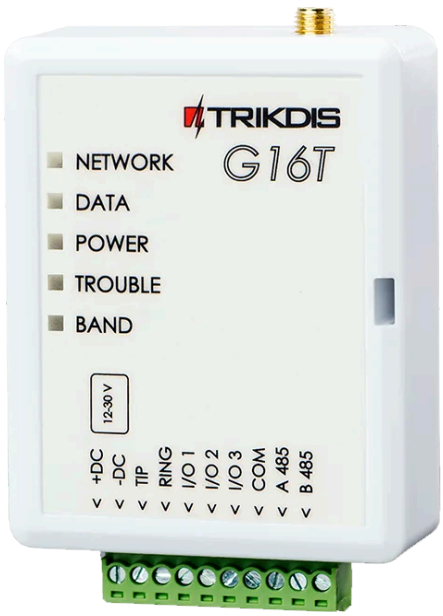
mobilamb
TRIKDIS Official Distributor

Comunicador G16T – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Trikdis G16T: conexión a la central de alarma, tarjeta SIM y configuración en TrikdisConfig, transmisión a la CRA, aplicación Protegus 2, comprobación y resolución de problemas.



Edición: 2026-11-17
Versión web siempre actualizada: https://trikdis.es/manual-g16t

Índice

1. Descripción general

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

2. Puesta en marcha rápida con TrikdisConfig

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

3. Instalación y conexionado

3.1 Pasos de la instalación
3.2 Ubicación y antena
3.3 Conexión a la central de alarma
3.3.1 Si está justificado: supervisión de línea
3.4 Conexión de la zona de interruptor de llave
3.5 Conexión de 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 Programación del marcador de la Honeywell Vista
4.2 Centrales de otros fabricantes

5. Control a distancia con la aplicación Protegus 2

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

6. TrikdisConfig – los ajustes en detalle

6.1 La barra de estado
6.2 System settings
6.3 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 los ajustes de fábrica

7. Programación a distancia

8. Comprobación del funcionamiento del comunicador

9. Actualización del firmware

10. Resolución de problemas y preguntas frecuentes

11. Normas de seguridad

Ver también

1. Descripción general

El G16T es el **comunicador universal de red móvil** de Trikdis: se conecta a la salida de línea telefónica (TIP/RING) de la central de alarma y se comporta como una centralita telefónica. La central de alarma «marca», envía el mensaje Contact ID con tonos DTMF, y el G16T descuelga la línea, decodifica el mensaje y lo transmite por conexión de datos móviles al receptor de la CRA, así como a la nube de Protegus, a la aplicación del usuario. Así se puede usar con **centrales de cualquier marca** que tengan marcador Contact ID: no hace falta cambiar la central, solo configurar su marcador. Los comunicadores G16T están certificados en el grado de seguridad más alto, **EN 50131 Grade 4**.

1.1 Para qué sirve y cómo funciona

- **Transmite a la CRA.** Envía los eventos por conexión IP al receptor de software o de hardware de Trikdis (protocolo TRK) –que funcionan con cualquier software de CRA– o a cualquier receptor universal (SIA DC-09 2007/2012, SUR-GARD TL150). Hacia un receptor SUR-GARD convierte los códigos Contact ID recibidos de la central en códigos SIA; la tabla de conversión está en el apéndice de la documentación en inglés de Trikdis. Por defecto comprueba la conexión cada 30 segundos (o con el intervalo configurado) y, si hay un fallo, pasa al canal de respaldo.
- **Avisa al usuario.** La aplicación Protegus 2 muestra lo ocurrido con notificaciones push, con un sonido propio y en la lista de eventos; desde la aplicación el usuario puede armar y desarmar, y accionar los equipos conectados (iluminación, puerta, ventilación, calefacción, riego, etc.). La aplicación funciona con cualquier central de alarma a la que esté conectado el comunicador, sea cual sea el fabricante de la central.
- **Funciona a la vez o por separado** con la CRA y con el usuario: se puede usar solo con Protegus 2 (sin CRA), solo con la CRA o con ambos. Si ambos están configurados, envía el evento primero a la CRA y después al usuario.
- **Respaldo por SMS.** Avisa también a la CRA por SMS si la conexión de datos no funciona en la red del operador; puede enviar en paralelo a dos receptores, cada uno con su propio canal de respaldo.
- **Tiene entradas y salidas propias.** Tres bornes I/O de doble función se pueden usar como entrada (detector, tamper) o como salida controlable (zona de interruptor de llave, relé). En el bus RS485 de la versión 4G, con el expansor iO-8 se añaden otras 8 I/O (con otro expansor cableado o inalámbrico de la serie iO, más entradas y salidas; con el expansor iO o iO-WL, supervisión remota de temperatura), 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 muestra en la figura siguiente: la salida de línea telefónica de la central de alarma se conecta al G16T, el G16T llega a internet a través de la red móvil y desde allí al receptor de la CRA y a la nube de Protegus, y el usuario ve el sistema en la aplicación Protegus 2.

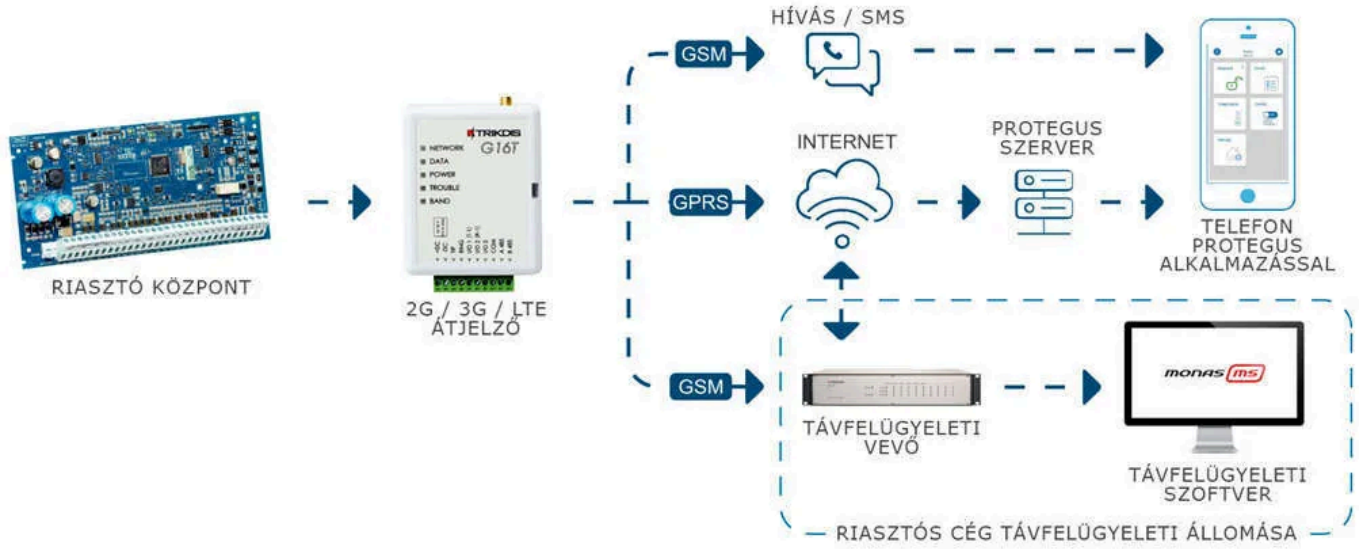


Figura 1. El lugar del G16T en el sistema: central de alarma → G16T → red móvil → receptor de la CRA y nube de Protegus → aplicación Protegus 2.

1.2 Versiones

Este manual se ha escrito para la **versión de hardware 4** del G16T, 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. Las diferencias se resumen en la tabla siguiente; donde 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	G16T_321x (2G), G16T_331x (3G), G16T_341x (4G), G16T_3M10 (LTE Cat-M1 + 2G) – todos con 1 tarjeta SIM	G16T_G410 (2G), G16T_E120 (4G, con respaldo 2G)
Entradas/salidas	2 entradas de tipo seleccionable (T-1/IN1, R-1/IN2 – también se pueden usar para supervisar la línea telefónica) + 1 salida de colector abierto (OUT, máx. 0,15 A)	3 bornes I/O 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)
Consumo	60–100 mA; durante el envío, 250 mA como máximo	60–100 mA; durante el envío, 500 mA como máximo
Frecuencias del módem	2G: 850 / 900 / 1800 / 1900 MHz; 3G: 800 / 850 / 900 / 1900 / 2100 MHz; 4G: según la región	2G: 850 / 900 / 1800 / 1900 MHz; 4G: según la región
Dimensiones	92 × 62 × 26 mm	92 × 65 × 26 mm
Bus RS485 (iO-8, W485, E485)	sí	solo en la versión 4G (G16T_E120)

La versión de hardware 4 se fabrica con dos módems:

Modelo	**Módem**	**Frecuencias**	**RS485 (iO-8, W485, E485)**
G16T_G410	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz	no
G16T_E120	4G (LTE), con respaldo 2G	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 dispositivo.

1.3 Características principales

Conexión con la central de alarma

- Conexión normal a la salida de línea telefónica de la central: DC+, DC−, TIP y RING. Si está justificado, también se puede conectar con supervisión de línea (con los hilos T-1 y R-1): en ese caso el enlace entre la central y el comunicador está **supervisado** y el comunicador avisa si se corta el cable.
- La central envía los eventos en formato Contact ID, con marcación DTMF; el G16T transmite la información completa del evento (código, partición, zona o usuario).

Comunicación con la CRA

- Conexión IP con los receptores de 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 eventos de 60 mensajes.

Funciones para el usuario

- Aplicación móvil y web Protegus 2: notificación push con sonido propio, lista de eventos, armado y desarmado, accionamiento de salidas.
- Supervisión remota de temperatura (con expansor iO o iO-WL).
- Control y configuración básica también con comandos SMS.
- Aviso también por SMS y por llamada telefónica, a un máximo de 4 números de teléfono.
- Derechos de usuario de varios niveles en la aplicación (administrador, instalador, usuario).

Instalación y configuración

- Los ajustes se pueden guardar en un archivo y cargar en otro comunicador.
- Dos niveles de acceso: administrador (el de la CRA) e instalador.
- Se puede configurar y actualizar a distancia con el software TrikdisConfig.

1.4 Partes del comunicador

El G16T 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 figura siguiente se ve la versión 4G; la versión 2G no tiene LED BAND ni bornes A 485 / B 485.

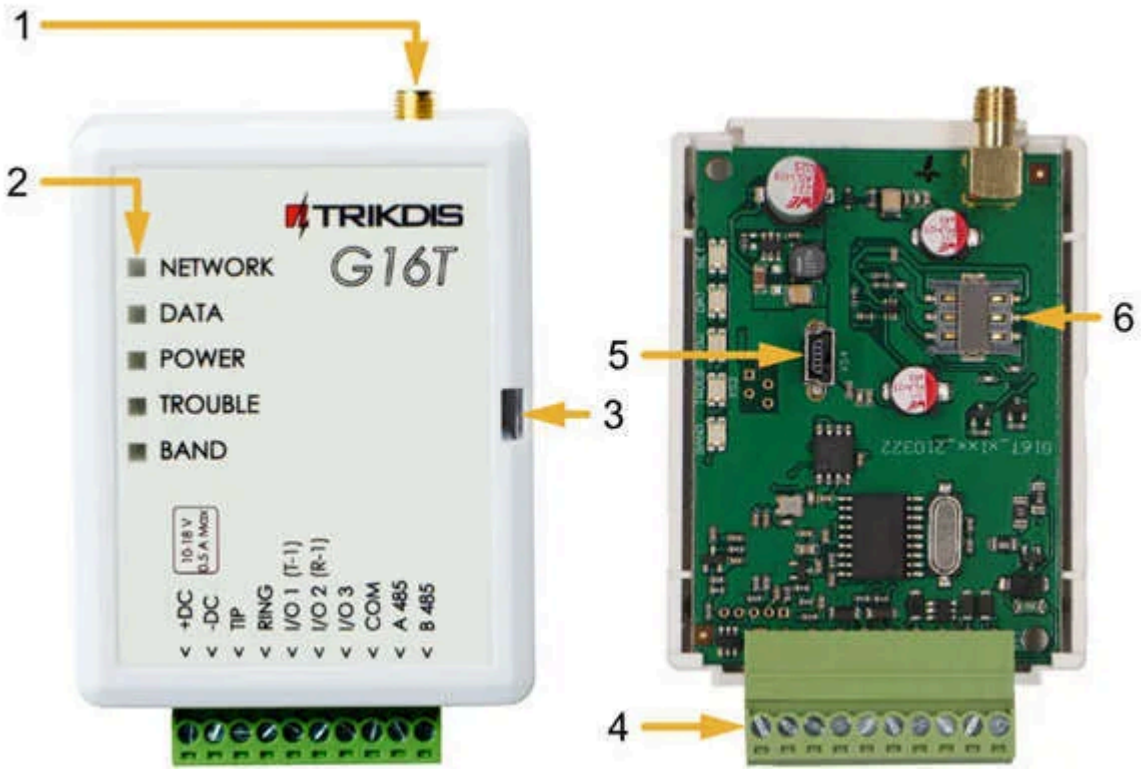


Figura 2. Partes del G16T (versión 4G), de frente y con la caja abierta.

