
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.

En el campo **Device**, con el G16 debe figurar el modelo del G16 (por ejemplo G16_G410 o G16_54E0). Después de la lectura, el programa muestra la configuración guardada en el G16; ajústala según las descripciones de las páginas que siguen.



Figura 32. Barra de estado de TrikdisConfig con un G16 leído: identificador, estado, modelo, número de serie, versiones, modo de conexión y nivel de acceso.

6.2 System settings

La página tiene dos grupos: en el grupo **General** configuras el funcionamiento básico del equipo y su conexión con la central de alarma, y en el grupo **Access**, los niveles de acceso.

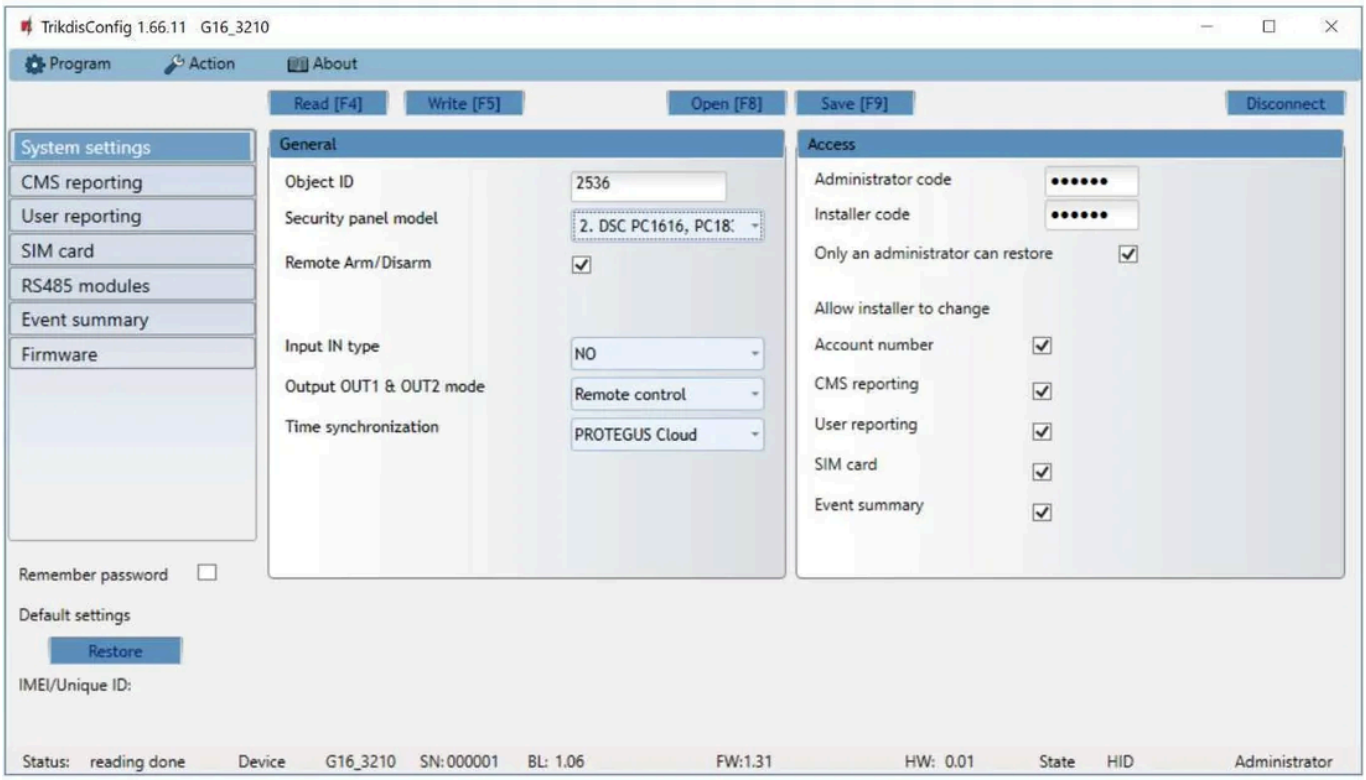


Figura 33. TrikdisConfig – página System settings: grupos General y Access (en la imagen, la versión de hardware 3, G16_3210; la versión 4 no tiene los campos Input IN type y Output OUT1 & OUT2 mode, que han pasado a la página IN/OUT).

- **Object ID** – el identificador de abonado que te da la CRA (4 caracteres hexadecimales, 0–9, A–F). Es obligatorio si el equipo también transmite a la CRA; no se pueden usar `FFFE` ni `FFFF`.
- **Security panel model** – el modelo de la central de alarma conectada, elegido de la lista. De él depende cómo lee el comunicador el bus, así que elige el modelo exacto de la central conectada.
- **Remote Arm/Disarm** – marcado, el comunicador controla la central directamente: el usuario arma y desarma desde Protegus 2 con su código de teclado. Solo aparece en los modelos de central de control directo; según el fabricante, hay que configurar la central (capítulo 4). Con el armado por zona de llave, déjalo sin marcar.
- **Security panel PC download password** – para el control directo de las centrales Paradox y Texecom, la contraseña de PC o de UDL de la central (4 caracteres); debe coincidir con la configurada en la central (apartados 4.2 y 4.3).
- **Time set** – la fuente del reloj del equipo (por defecto **Cloud application**, la nube de Protegus).
- En la **versión de hardware 3**, aquí también están los campos **Input IN type** (el tipo de la entrada: NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL) y **Output OUT1 & OUT2 mode** (el modo de las dos salidas; para el armado con zona de llave, **Remote control**).

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

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

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

¡No dejes las contraseñas de fábrica en el dispositivo!

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

6.3 CMS reporting

El comunicador envía los eventos a la CRA por conexión de datos móviles (IP) o por SMS. Los eventos pueden ir por varios canales: el canal **principal** y el **paralelo** funcionan a la vez (a dos receptores a la vez), y cada uno tiene un canal de **respaldo**, que entra en funcionamiento si ese canal se interrumpe. La comunicación está cifrada y protegida con contraseña; para recibirla hace falta un receptor Trikdis (receptor de software IPcom, RL14, RM14) o un receptor universal que conozca el protocolo DC-09 / TL150. Los receptores Trikdis transmiten los eventos al software de CRA: por conexión IP, el receptor de software **IPcom** (Windows / Linux), el receptor IP/SMS **RL14** o el receptor multicanal **RM14**; para recibir SMS, el RL14, el RM14 o el receptor SMS **GM14**.