- 1 Conector SMA de la antena GSM
- 2 Indicadores LED (NETWORK, DATA, POWER, TROUBLE, BAND)
- 3 Ranura que ayuda a 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 dispositivo se puede desconectar de la alimentación o reiniciar con un solo gesto, es más cómodo de manejar durante el cableado y, para programarlo por USB, se puede llevar al ordenador.

1.5 Bornes

Borne	Función
+DC	Alimentación, +10–18 V DC
–DC	Alimentación, negativo
TIP	Borne TIP de la central de alarma
RING	Borne RING de la central de alarma
I/O 1 (T-1)	Entrada/salida 1, o punto T-1 de la supervisión de la línea telefónica
I/O 2 (R-1)	Entrada/salida 2, o punto R-1 de la supervisión de la línea telefónica
I/O 3	Entrada/salida 3
COM	Punto común (negativo) de las entradas y salidas
A 485	Hilo A del bus RS485 (solo versión 4G)
B 485	Hilo B del bus RS485 (solo versión 4G)

La rotulación de la regleta de bornes también figura en la tapa frontal, así que para el cableado no hace falta quitar la tapa.

1.6 Indicaciones LED

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

NETWORK – conexión de red

Indicación	Significado
apagado	Sin conexión con la red móvil
parpadea en amarillo	Conexión a la red móvil en curso
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 3G/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	Envío o recepción de datos en curso (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 inadecuada (11,5 V como máximo)
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 (no hay APN)
4 destellos rojos	No puede registrarse en la red móvil (error de registro)
5 destellos rojos	No puede conectarse a la red de datos (GPRS/UMTS/LTE)
6 destellos rojos	Sin conexión con el receptor de la CRA
7 destellos rojos	Se ha perdido la conexión con la central de alarma
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)

1.7 Datos técnicos

Parámetro	Valor
Conexión con la central de alarma	línea telefónica cableada (TIP/RING), Contact ID, DTMF
Entradas/salidas	3 I/O 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 I/O) 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; 500 mA como máximo durante el envío
Protocolos de transmisión	TRK, DC-09_2007, DC-09_2012, TL150
Memoria de eventos	60 mensajes
Cifrado	AES-128

Parámetro	Valor
Programación	TrikdisConfig (Windows) con cable USB Mini-B o a distancia; comandos SMS
Entorno 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

Todos los ajustes del G16T se hacen con el programa **TrikdisConfig**, que funciona en Windows, por cable USB o a distancia. En este capítulo describimos el camino más corto: configuras el dispositivo sobre la mesa, antes del cableado, 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 hacia la central · destornillador plano de 2,5 mm · antena móvil con la ganancia adecuada (si en la instalación la cobertura es débil) · tarjeta nano-SIM activa con servicio de datos móviles · 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 G16T. Introduce un destornillador plano en la ranura lateral y suelta la tapa con cuidado. La figura siguiente muestra dónde está el enganche y los orificios para tornillos de la base.

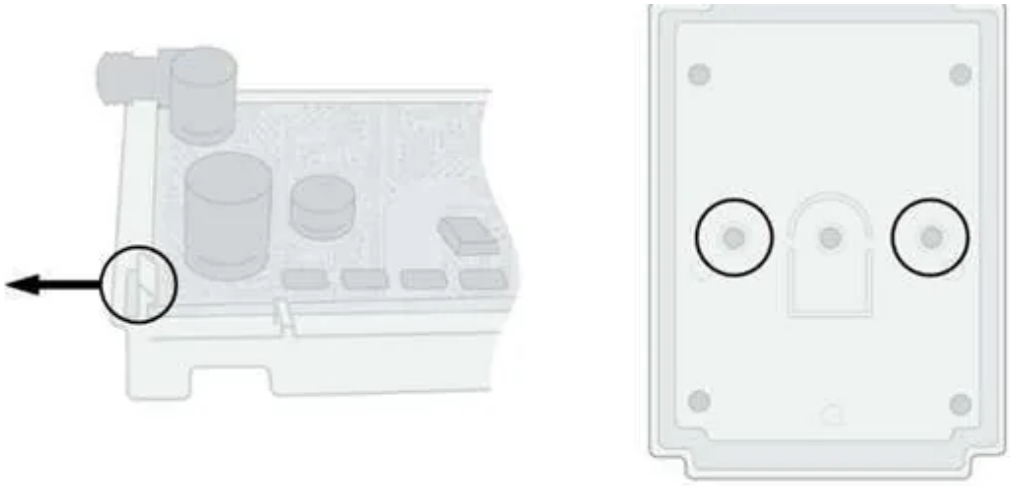


Figura 3. Cómo soltar la tapa frontal (izquierda) y los orificios de fijación de la base (derecha).

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

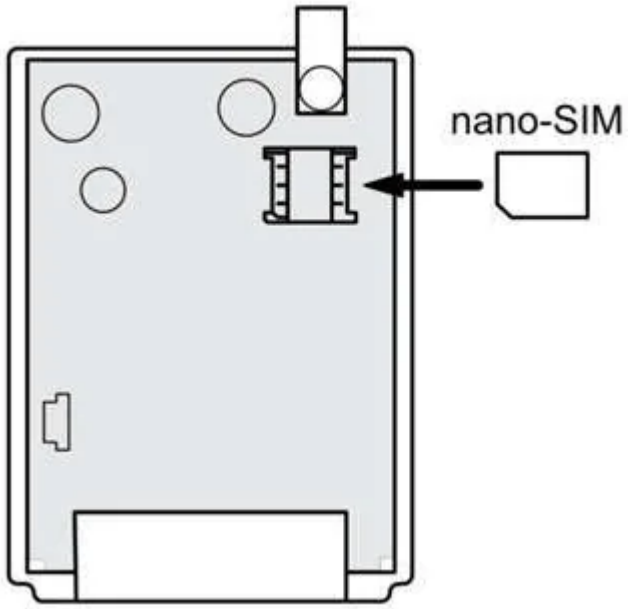


Figura 4. Posición de la tarjeta nano-SIM en la placa de circuito impreso.

4. Conecta el G16T al ordenador con un cable USB Mini-B. El USB da alimentación suficiente para la programación; no hace falta otra fuente de alimentación.



Figura 5. Conexión al ordenador con cable USB Mini-B.

Advertencia

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

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

2.2 Conexión con la aplicación Protegus 2

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

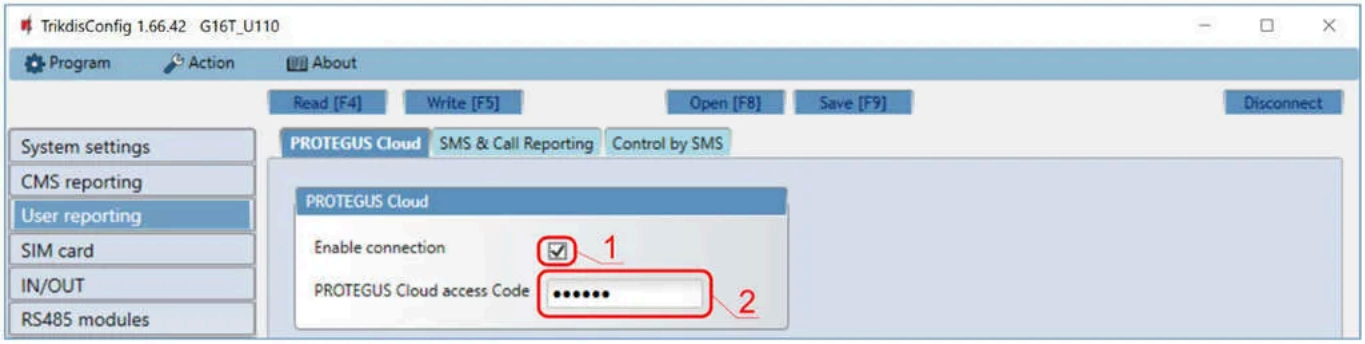


Figura 6. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- 1 **Enable connection** – márcalo: habilita la conexión con la nube de Protegus.
- 2 **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 modificar.**

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

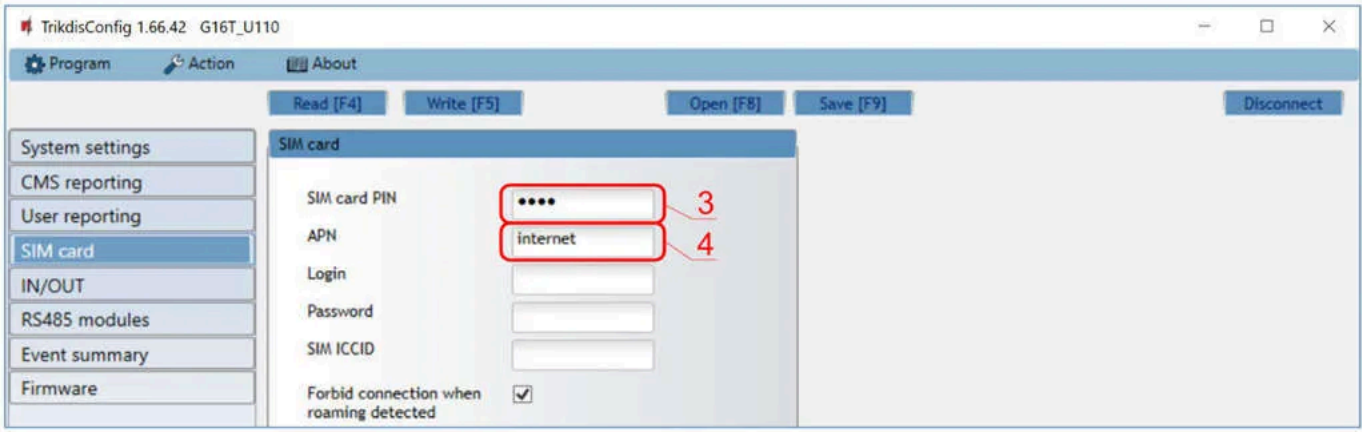


Figura 7. TrikdisConfig – página SIM card.

- 3 **SIM card PIN** – el código PIN de la tarjeta (si la petición del PIN está desactivada, puede quedarse el valor de fábrica).
- 4 **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 dispositivo no puede conectarse a internet. El valor exacto te lo da el operador de la tarjeta SIM. Las APN conocidas de los operadores húngaros y de otros países europeos las recogemos en un artículo aparte: Configuración del APN

– lista de operadores móviles europeos. Si el operador no te ha dado otro dato, prueba el APN `internet`: es genérico y funciona en la red de muchos operadores.

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

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

No te olvides de activar y configurar el marcador de línea telefónica de la central de alarma; de lo contrario, la central no envía eventos. La configuración de la central se describe en el capítulo 4.

2.3 Conexión con la CRA

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

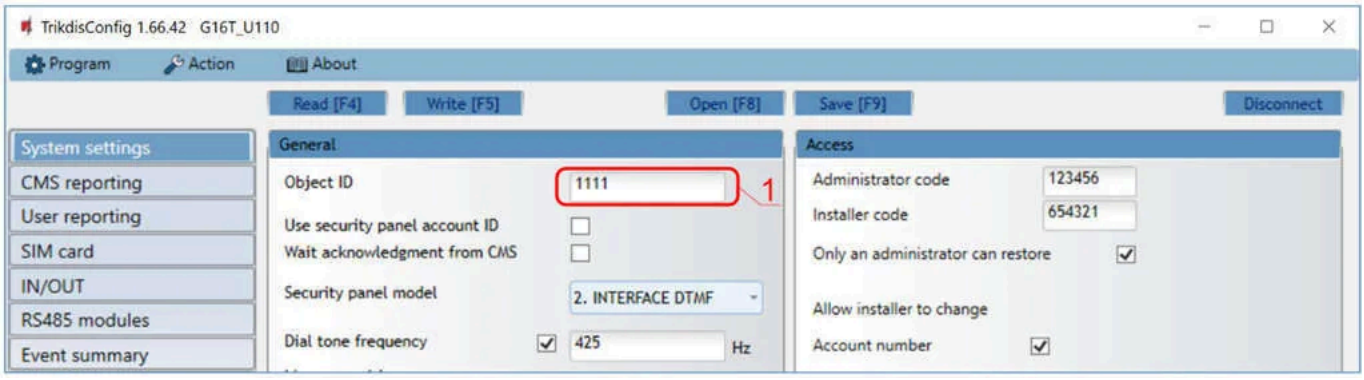


Figura 8. TrikdisConfig – página System settings, grupo General.

- 1 **Object ID** – el identificador de abonado que te da la CRA (4 caracteres hexadecimales, 0–9, A–F). `FFFE` y `FFFF` no se pueden usar.