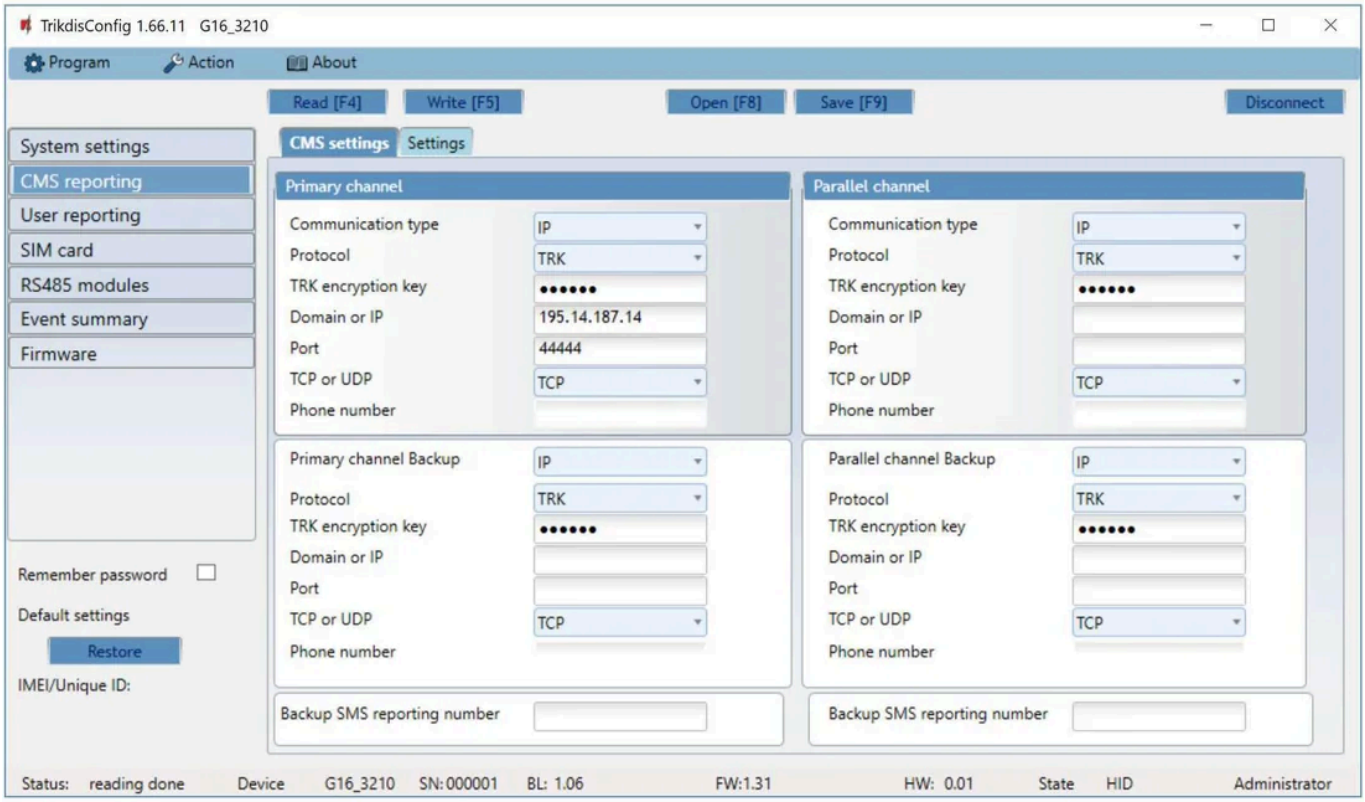


Figura 34. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal, de respaldo y paralelo.

Primary channel – canal principal

- **Communication type** – IP o SMS. El SMS sirve bien como respaldo –funciona aunque no haya conexión de datos móviles–, pero no se recomienda como canal principal.
- **Protocol** – TRK (receptores Trikdis), DC-09_2007 o DC-09_2012 (receptores universales), TL150 (SUR-GARD).
- **TRK encryption key** – clave de cifrado de 6 dígitos; debe ser la misma en el comunicador y en el receptor.
- **Domain or IP**, **Port** – la dirección y el puerto del receptor.
- **TCP or UDP** – el protocolo de transmisión.
- **Phone number** – solo para la comunicación por SMS: el número de teléfono del receptor SMS de Trikdis con el código de país (p. ej. `CCxxxxxxxxx`, donde CC es el código de país).

Primary channel Backup – canal de respaldo. Asume la comunicación si el canal principal no funciona; su configuración es igual que la anterior.

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). Tiene su propio canal de respaldo.

Backup SMS reporting number – número SMS de respaldo. Entra en funcionamiento si no se consigue enviar ni por el canal principal, ni por el paralelo, ni por el de respaldo; es útil porque funciona también sin conexión IP. Solo está activo si el canal principal y el de respaldo están en modo IP. El equipo envía un SMS al receptor SMS de la CRA después del primer arranque, y también si la conexión TCP/IP o UDP/IP se interrumpe tanto en el canal principal como en su respaldo. En el campo escribe el número de teléfono del receptor SMS de Trikdis de la CRA, con el código de país (p. ej. `CCxxxxxxxxx`).

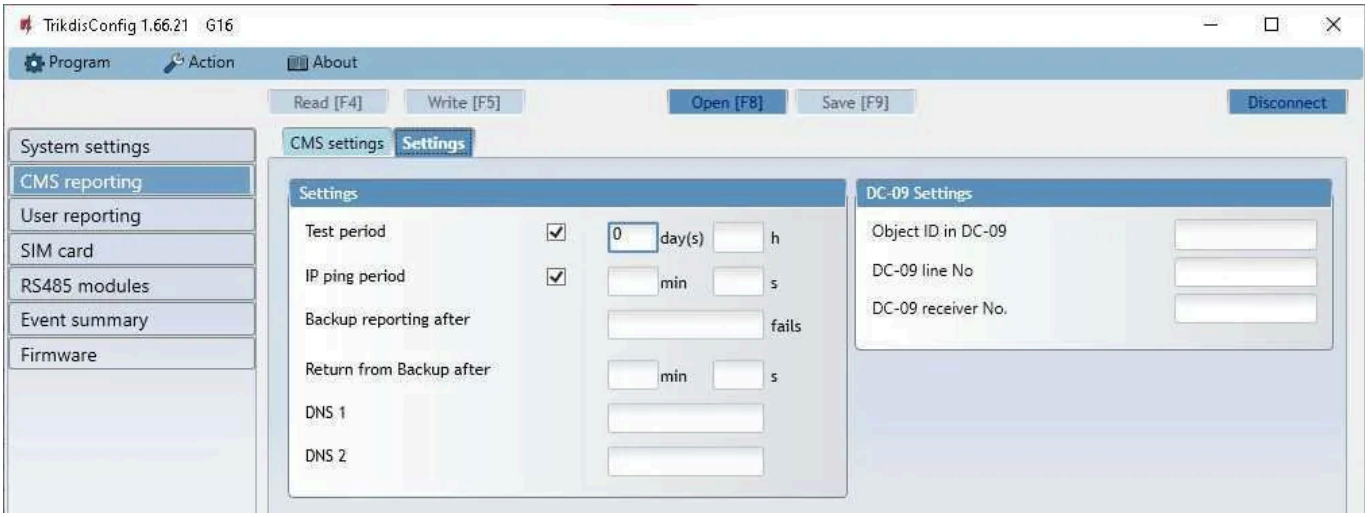


Figura 35. TrikdisConfig – CMS reporting, pestaña Settings: test periódico, PING, temporizaciones del canal de respaldo, DNS y datos DC-09.

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

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

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

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

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

Al pie de la pestaña: **DNS 1, DNS 2** – servidores de nombres; hacen falta si has indicado el receptor con un nombre de dominio y no con una dirección IP. Por defecto, el DNS público de Google. El grupo **DC-09 settings** solo se ve si en algún canal está configurado el protocolo DC-09.

6.4 User reporting

En la pestaña **PROTEGUS Cloud** habilitas el servicio Protegus. Con el servicio Protegus, el usuario puede vigilar y controlar a distancia el comunicador y el sistema; más información: www.protegus.app.

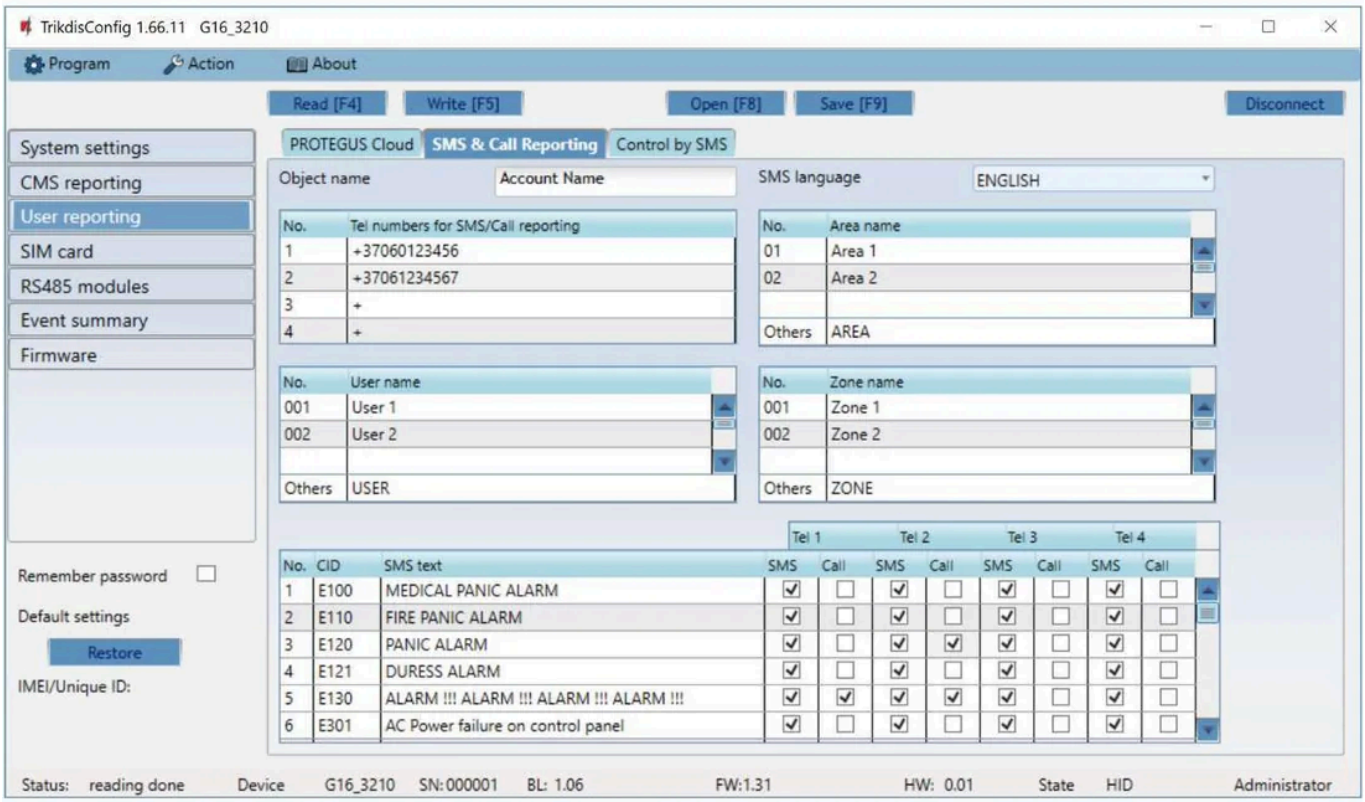


Figura 36. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- **Enable connection** – habilita la conexión con la nube de Protegus y el acceso remoto de TrikdisConfig.
- **Protegus Cloud access code** – código de 6 dígitos para la conexión con Protegus (por defecto `123456`). Solo se puede configurar antes de crear el sistema en Protegus 2; después no se puede cambiar.

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

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

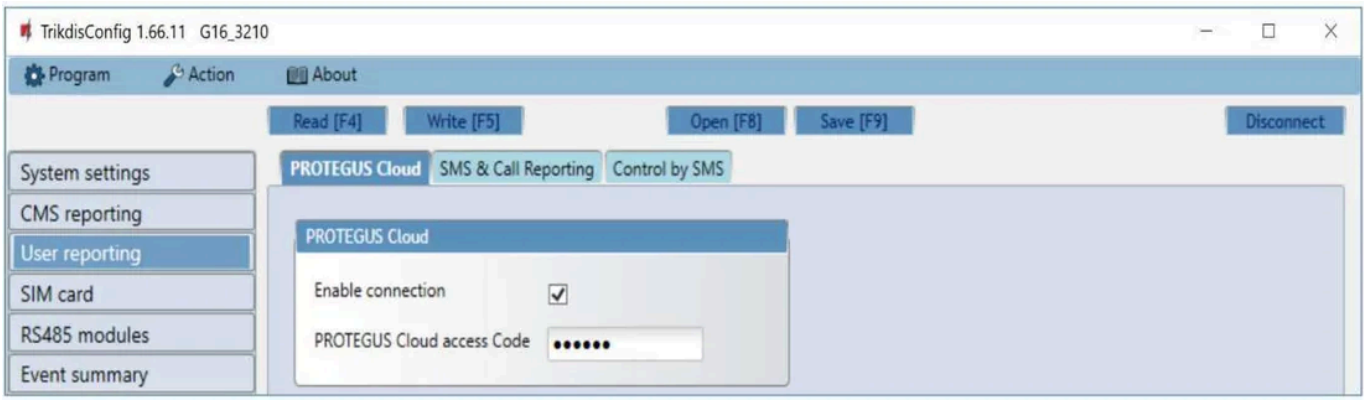


Figura 37. TrikdisConfig – User reporting, pestaña SMS & Call Reporting.