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

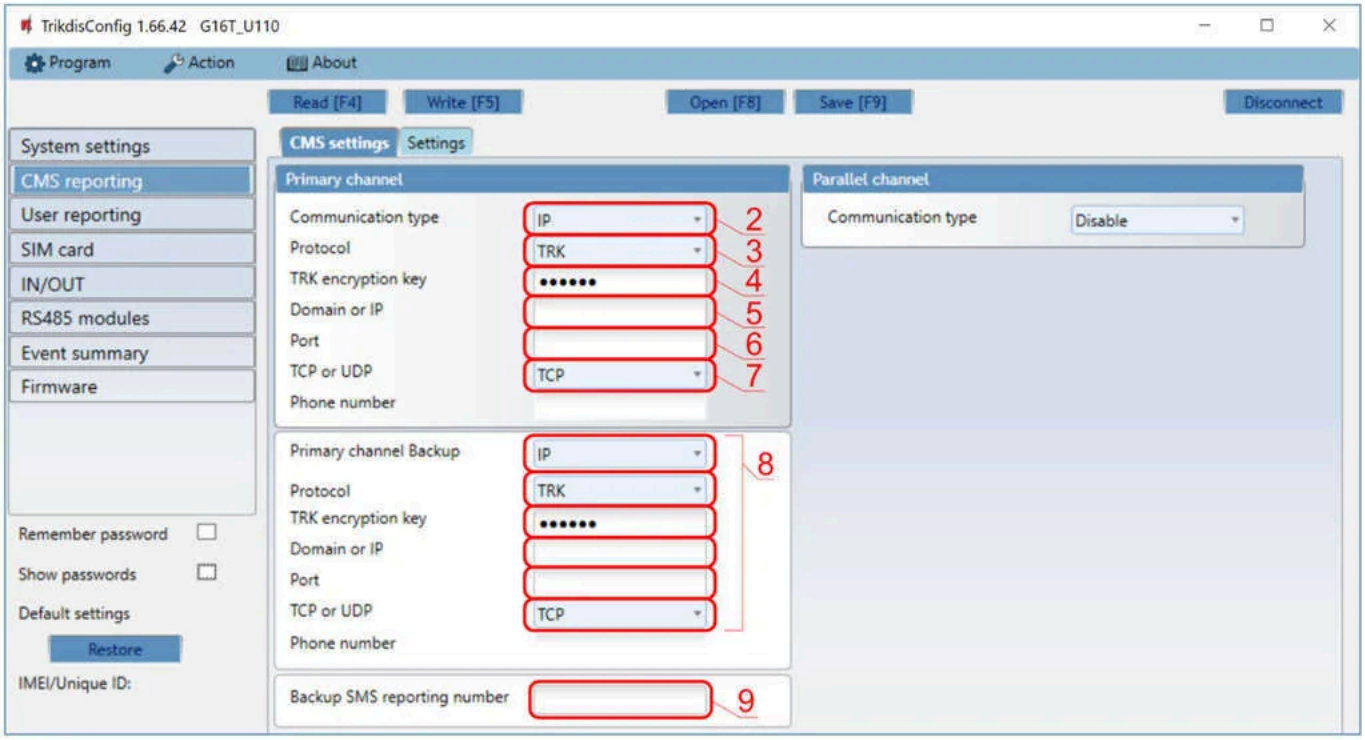


Figura 9. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 2 **Communication type** – elige la conexión **IP** (el SMS no se recomienda como canal principal).
- 3 **Protocol** – **TRK** para un receptor de Trikdis, **DC-09_2007** o **DC-09_2012** para un receptor universal, **TL150** para un receptor SUR-GARD.
- 4 **TRK encryption key** – la clave de cifrado de 6 dígitos configurada en el receptor.
- 5 **Domain or IP** – el nombre de dominio o la dirección IP del receptor.
- 6 **Port** – el número de puerto del receptor.
- 7 **TCP or UDP** – el protocolo de transmisión; se ajusta a la configuración del receptor.
- 8 **Primary channel Backup** – canal de respaldo para el fallo del canal principal; rellénalo igual; se recomienda configurarlo.
- 9 **Backup SMS reporting number** – si hay un receptor SMS de Trikdis, escribe aquí su número de teléfono: el dispositivo envía un SMS a este número 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 2.2.

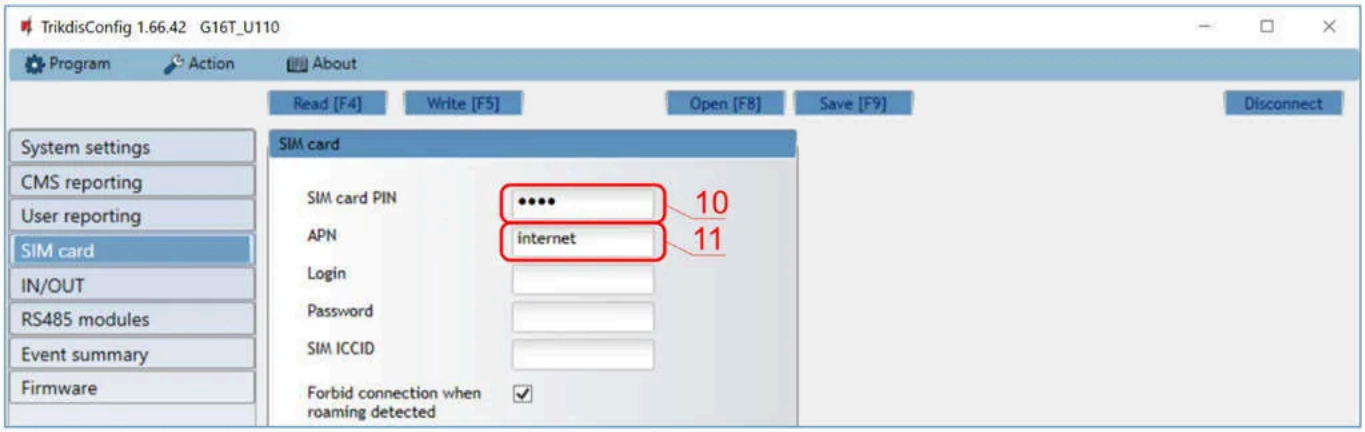


Figura 10. TrikdisConfig – página SIM card.

- 10 **SIM card PIN** – el código PIN de la tarjeta.
- 11 **APN** – el punto de acceso del operador (ver el apartado 2.2).

La **transmisión por SMS** a la CRA solo funciona con un receptor de 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**, en la pestaña **Settings** introduce también el número de abonado, de línea y de receptor DC-09.

Al terminar los ajustes, pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB. El dispositivo ya está listo para el cableado. También en este caso hay que activar y configurar el marcador de línea telefónica de la central de alarma; de lo contrario, la central no envía eventos (capítulo 4).

3. Instalación y conexionado

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 has hecho ya durante la puesta en marcha.
3. Saca la placa de circuito impreso de la base: abre el enganche de la esquina (ver la figura del apartado 2.1).
4. Fija la base con tornillos en el lugar elegido.
5. Vuelve a colocar la placa de circuito impreso en la base y vuelve a enchufar la regleta de bornes.
6. Enrosca la antena GSM.
7. Vuelve a colocar la tapa frontal.

La tarjeta SIM debe estar activa y, para el uso por IP, debe funcionar en ella la conexión de datos móviles. Si no quieres que TrikdisConfig pida el código PIN, desactiva la petición del PIN en la tarjeta con 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 cableado sea corto.
- **Dentro de una caja metálica** la señal móvil se debilita mucho. Si el comunicador va dentro de la caja metálica de la central, saca la antena fuera de la caja o usa una antena con cable más largo.
- Antes de la fijación definitiva, **comprueba el nivel de señal**: el número de destellos amarillos del LED NETWORK debe ser al menos 5 en 2G y al menos 3 en 4G (ver el apartado 1.6). Si es menor, busca un lugar mejor o cambia a una antena más sensible que se pueda colocar más lejos.
- Mantén la antena y el comunicador alejados del transformador de la central y de los cables de red eléctrica.



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

3.3 Conexión a la central de alarma

El G16T se conecta a la salida de línea telefónica (TIP/RING) de la central, y recibe la alimentación de la salida de alimentación auxiliar de 12 V (AUX) de la central.

Conexión recomendada y normal: DC+, DC–, TIP y RING. En este caso el comunicador no detecta si se corta el cable.

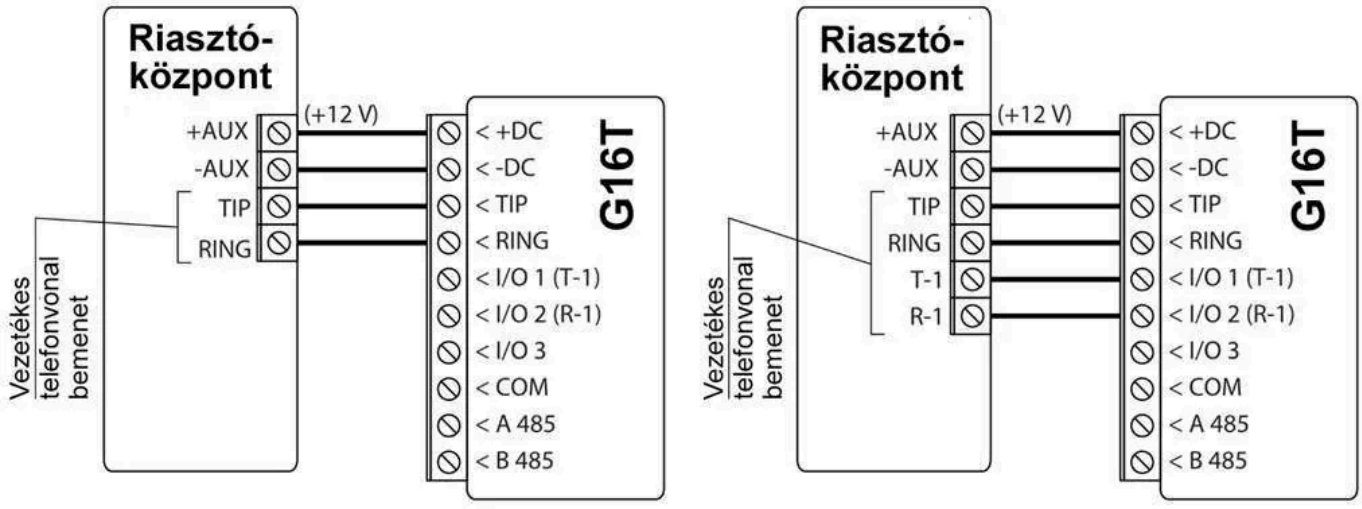


Figura 11. Conexión a la salida de línea telefónica de la central: a la izquierda la conexión normal, a la derecha la conexión con supervisión de línea.

Durante el envío, el G16T puede consumir hasta 500 mA. Comprueba que la salida AUX de la central lo soporta junto con los demás equipos conectados a ella. Como la alimentación la da la central, durante un corte de corriente la batería de la central alimenta también al comunicador.

3.3.1 Si está justificado: supervisión de línea

Solo hace falta si se necesita supervisión de línea: así el comunicador avisa si se corta el enlace entre él y la central de alarma.

1. Además de la conexión normal, conecta también estos dos hilos: el borne **T-1** de la central al borne **I/O 1 (T-1)** del comunicador, y el borne **R-1** de la central al borne **I/O 2 (R-1)**.
2. En la página **System settings** de TrikdisConfig, activa la opción **Line supervision**.
3. Los ajustes necesarios en la central de alarma, compruébalos en el manual de instalación de la central.

En este caso, I/O 1 e I/O 2 no se pueden usar para otra cosa.

3.4 Conexión de la zona de interruptor de llave

Si quieres armar y desarmar la central a distancia, desde la aplicación Protegus 2, configura uno de los bornes I/O del comunicador **como salida** y conéctalo a una **zona de interruptor 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 G16T tiene tres bornes I/O, se pueden controlar hasta tres particiones, cada una con su propia salida. El borne usado para el interruptor de llave ponlo en la función **OUT** en la página **IN/OUT** de TrikdisConfig (apartado 6.6). El hardware 3 tiene una salida programable (OUT), que puede controlar una partición; allí, el campo **Output OUT1 mode** de la página **System settings** debe estar en **Remote control** (es el ajuste de fábrica).

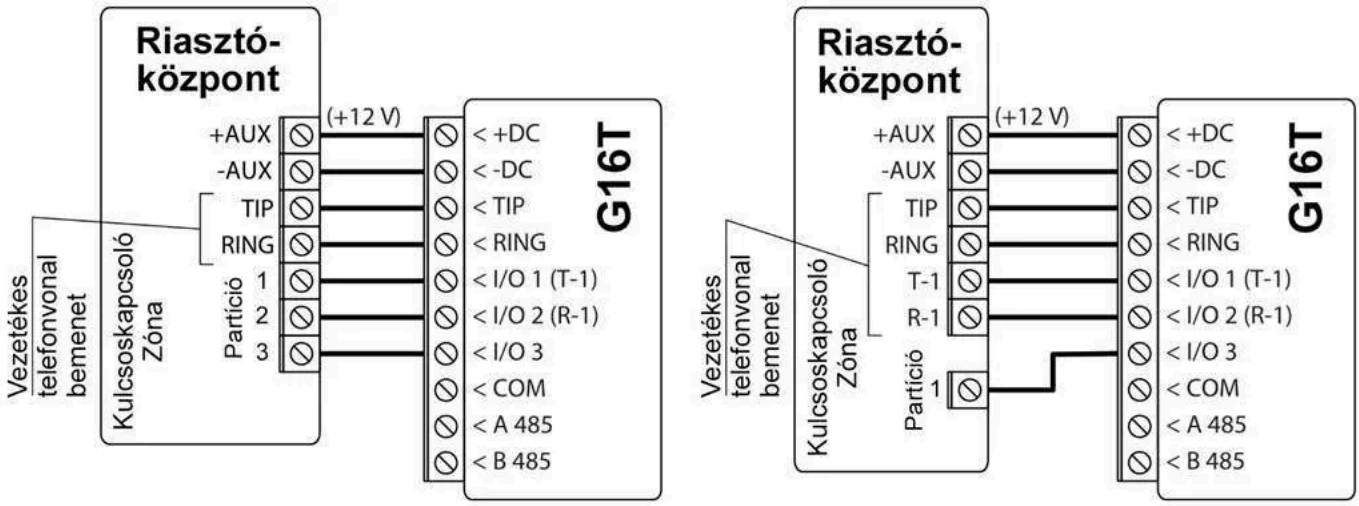


Figura 12. Armado y desarmado con una zona de interruptor de llave: a la izquierda la conexión normal, a la derecha la conexión con supervisión de línea (en este caso queda I/O 3 para el interruptor de llave).

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

3.5 Conexión de entradas

Los bornes I/O del comunicador, como entradas, también sirven para recibir otros detectores (p. ej. interruptor de tamper, pulsador de pánico, termostato), con independencia de la central de alarma. La entrada se conecta entre el I/O elegido 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	–
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 NC, NO, EOL y DEOL con resistencia de fin de línea de 2,2 kΩ; en los tipos DEOL, con circuito de tamper.

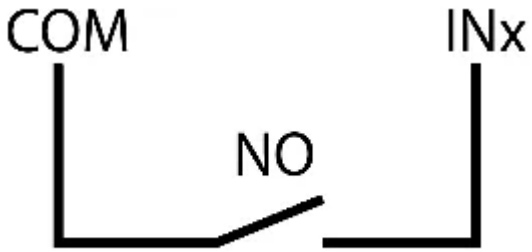


Figura 13. NO – circuito normalmente abierto: cerrado – alarma, abierto – reposo.

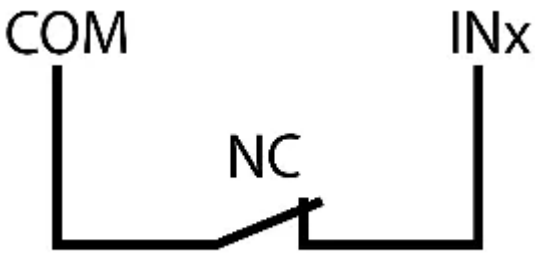


Figura 14. NC – circuito normalmente cerrado: abierto – alarma, cerrado – reposo.

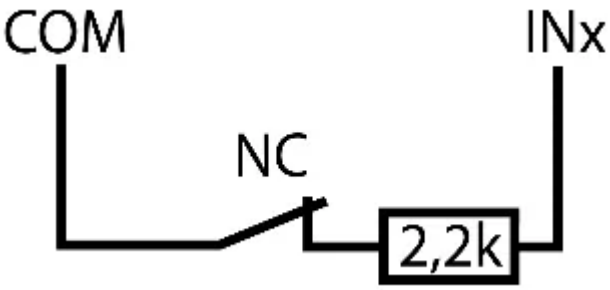


Figura 15. NC/EOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

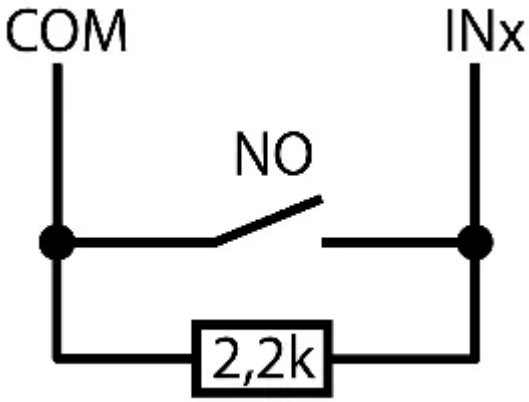


Figura 16. NO/EOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

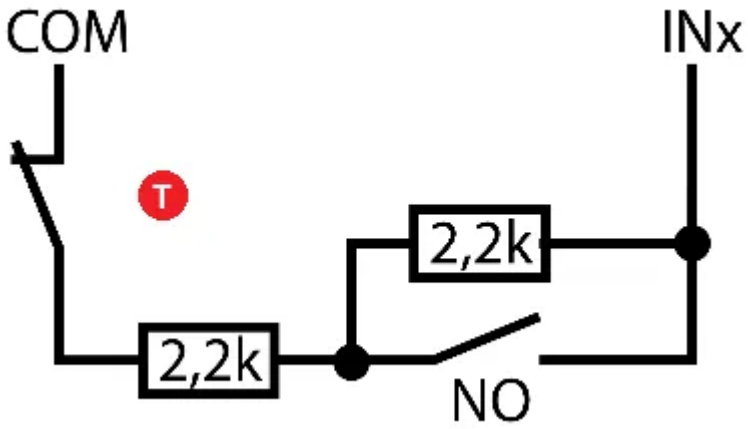


Figura 17. NO/DEOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ y detección de tamper: cortocircuito o corte – tamper, 2,2 kΩ – alarma, 3,3–5,5 kΩ – reposo.

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

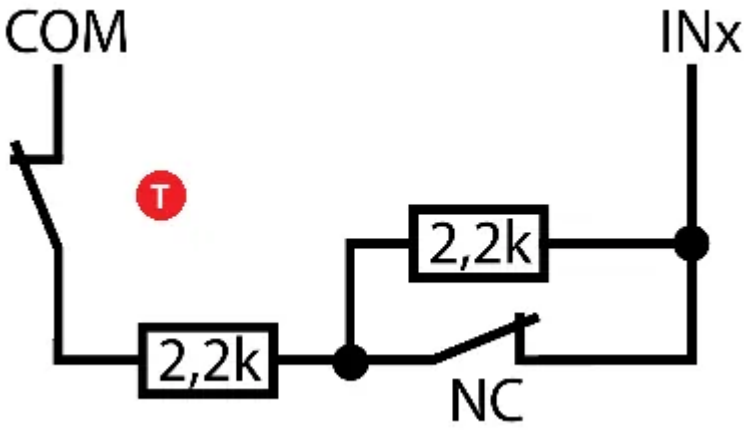


Figura 18. NC/DEOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ y detección de tamper: cortocircuito o corte – tamper, 2,2 kΩ – reposo, 3,3–5,5 kΩ – alarma.

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

3.6 Conexión de una salida con relé

Como salidas, los bornes I/O son salidas de colector abierto (OC): en estado activo llevan la carga conectada al negativo, con un máximo de 0,15 A, hasta 30 V DC. Un consumidor mayor o un equipo a tensión de red conéctalo **a través de un relé**: un extremo de la bobina del relé va a +DC y el otro al borne I/O.

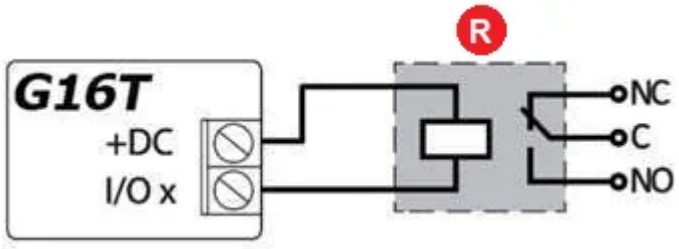


Figura 19. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne I/O x, y los contactos (NC, C, NO) accionan el consumidor.

- R relé («Relay»)

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

3.7 Conexión del expansor iO-8

Si 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 I/O de doble función. Al mismo bus se pueden conectar también los demás expansores cableados o inalámbricos de la serie iO de Trikdis, por ejemplo si quieres conectar sondas de temperatura: el expansor **iO** tiene 1 entrada, 1 salida de relé y un bus 1-Wire para sondas de temperatura (su configuración está en el apartado 6.7). Une los bornes A 485 y B 485 con los bornes A y B del módulo, y toma la alimentación del módulo de los 12 V de la central. El módulo hay que darlo de alta en la página **RS485 modules** de TrikdisConfig (apartado 6.7).

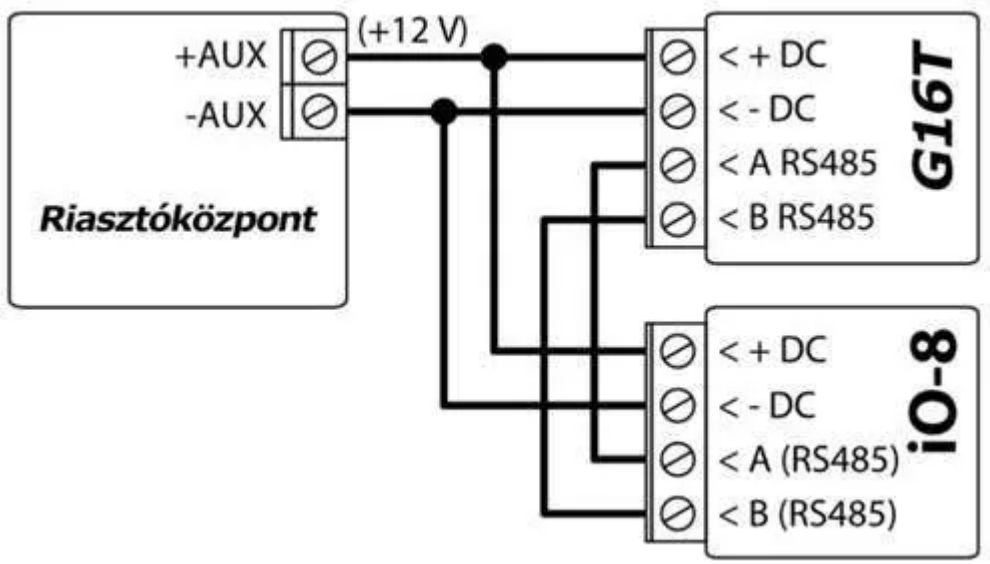


Figura 20. Conexión del expansor iO-8 al bus RS485 del G16T; la alimentación, de la salida AUX de la central de alarma.

El G16T con módem 2G (G16T_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 funciona, el G16T se comunica a través de ella (los mensajes para la CRA y para Protegus van por el router WiFi o por internet por cable; la conexión de datos móviles no se usa en ese caso); si se corta, pasa a la conexión de datos móviles y, cuando la conexión se restablece, vuelve al módulo. Para que el módulo funcione, **el G16T debe tener una tarjeta SIM**.

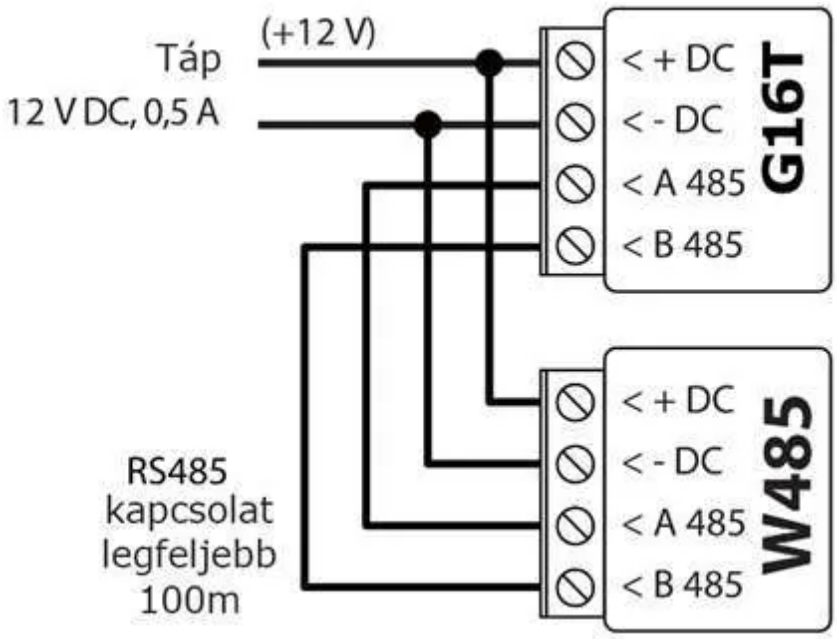


Figura 21. Conexión del módulo WiFi W485 al G16T por el bus RS485. Los dos equipos funcionan con una alimentación común de 12 V DC (de al menos 0,5 A) (la entrada de alimentación del módulo es de 9–28 V DC); el cable RS485 puede tener como máximo 100 m.