- **Object name** – el nombre del sistema; aparece en todos los SMS.

- **SMS language** – el idioma de los SMS (para los caracteres especiales y acentuados del idioma).
- **Tel numbers for SMS/Call reporting** – hasta 4 números de teléfono con el código de país (`+CC…`, `00CC…` o `CC…`, donde CC es el código de país).
- **Area name, User name, Zone name** – los nombres de las particiones, los usuarios y las zonas; el equipo los usa en el texto de los SMS. En la tabla correspondiente escribe el número de la partición, del usuario o de la zona y, al lado, su nombre. Con una central leída por el bus llegan los números de zona y de usuario propios de la central; asígnales los nombres a esos.
- **CID event table** – para cada evento se puede configurar qué número recibe SMS o llamada; también se pueden cambiar el texto del mensaje y el código Contact ID, y añadir eventos nuevos.

En la pestaña **Control by SMS** configuras la recepción de comandos SMS (los comandos se describen en el apartado 5.5).



Figura 38. TrikdisConfig – User reporting, pestaña Control by SMS.

- **Reply text** – el texto de los cuatro mensajes de respuesta a un comando SMS: comando ejecutado (Command done), contraseña incorrecta (Wrong password), comando incorrecto (Wrong command), datos incorrectos (Wrong data).
- **Tel numbers for control by SMS** – hasta 4 números; el equipo solo acepta comandos de estos números. Si está vacío, acepta el comando con la contraseña correcta desde cualquier número; aun así, la seguridad la da que en el comando es obligatoria la contraseña de administrador o de instalador.

6.5 SIM card

Sin los datos de la tarjeta SIM, el equipo no se conecta a la red de datos.

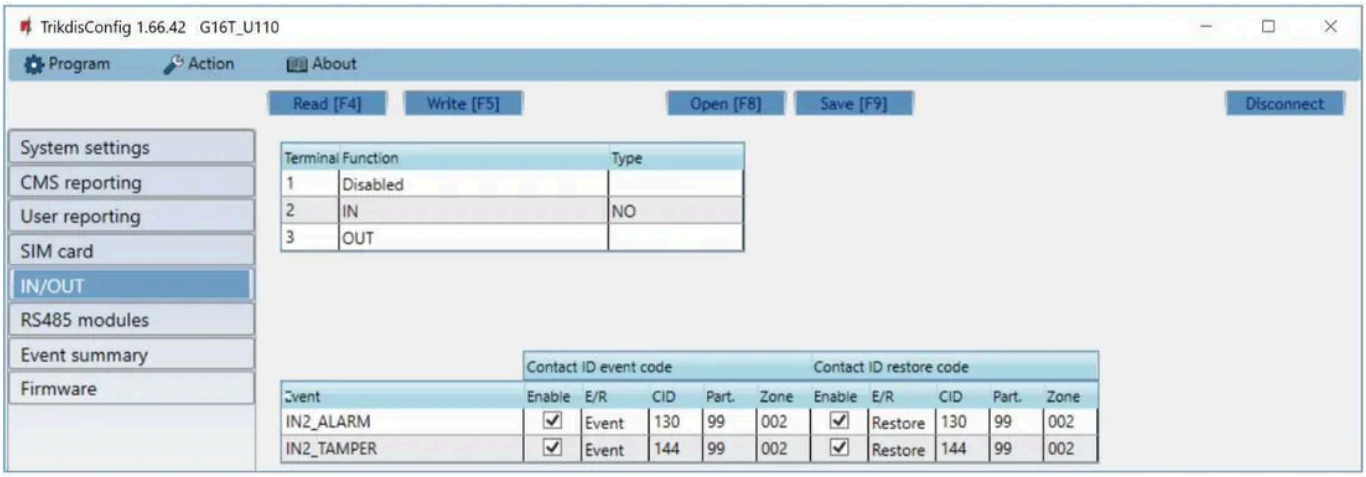


Figura 39. TrikdisConfig – página SIM card.

- **SIM card PIN** – el código PIN de la tarjeta. Puedes desactivar la petición de PIN poniendo la tarjeta en un teléfono móvil y desactivándola allí. Si la petición de PIN está desactivada, el campo puede quedarse con el valor de fábrica.
- **APN** – el punto de acceso del operador (Access Point Name); sin él, el comunicador no puede conectarse a internet. También lo encuentras en la web del operador; el APN «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 del APN, si el operador los exige.
- **Forbid connection when roaming detected** – útil cerca de una frontera: impide que el equipo se conecte a la red del país vecino.

Antes de usarla, asegúrate de que la tarjeta SIM está activa y de que tiene habilitado el servicio de datos móviles para la comunicación IP.

6.6 IN/OUT

Aquí indicas la función de los tres bornes de E/S de doble función del comunicador: **Disabled** (sin usar), **IN** (entrada) u **OUT** (salida). En las entradas también hay que indicar el tipo (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Configuración de fábrica: I/O 1 sin usar, I/O 2 entrada (NO), I/O 3 salida.



Figura 40. TrikdisConfig – página IN/OUT: función de los bornes de E/S y eventos de las entradas.

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

- **Enable** – habilita el envío del mensaje.
- **E/R** – el tipo de evento: Event (alarma) o Restore (restauración).
- **CID** – el código Contact ID.
- **Part.** – el número de partición en el mensaje.
- **Zone** – el número de zona en el mensaje.

En la **versión de hardware 3** no hay página IN/OUT: el tipo de la única entrada se configura en el campo **System settings** → **Input IN type**, el modo de las dos salidas en el campo **Output OUT1 & OUT2 mode**, y los eventos de la entrada (IN_ALARM, IN_TAMPER), en la página **Event summary**.

6.7 RS485 modules

Los expansores iO-8 y los módulos W485 / E485 conectados al bus RS485 se añaden en la pestaña **Modules list**.

En el G16 con módem 2G (G16_G410) esta página no se puede usar: la versión 2G no tiene bus RS485.