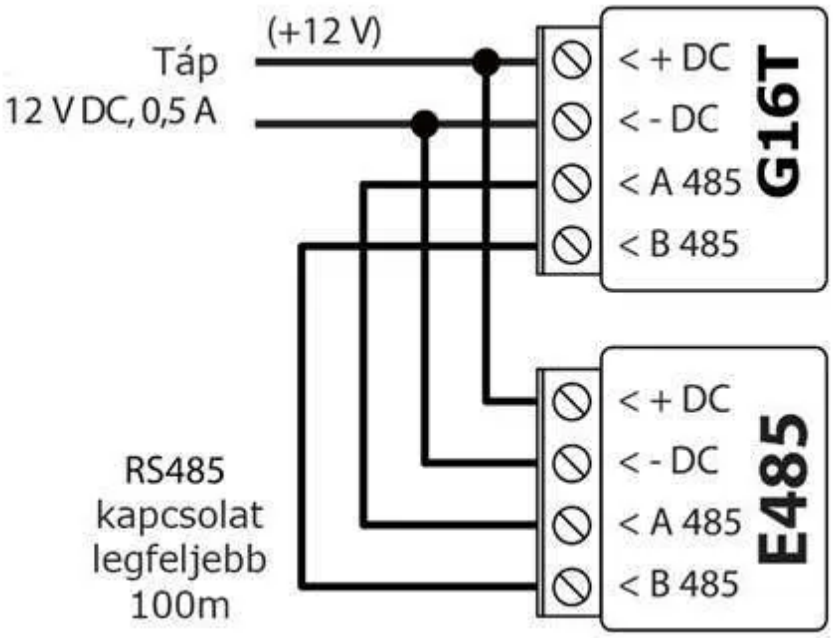


Figura 22. Conexión del módulo Ethernet E485 al G16T por el bus RS485. Los dos equipos funcionan con una alimentación común de 12 V DC (de al menos 0,5 A) (la entrada de alimentación del módulo es de 9–28 V DC); el cable RS485 puede tener como máximo 100 m.

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.

Los ajustes de red de los módulos se hacen 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.

Tras el cableado, al encender la central de alarma arranca también el comunicador. En la tapa frontal debes ver esto:

- **POWER** verde fijo – la alimentación es correcta;
- **NETWORK** verde fijo y parpadeando en amarillo – conectado a la red; el número de destellos es el nivel de señal (en 2G, 5, y en 4G, 3, es bueno); si cuentas menos, la señal es débil: busca otro lugar para el comunicador o usa una antena más sensible (apartado 3.2);
- **TROUBLE** apagado.

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

4. Programación de la central de alarma

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

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

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

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

4.1 Programación del marcador de la Honeywell Vista

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

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

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

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

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

4.2 Centrales de otros fabricantes

En el manual de instalación de cualquier central, busca los mismos cuatro ajustes: la habilitación del comunicador de línea telefónica, el número de teléfono del receptor, el modo de marcación (DTMF) y el formato de comunicación (Contact ID). Si la central espera un tono de llamada (dial tone) antes de marcar, el G16T lo proporciona; si aun así no empieza la llamada, desactiva en la central la detección del tono de llamada («marcar sin tono de llamada» u opción similar).

Si la central indica un error al final de la llamada aunque el evento haya llegado, comprueba el ajuste **Wait acknowledgment from CMS** en la página **System settings** de TrikdisConfig: si está activado, el comunicador solo cierra la llamada después de la confirmación del receptor de la CRA (kiss-off). En un sistema sin CRA, solo con Protegus 2, déjalo desactivado (es el estado de fábrica), porque no hay ningún receptor que confirme.

5. Control a distancia con la aplicación Protegus 2

Con la aplicación móvil y web Protegus 2, el usuario ve a distancia el estado del sistema, recibe avisos de los eventos, puede armar y desarmar, y puede accionar las salidas del comunicador.

5.1 Cómo añadir el dispositivo

Antes de añadir el dispositivo, comprueba:

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

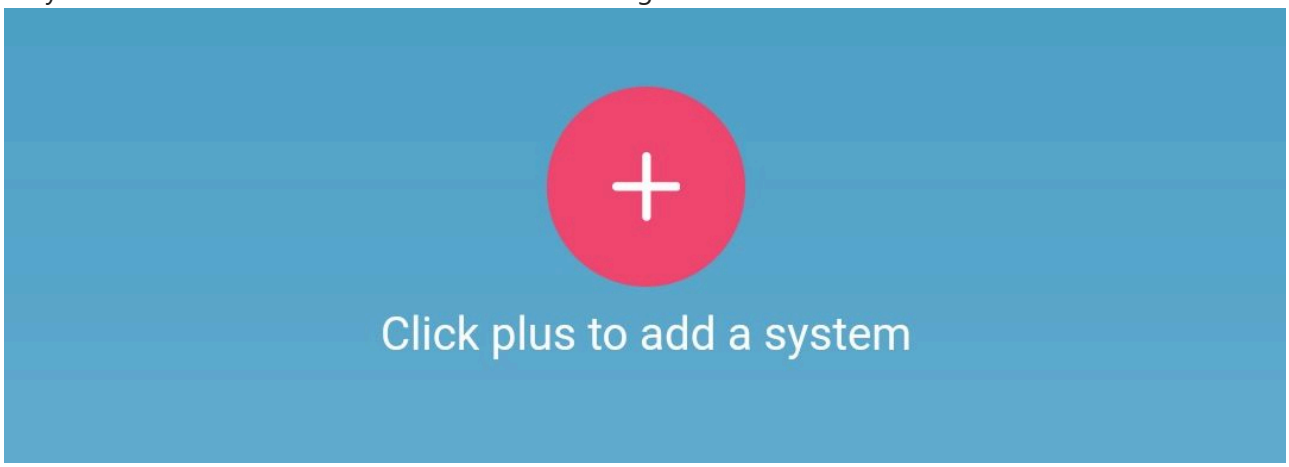
El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del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



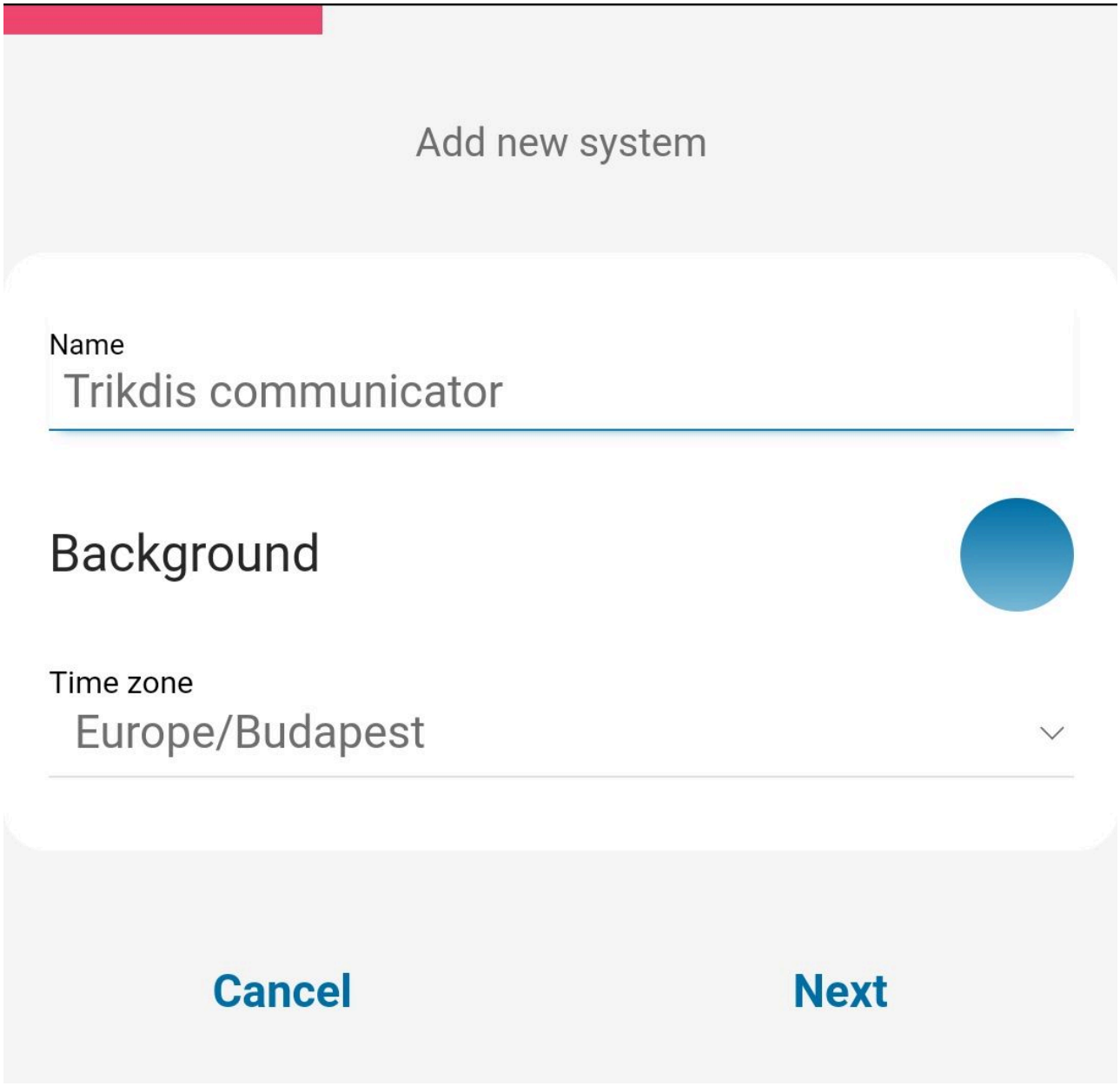
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



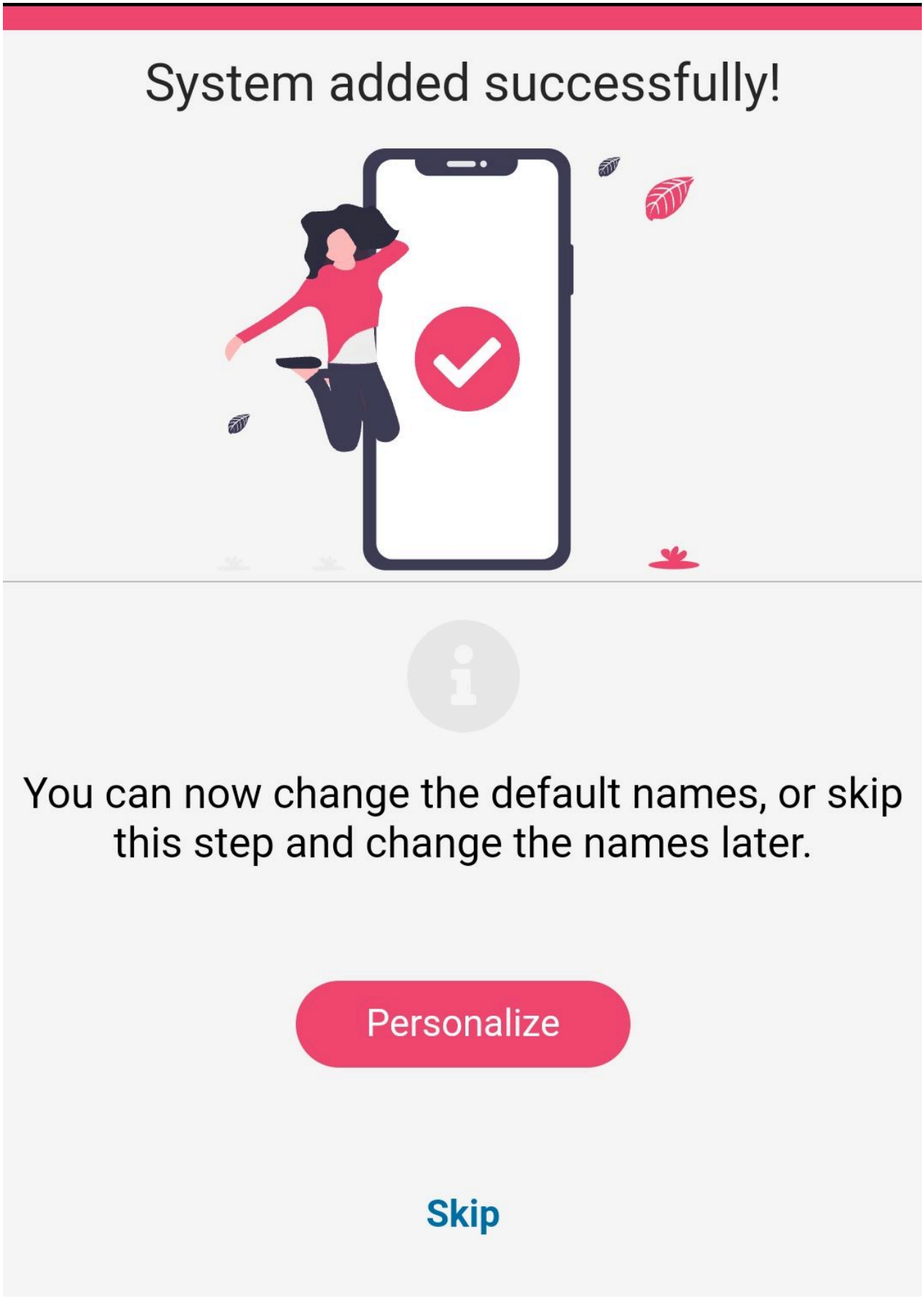
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



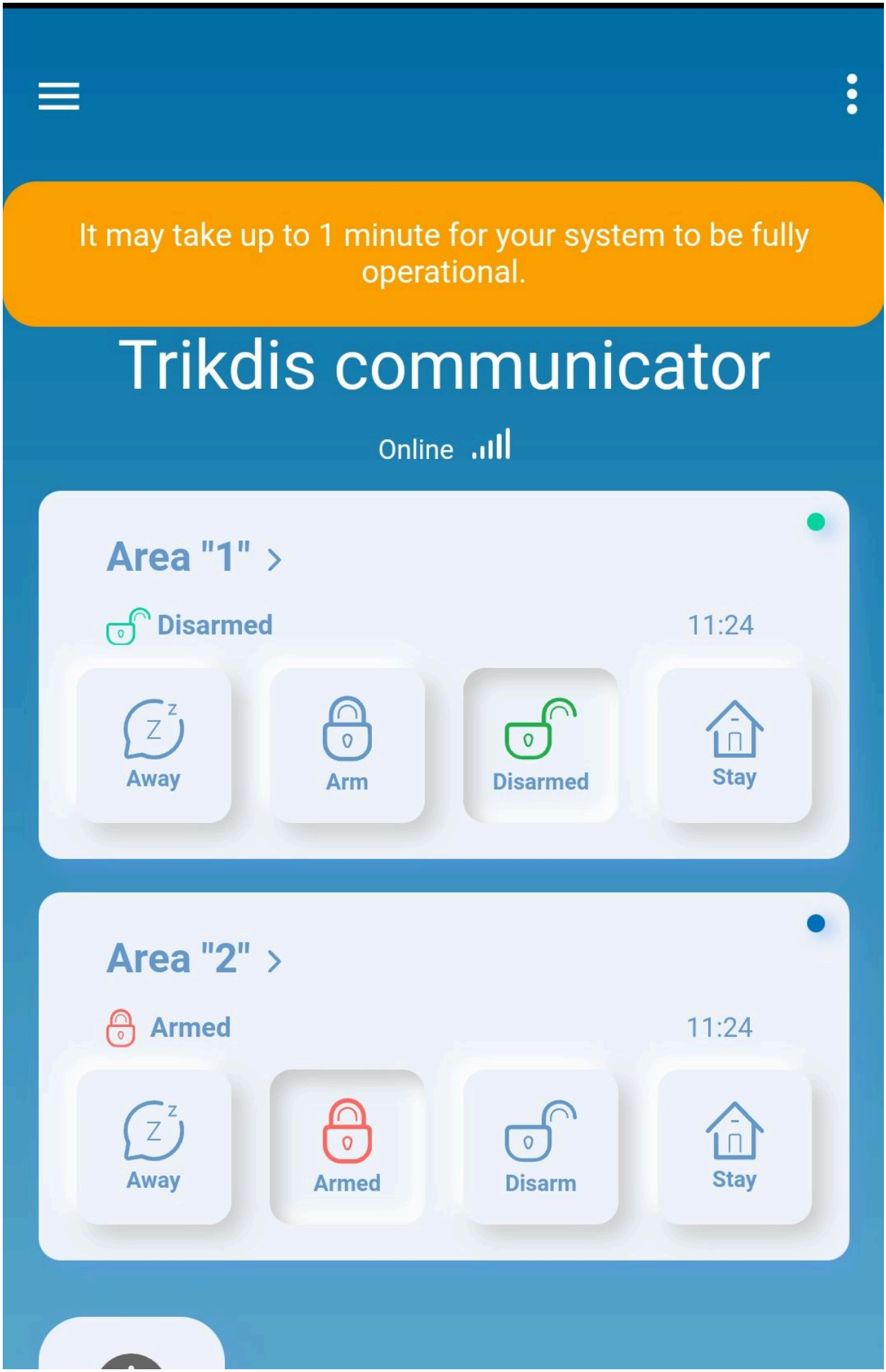
6. Add meg a rendszer nevét és válassz idozónát



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

5.2 Armado y desarmado con una salida

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

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

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

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

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

5.3 Armado y desarmado desde la aplicación

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

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

5.4 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.

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`
`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`

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.

En el G16T, el comando `CONNECT` tiene un dato más: `CP=1` desactiva y `CP=2` activa la interfaz de línea telefónica del comunicador. Ejemplo: `123456 CONNECT CP=2`.

6. TrikdisConfig – los ajustes en detalle

En la parte izquierda de la ventana de TrikdisConfig se ve la lista de páginas (System settings, CMS reporting, User reporting, SIM card, IN/OUT, RS485 modules, Event summary, Firmware); arriba, la barra de botones (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), y abajo, la barra de estado. Este capítulo recorre página por página los ajustes del G16T.

6.1 La barra de estado

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

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

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



Figura 23. La barra de estado de TrikdisConfig con un G16T leído: identificador, estado, modelo, número de serie, versiones, modo de conexión y nivel de acceso.

Tras **Read [F4]**, el programa lee y muestra los valores configurados en el dispositivo; haz los ajustes necesarios según las descripciones de las páginas que siguen.

6.2 System settings

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

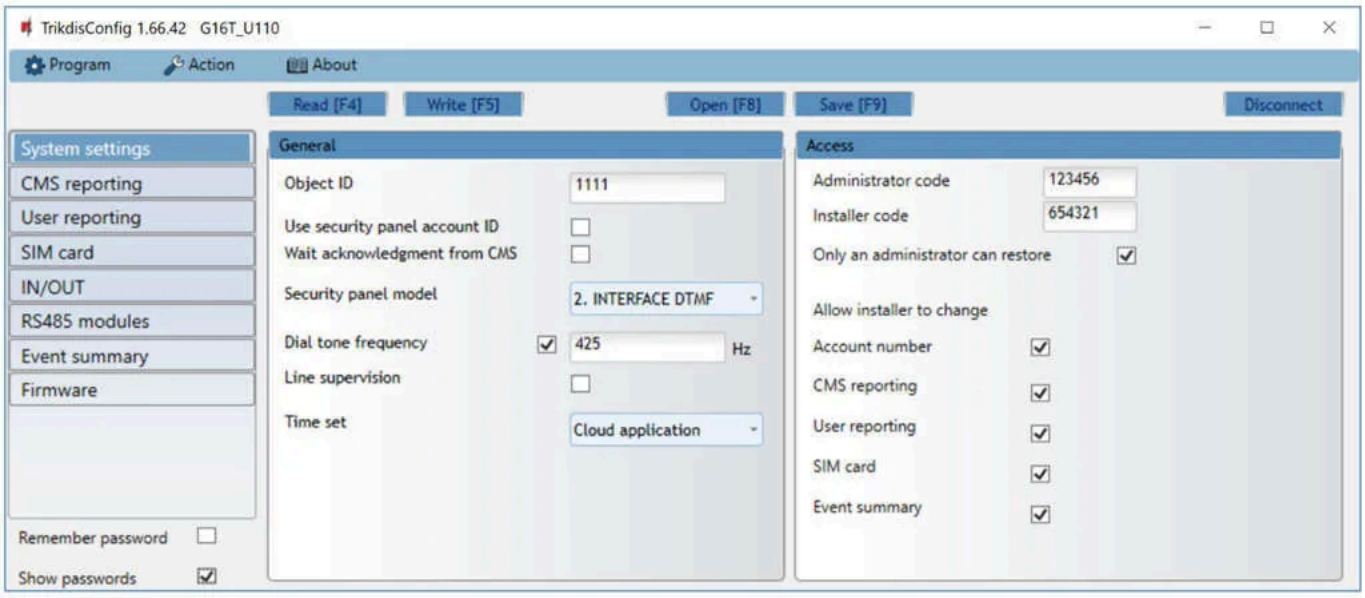


Figura 24. TrikdisConfig – página System settings: grupos General y Access.

- **Object ID** – el identificador de abonado que te da la CRA (4 caracteres hexadecimales: 0–9, A–F; `FFFE` y `FFFF` no se pueden usar). Es obligatorio si el dispositivo también transmite a una CRA.
- **Use security panel account ID** – si está marcado, el comunicador no usa su propio Object ID, sino el identificador que envía la central en el mensaje Contact ID. Es útil si varias particiones transmiten con identificadores distintos.
- **Wait acknowledgment from CMS** – si está marcado, después de cada evento el comunicador espera la confirmación del receptor y solo después envía a la central la señal de cierre (kiss-off). Si no hay confirmación, la central vuelve a enviar el evento. En un sistema sin CRA, solo con Protegus 2, déjalo desactivado (estado de fábrica).
- **Security panel model** – el tipo de interfaz de línea telefónica (con él habilitas o deshabilitas la interfaz de línea telefónica DTMF del comunicador); por defecto **2. INTERFACE DTMF**.
- **Dial tone frequency** – la frecuencia del tono de llamada que el G16T da hacia la central (por defecto 425 Hz, el tono de llamada habitual en España y en la mayoría de los países europeos).
- **Line supervision** – supervisión del cable entre la central y el comunicador; requiere conectar también los hilos T-1 y R-1 (apartado 3.3.1).
- El tipo de las entradas y la función de las salidas, en el hardware 4, se configuran en la página **IN/OUT** (apartado 6.6). En el hardware 3, estos dos campos están aquí: **Input IN1-IN2 type** – el tipo de entrada, de la lista (NO, NC, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL); **Output OUT1 mode** – el modo de funcionamiento de la salida, de la lista.
- **Time set** – la fuente del reloj del dispositivo (por defecto **Cloud application**, la nube de Protegus).

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 corta. La comunicación está cifrada y protegida con contraseña; para recibirla y reenviar los eventos al software de la CRA hace falta un receptor de Trikdis (receptor de software IPcom –Windows o Linux–, RL14, RM14; para recibir SMS, receptor IP/SMS RL14, receptor multicanal RM14 o receptor SMS GM14) o un receptor universal que conozca el protocolo DC-09 / TL150. El SMS es especialmente útil como canal de respaldo, porque funciona sin internet móvil; como canal principal no lo recomendamos.

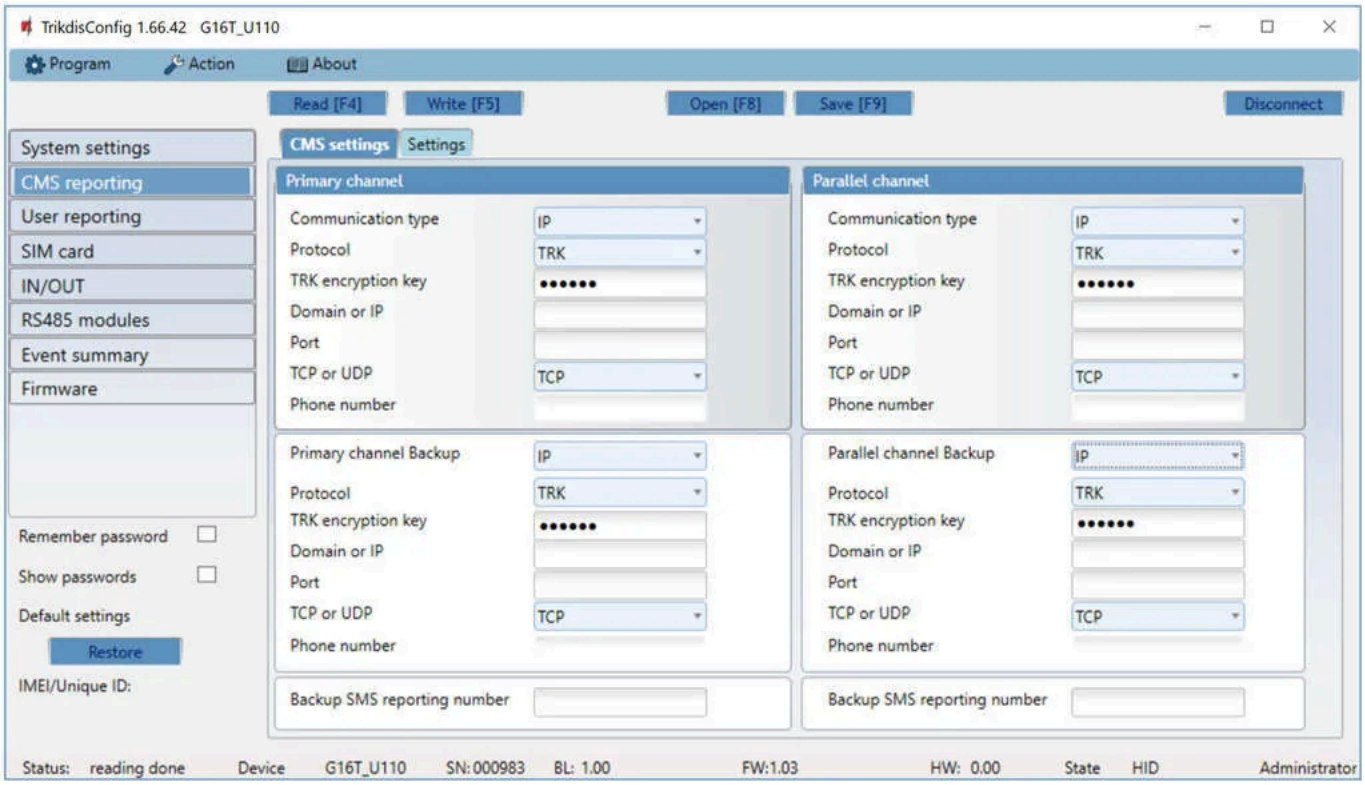


Figura 25. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal, de respaldo y paralelo.