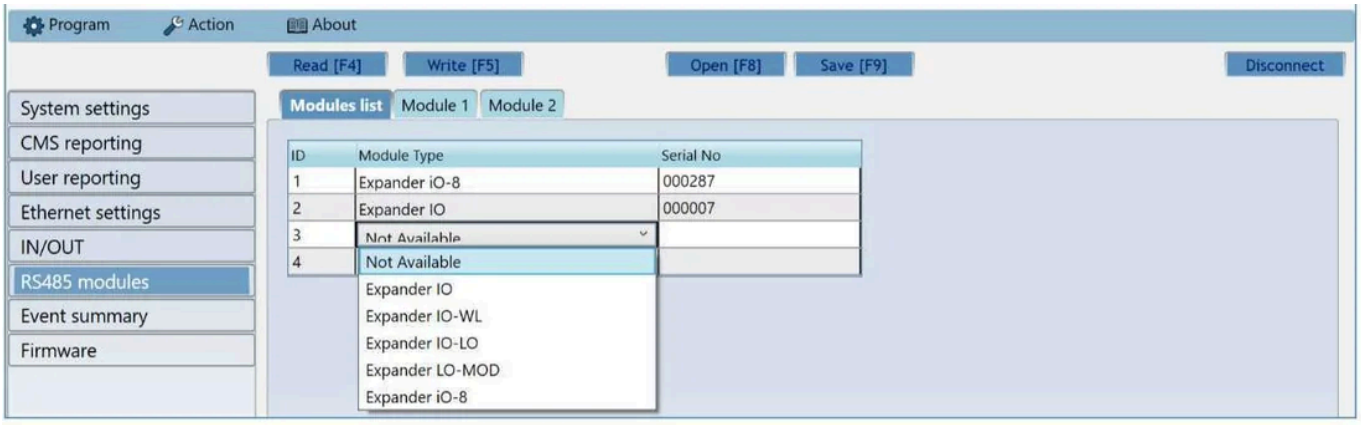


Figura 41. TrikdisConfig – RS485 modules, pestaña Modules list: tipo de módulo (Expander iO-8, W17u/W485, E485) y número de serie.

- **Module Type** – el tipo del módulo conectado, elegido de la lista (Expander iO-8, W17u/W485, E485).
- **Serial No** – el número de serie de 6 dígitos del módulo (en el módulo y en su caja, SN).

Después de elegir el módulo e introducir el número de serie, pulsa el botón **Write [F5]**, desconecta el cable USB y espera un minuto a que el comunicador registre el módulo. Después vuelve a conectar el cable, lee el equipo (**Read [F4]**) y en la página RS485 modules aparece la pestaña propia y numerada del módulo.

Expansor iO-8 – 8 E/S de doble función; se pueden conectar al comunicador hasta 4 módulos.

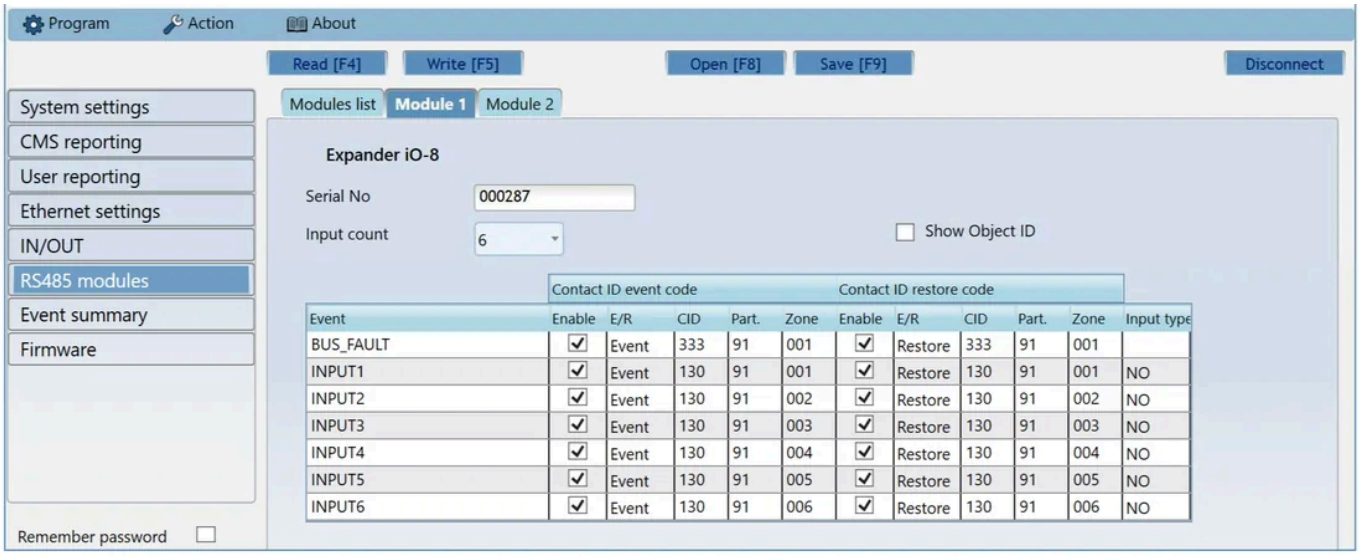


Figura 42. TrikdisConfig – RS485 modules, pestaña del módulo iO-8.

- **Input Count** – cuántos bornes serán entradas; los demás serán salidas. El tipo de entrada (**Input type**: NO o NC) se indica en la tabla. La función de las salidas (armado / desarmado con zona de llave o accionamiento de un equipo) se configura en la aplicación Protegus 2.
- En la tabla puedes asignar un código Contact ID al fallo del bus (**BUS_FAULT**, Contact ID 333) y a los eventos de activación y restauración de las entradas (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). Cuando se activa una entrada, el comunicador envía un evento con el código configurado al receptor

de la CRA, a la aplicación Protegus 2 y por SMS al número de teléfono del usuario. Por defecto, el módulo 1 transmite con la partición 91 y el módulo 4 con la partición 94. Marcando **Show Object ID** se puede indicar para las entradas un identificador de abonado distinto del del comunicador.

- Si el usuario también debe recibir SMS o llamada por las entradas del expansor, añade el código Contact ID asignado a la entrada también a la tabla de eventos de la pestaña **SMS & Call Reporting**.

Módulo WiFi W485 (en la lista, W17u/W485) – los datos de la red WiFi y la configuración de red.