Primary channel – canal principal

- **Communication type** – IP o SMS.
- **Protocol** – TRK (receptores de 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 prefijo internacional (p. ej. `34xxxxxxxxx` para un número español).

Primary channel Backup – canal de respaldo. Asume la comunicación si el canal principal no funciona; sus ajustes son los mismos que los de arriba.

Parallel channel – canal paralelo. Junto al principal, envía a la vez a un segundo receptor (por ejemplo, a una CRA local y a otra 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 sin conexión IP. Solo está activo si el canal principal y el de respaldo están en modo IP. El dispositivo envía un SMS al receptor SMS de la CRA después del primer arranque, y también si la conexión TCP/IP o UDP/IP se corta tanto en el canal principal como en su respaldo. Introduce el número de teléfono del receptor SMS de Trikdis con prefijo internacional (p. ej. `34xxxxxxxxx` para un número español).

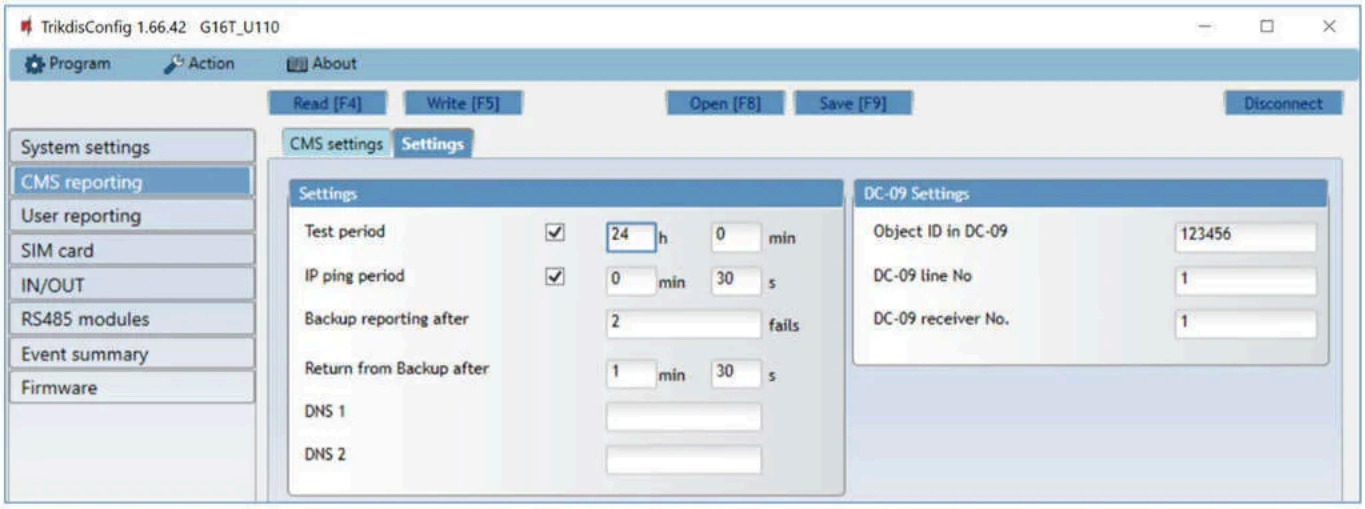


Figura 26. TrikdisConfig – CMS reporting, pestaña Settings: informe de prueba, PING, temporizaciones del canal de respaldo, DNS y datos DC-09.

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.

En la parte inferior de la pestaña: **DNS 1, DNS 2** – servidores de nombres (DNS, Domain Name System: da la dirección IP que corresponde a un nombre de dominio); hacen falta si has indicado el receptor con un nombre de dominio y no con una dirección IP. Por defecto, el DNS público de Google.

6.4 User reporting

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

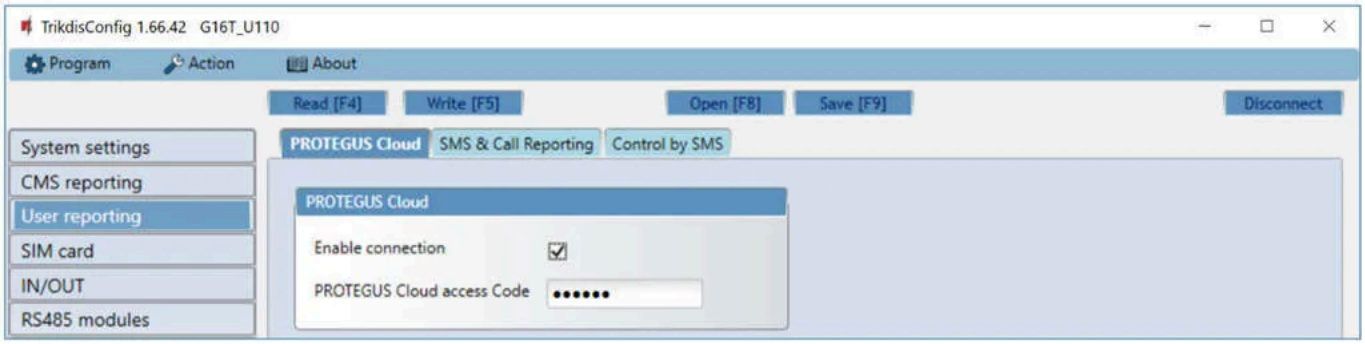


Figura 27. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- **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 (de fábrica `123456`). Solo se puede configurar antes de crear el sistema en Protegus 2; después ya no se puede modificar.

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.

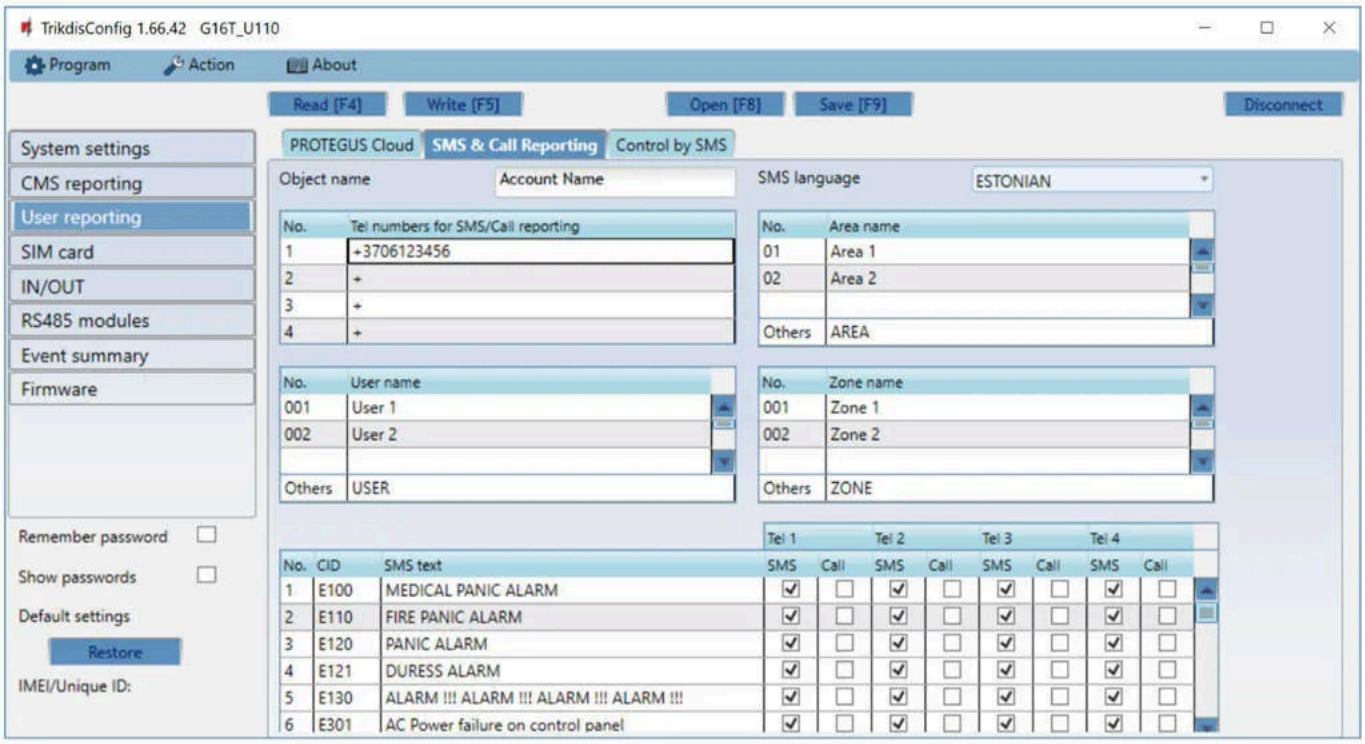


Figura 28. TrikdisConfig – User reporting, pestaña SMS & Call Reporting.

- **Object name** – el nombre del sistema; figura en todos los SMS.
- **SMS language** – el idioma de los SMS (para los caracteres acentuados del idioma).
- **Tel numbers for SMS/Call reporting** – hasta 4 números de teléfono con prefijo internacional (p. ej. para un número español `+34…`, `0034…` o `34…`).
- **Area name, User name, Zone name** – los nombres de las particiones, los usuarios y las zonas; el dispositivo los usa en el texto de los SMS. En la tabla correspondiente escribe el número de la partición, del usuario o de la zona y, a su lado, su nombre.
- **CID event table** – para cada evento se puede configurar qué número recibe SMS o llamada; también se pueden modificar 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 5.4).

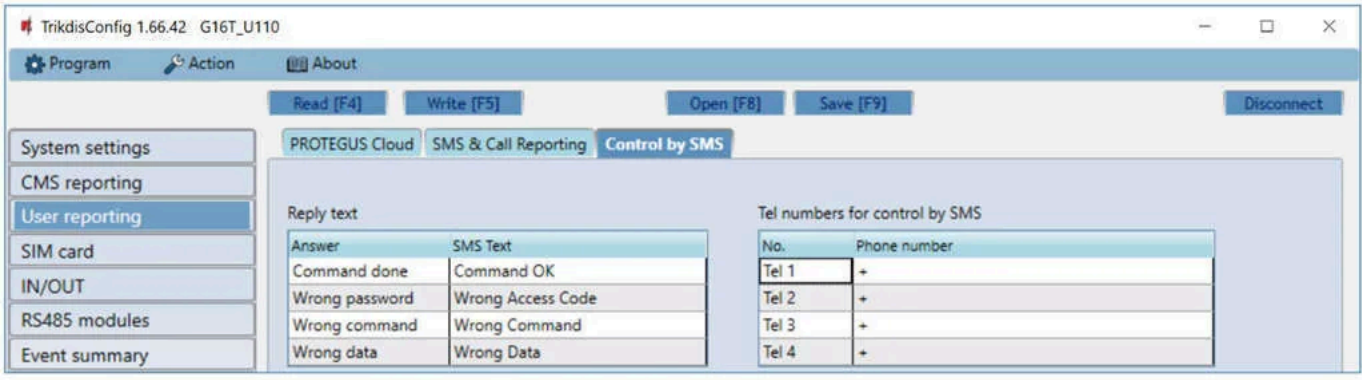


Figura 29. TrikdisConfig – User reporting, pestaña Control by SMS.

- **Reply text** – el texto de los cuatro mensajes de respuesta a un comando SMS: comando correcto (Command done), contraseña incorrecta (Wrong password), comando incorrecto (Wrong command), dato incorrecto (Wrong data). Los textos de respuesta se pueden editar.

- **Tel numbers for control by SMS** – hasta 4 números; el dispositivo solo acepta comandos desde estos números. Si está vacío, acepta de cualquier número un comando con la contraseña correcta. 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 dispositivo no se conecta a la red de datos.