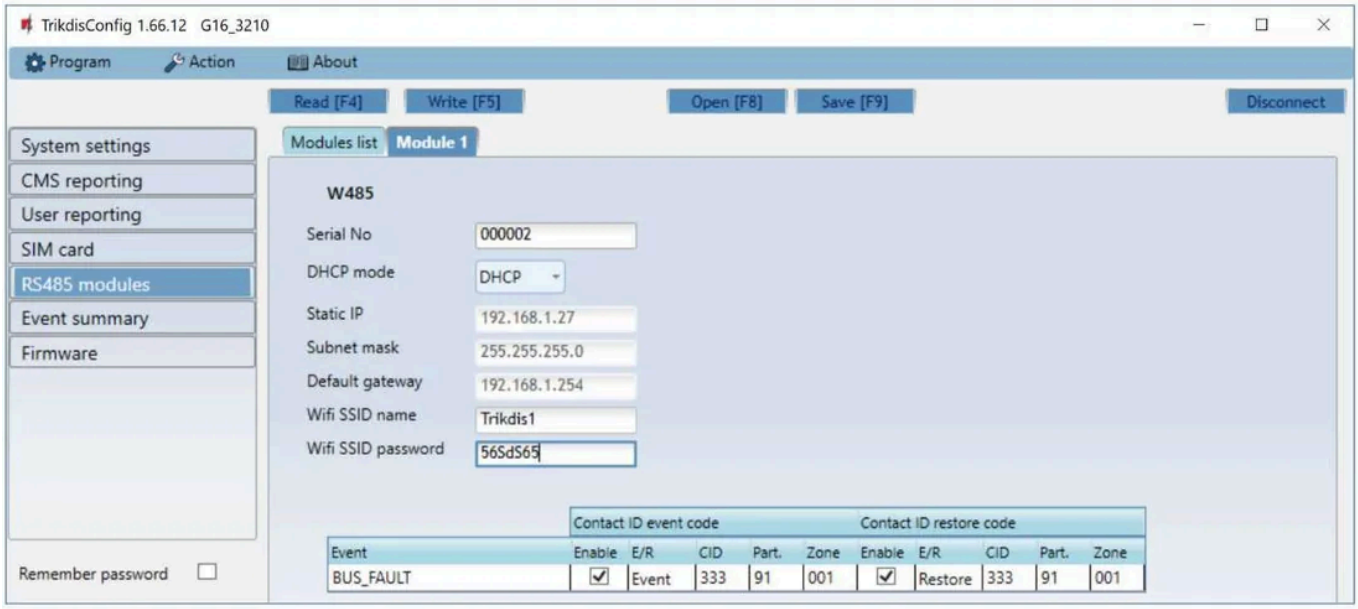


Figura 43. TrikdisConfig – RS485 modules, pestaña del módulo W485.

- **DHCP mode** – configuración de red automática (DHCP) o manual (Static).
- **Static IP**, **Subnet mask**, **Default gateway** – con la configuración manual.
- **Wifi SSID name**, **Wifi SSID password** – el nombre y la contraseña de la red WiFi.
- En la tabla puedes asignar un código Contact ID a los fallos del bus RS485 (interrupción y restablecimiento de la conexión entre el módulo y el G16); el evento lo reciben tanto la CRA como Protegus 2.

Módulo Ethernet E485 – la misma configuración de red, sin WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**); en la tabla también aquí puedes asignar un código Contact ID al fallo del bus RS485 (interrupción y restablecimiento de la conexión entre el E485 y el G16), que reciben tanto la CRA como Protegus 2.

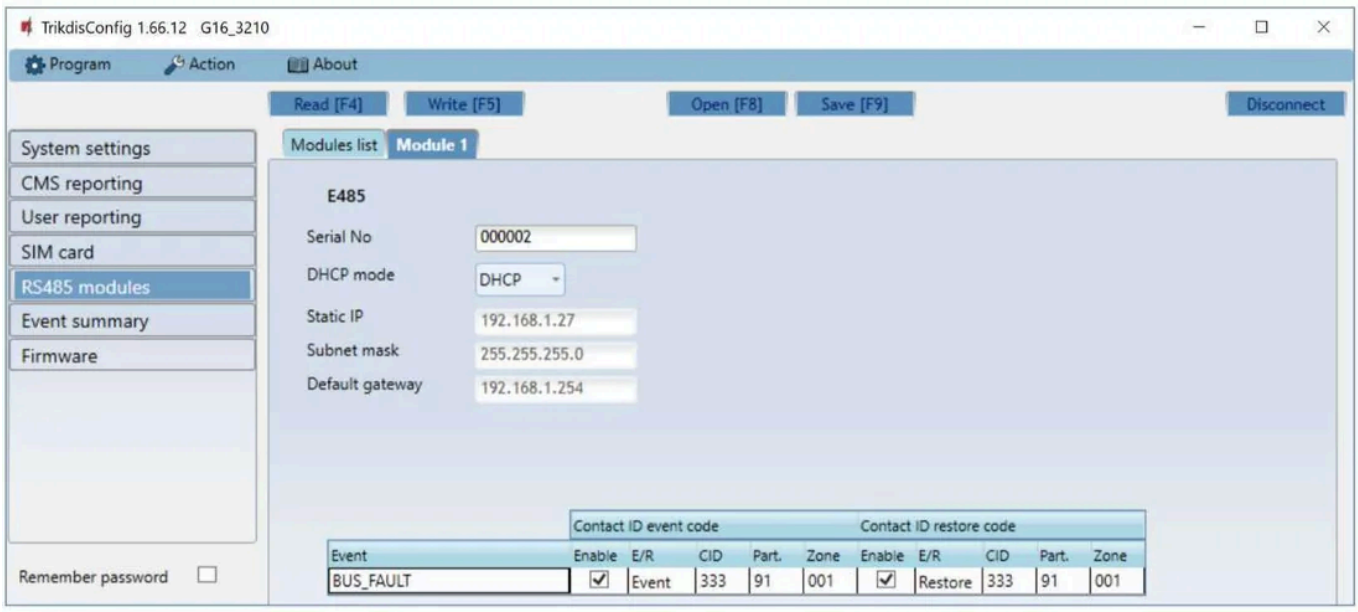


Figura 44. TrikdisConfig – RS485 modules, pestaña del módulo E485.

Para que funcionen el W485 y el E485, la conexión del G16 con la CRA y/o con Protegus debe estar configurada (apartados 2.3 y 2.4), y el G16 tiene que tener una tarjeta SIM. Mientras la conexión por cable o WiFi está activa, el comunicador se comunica por ella y no usa la conexión de datos móviles.

6.8 Event summary

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

Mensaje	Contact ID	Cuándo se genera
COMMUNICATION	350	Se ha interrumpido la comunicación entre el comunicador y la central de alarma (desactivado de fábrica). El comunicador conectado al bus o al puerto serie lo detecta directamente; el comunicador de línea telefónica, solo con **Line supervision** activado.
POWER	302	Tensión de alimentación inadecuada (baja); su restablecimiento es un mensaje aparte.
REMOTE_STARTED	411	Ha comenzado una programación remota con TrikdisConfig.
REMOTE_FINISHED	412	La programación remota ha terminado.
START	700	El dispositivo se ha conectado a la red (arranque).
TEST	602	Informe de prueba periódico.
PING	760	El mensaje de señal de vida PING. No figura en la lista de todos los dispositivos: en la pantalla de la versión de hardware anterior sí, pero en la página Event summary de las versiones más nuevas no hay esta fila. Su intervalo se ajusta en el campo **CMS reporting → Settings → IP ping period**.

- **Enable** – habilita el envío del mensaje a la CRA y a Protegus 2.
- **E/R** – tipo de mensaje: Event (evento) o Restore (restablecimiento); la fila indica que el evento se ha producido o que se ha restablecido.

- **Part.** – número de partición (área) que envía el dispositivo con el evento interno y con el restablecimiento.
- **Zone** – número de zona que envía el dispositivo con el evento interno y con el restablecimiento.
- El código **CID**, la **partición** y la **zona** se pueden cambiar en cualquier evento; donde hay restablecimiento (Restore), su código se puede indicar por separado.

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

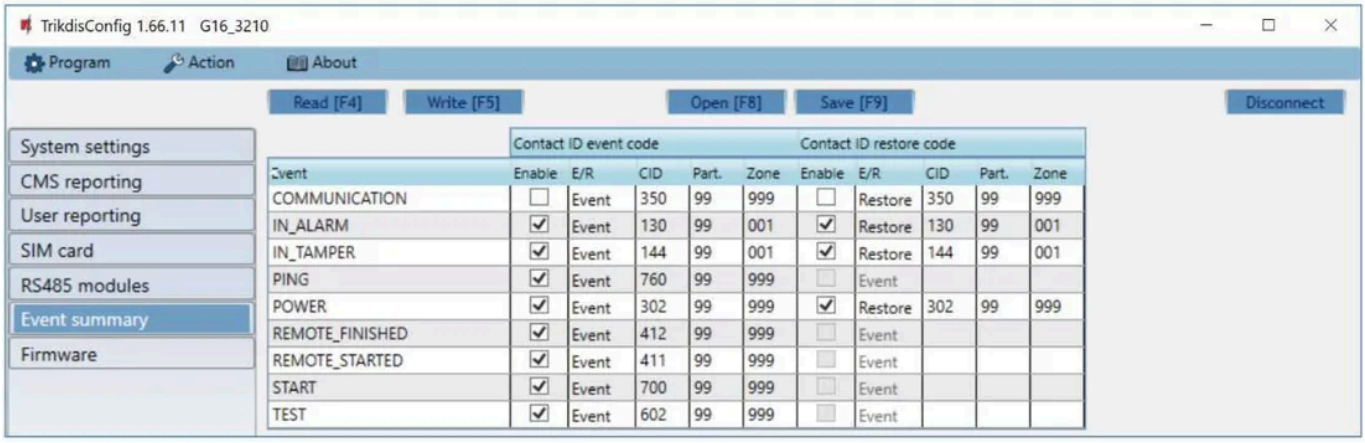


Figura 45. TrikdisConfig – página Event summary: los mensajes internos del equipo (en la imagen, la versión de hardware 3, en la que los eventos IN_ALARM e IN_TAMPER de la entrada y el PING también figuran aquí; en la versión 4, los eventos de las entradas están en la página IN/OUT).

6.9 Restablecer la configuración de fábrica

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

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

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.

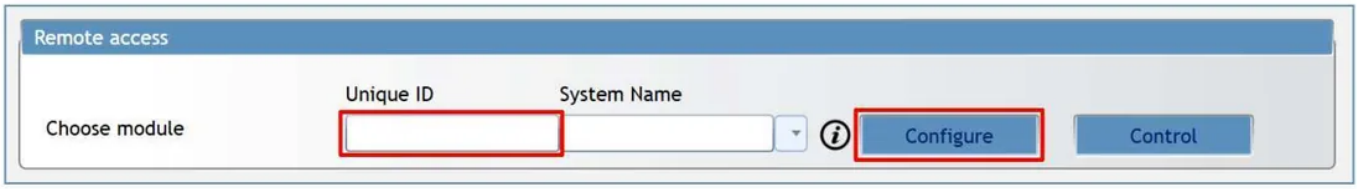


Figura 46. TrikdisConfig – Remote access: el identificador del equipo, el nombre del sistema y el botón Configure.

8. Comprobación 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.

Con una central conectada al bus, comprueba también que el comunicador lee realmente de la central: arma y desarma la central desde el teclado y mira si el evento aparece en la lista de eventos de Protegus 2 (y en la CRA) con el número de partición y de usuario correctos. Con el control directo, haz también un armado de prueba desde la aplicación, con el código de teclado del usuario.

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.

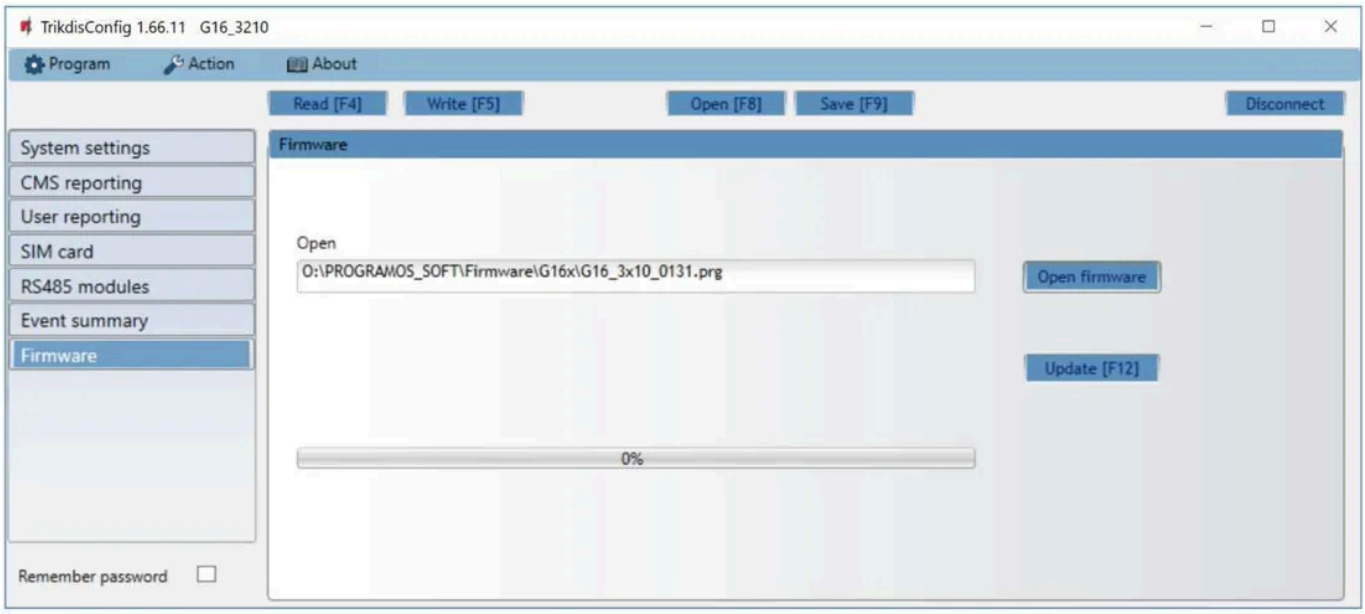


Figura 47. TrikdisConfig – página Firmware: Open firmware y Update [F12].

Para la actualización hace falta conexión a internet. Un antivirus, un cortafuegos o una configuración de red estricta pueden impedir la descarga automática del firmware; en ese caso cambia la configuración del antivirus (permite el acceso a internet de TrikdisConfig) o descarga el archivo a mano y ábrelo en la página Firmware.

10. Problemas y preguntas frecuentes

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

El LED NETWORK no se enciende: no hay red

1. Mira los destellos del LED **TROUBLE**: 1 = no hay SIM, 2 = PIN incorrecto, 3 = falta el APN, 4 = no puede conectarse a la red móvil, 5 = no puede conectarse a la red de datos.
2. Comprueba que la tarjeta SIM esté activa, tenga servicio de datos y esté bien colocada en la ranura.
3. Si la petición de PIN está activada en la tarjeta, introduce el PIN en la página **SIM card** o desactiva la petición de PIN en un teléfono.
4. Comprueba la antena: está enroscada, no está dentro de una caja metálica y el nivel de señal es suficiente (apartados 1.7 y 3.2).

Hay red, pero la CRA no recibe eventos

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

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

El LED TROUBLE da siete destellos: el comunicador no ve la central

1. Comprueba la conexión según el esquema del apartado 3.3: el fallo más frecuente es que los cables **CLK** y **DATA** estén intercambiados o que la línea de datos esté conectada a un borne equivocado de la central.
2. En el campo **System settings** → **Security panel model** de TrikdisConfig debe estar elegido el modelo exacto de la central conectada.
3. En las centrales Texecom, Caddx, Honeywell e InnerRange también hay que configurar la central (capítulo 4); sin ello, la central no da datos en el bus.
4. En las centrales Paradox, puede que el puerto serie venga bloqueado de fábrica: así puedes desbloquearlo.
5. Después de conectar una central Pyronix, déjala sin alimentación y reiníciala para que acepte el comunicador.
6. Con la central DSC PowerSeries **NEO**, el G16 no funciona (el bus de la NEO no admite dispositivos externos); en ese caso hace falta un comunicador de línea telefónica.

Los eventos llegan, pero no puedo armar desde la aplicación

Con el control directo:

1. En la página **System settings** debe estar marcado **Remote Arm/Disarm**.
2. En las centrales Paradox y Texecom, el **Security panel PC download password** debe coincidir con la contraseña de PC o de UDL de la central (apartados 4.2 y 4.3).
3. En las centrales Paradox, el firmware de la central debe ser como mínimo **V.4**; el código del usuario no debe ser el código maestro; después de cambiar un código, reinicia el comunicador.

4. En las centrales Honeywell Vista, debe estar habilitada la 2.ª dirección AUI (apartado 4.6).
5. En Protegus 2, la partición **no** debe tener ninguna salida asignada (Control with Protegus2 desactivado).

Con zona de llave:

1. **Remote Arm/Disarm** debe estar sin marcar, y el borne de E/S debe estar en **OUT** en la página **IN/OUT**.
2. La zona de la central debe ser de tipo llave, y en Protegus 2 la partición debe tener asignada la salida correspondiente, en modo de impulso o biestable según la zona (apartado 5.3).

Protegus 2 no ve el equipo

1. En la pestaña **User reporting → PROTEGUS Cloud** debe estar marcado **Enable connection**.
2. Al crear el sistema hay que introducir el **Protegus Cloud access code** configurado en el equipo; una vez creado el sistema, ya no se puede cambiar en el equipo.
3. Escribe el IMEI exactamente, tomándolo de la caja o de la parte trasera.
4. El servicio de datos de la tarjeta SIM y el APN deben estar bien (el LED NETWORK está verde y el LED DATA se apaga después de un evento).

No puedo entrar a distancia con TrikdisConfig

1. El equipo debe estar en línea (LED NETWORK verde) y la conexión con Protegus debe estar habilitada.
2. **CMS reporting → Settings → IP ping period** no debe ser de más de 5 minutos: el PING mantiene la conexión necesaria para el acceso remoto.
3. Comprueba la contraseña de administrador o de instalador.

He olvidado la contraseña

Una contraseña olvidada no se puede consultar ni borrar restableciendo los ajustes de fábrica, porque el restablecimiento también requiere contraseña. En ese caso solo el fabricante o el distribuidor puede restablecerla: hay que hacerle llegar el equipo. Por eso, anota las contraseñas que configures en un lugar seguro.

¿Por qué no veo la página RS485 modules, o por qué no funciona el iO-8?

El G16 con módem 2G (G16_G410) no tiene bus RS485; los módulos iO-8, W485 y E485 solo se pueden conectar a la versión 4G (G16_54E0). Para los módulos W485 y E485, el G16 también tiene que tener una tarjeta SIM.

Tengo un equipo 2G: ¿hasta cuándo funcionará?

El apagado de las redes 2G avanza a distinto ritmo en cada operador; para un funcionamiento a largo plazo recomendamos la versión 4G, que además se puede ampliar con el bus RS485.

¿Cuánto tráfico de datos usa el equipo?

Los mensajes de eventos y los PING son muy pequeños; el tráfico depende sobre todo del periodo de PING y de la frecuencia de los test periódicos. En un sistema doméstico medio, el tráfico mensual suele quedarse 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.

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 atentamente el manual; no seguir las instrucciones puede provocar un funcionamiento incorrecto o una avería.
- Antes de la conexión, en cada conexión eléctrica y antes de cualquier reparación, desconecta el equipo de la alimentación.
- Los fallos debidos a una instalación o un uso incorrectos, así como las modificaciones y reparaciones no autorizadas por el fabricante, anulan la garantía.
- Respeta las normas locales de gestión de residuos: no tires el equipo averiado ni sus piezas a la basura doméstica.

Ver también

- Buscador de compatibilidad: qué comunicador corresponde a cada central de alarma.
- G16 – control directo de las centrales de alarma DSC PowerSeries: armado con el código de teclado, estado de las zonas, anulación de zonas.
- DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones: por qué el G16 no se puede conectar a la NEO y cuál es la solución.
- Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox: desbloqueo del puerto serie de las centrales Paradox más nuevas.
- Armado a distancia con zona de llave desde la aplicación Protegus 2: los detalles y las trampas del armado con zona de llave.
- Llega la versión de hardware v4 de los comunicadores GSM G16 y G16T: qué ha cambiado respecto a la versión 3.
- Configuración del APN – lista de operadores móviles europeos: el APN de la tarjeta SIM según el operador.
- Documentación en inglés: docs.trikdis.com.

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

Productos relacionados

Trikdis G16 4G GSM comunicador inteligente | **Trikdis G16 2G GSM comunicador inteligente**

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

CRP2B cable de conexión puerto serie para paneles de alarma Paradox

Trikdis CRP4 cable serie para paneles de control Texecom

Trikdis iO8 módulo expansor cableado

Derechos de autor

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

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

Versión siempre actualizada de este manual: https://trikdis.es/manual-g16