Figura 30. TrikdisConfig – página SIM card.

- **SIM card PIN** – el código PIN de la tarjeta. La petición del PIN la puedes desactivar poniendo la tarjeta en un teléfono móvil y deshabilitándola allí. Si la petición del PIN está desactivada, el campo puede quedarse con el valor de fábrica.
- **APN** – el punto de acceso del operador; las APN conocidas de los operadores figuran en el artículo de APN (para una tarjeta IoT / M2M, el operador da un APN aparte, ver el apartado 2.2). El APN es necesario para la conexión a internet del dispositivo; si no tienes otro dato, prueba el APN `internet`, que es genérico y funciona en la red de muchos operadores.
- **Login, Password** – nombre de usuario y contraseña del APN, si el operador los pide.
- **Forbid connection when roaming detected** – útil cerca de una frontera: impide que el dispositivo se conecte a la red del país vecino.

Antes de usarlo, 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 I/O de doble función del comunicador: **Disabled** (sin uso), **IN** (entrada) u **OUT** (salida). Para una entrada también hay que indicar el tipo (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). En el hardware 3, estos ajustes están en la página **System settings** (apartado 6.2).

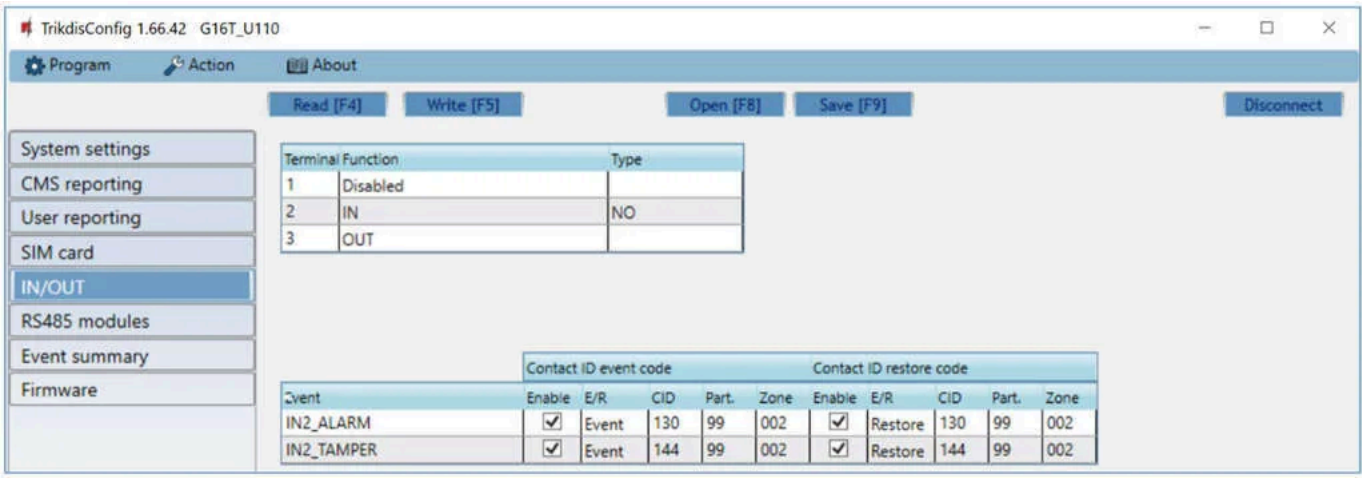


Figura 31. TrikdisConfig – página IN/OUT: función de los bornes I/O y eventos de las entradas.

Cuando se activa el detector conectado a la entrada, el comunicador envía un evento propio (**INx_ALARM**, Contact ID 130), y cuando se activa el circuito de tamper, un evento de tamper (**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.

6.7 RS485 modules

Con los expansores de la serie iO se pueden añadir al comunicador más entradas, salidas y un bus serie para sondas de temperatura. Los expansores iO-8 (y los demás expansores de la serie iO) y los módulos W485 / E485 conectados al bus RS485 hay que darlos de alta en la pestaña **Modules list**.

En el G16T con módem 2G (G16T_G410) esta página no se puede usar: la versión 2G no tiene bus RS485.

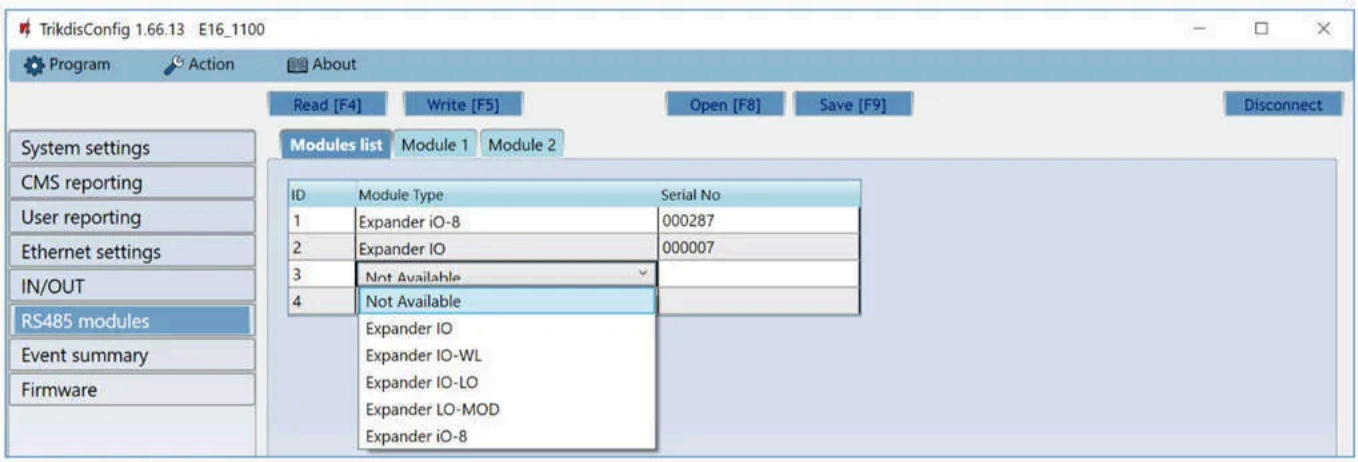


Figura 32. TrikdisConfig – RS485 modules, pestaña Modules list.

- **Module Type** – el tipo del módulo conectado, de la lista (iO-8 y otros expansores de la serie iO, 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 dispositivo (**Read [F4]**) y en la página RS485 modules aparece la pestaña propia del módulo, numerada.

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

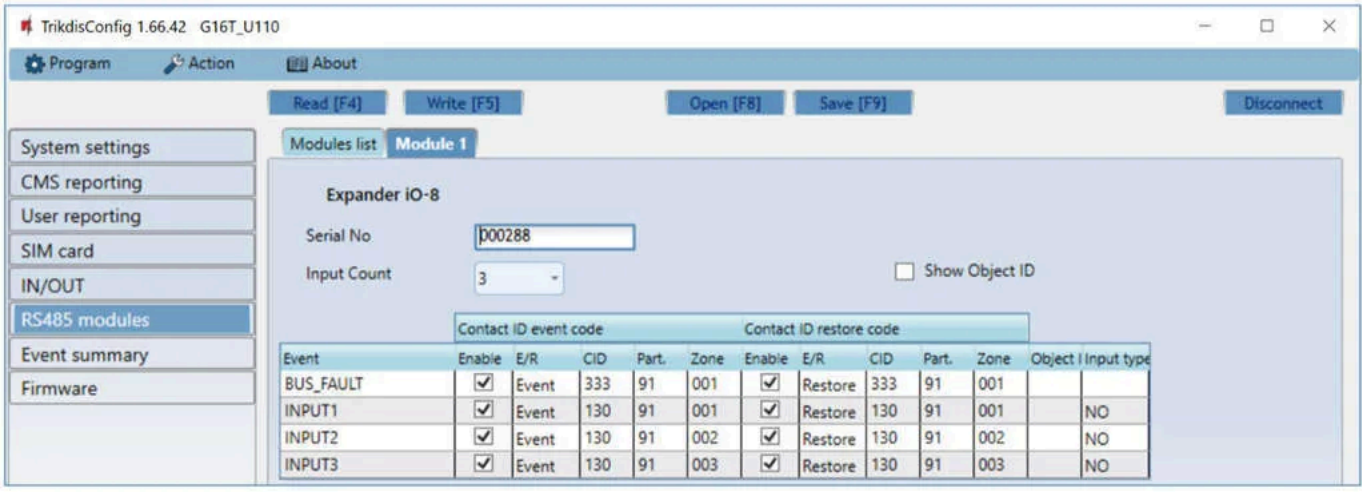


Figura 33. TrikdisConfig – RS485 modules, pestaña del módulo iO-8.

- **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 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 la entrada, el comunicador envía un evento con el código configurado al receptor de la CRA y a Protegus 2. 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 cuando se activan las entradas del expansor, añade el código de evento Contact ID asignado a la entrada también a la tabla de la pestaña **User reporting** → **SMS & Call Reporting**.

Expansor iO – 1 entrada, 1 salida de relé (contactos de relé) y un bus serie 1-Wire para sondas de temperatura. La salida de relé también se puede controlar según condiciones lógicas (SI … ENTONCES).

- **Input IN1 type** – el tipo de entrada (NO o NC).
- **Max °C (T1)** – si la temperatura es mayor, el dispositivo envía un evento; para ello hay que habilitar el evento en la tabla.
- **Min °C (T2)** – si la temperatura es menor, el dispositivo envía un evento; para ello hay que habilitar el evento en la tabla.
- En la tabla puedes asignar a la entrada un código Contact ID de evento y de restauración, igual que en el expansor iO-8; cuando se activa la entrada, el comunicador envía un evento con el código configurado al receptor de la CRA y a Protegus 2.

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

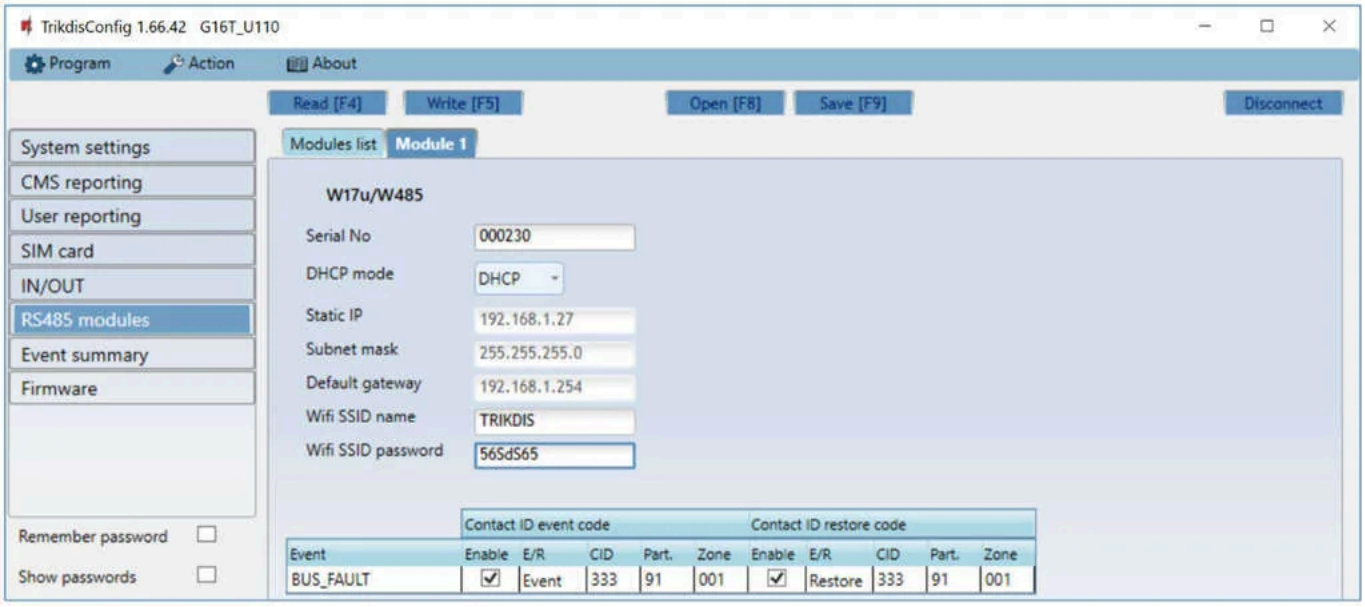


Figura 34. TrikdisConfig – RS485 modules, pestaña del módulo W485.

- **DHCP mode** – configuración de red automática o manual.
- **Static IP**, **Subnet mask**, **Default gateway** – en 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 (corte y restablecimiento de la conexión entre el módulo y el G16T); el evento lo reciben tanto la CRA como Protegus 2.

Módulo Ethernet E485 – los mismos ajustes de red, sin WiFi (**DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway**), y del mismo modo puedes asignar un código Contact ID a los fallos del bus RS485 (corte y restablecimiento de la conexión entre el módulo y el G16T); el evento lo reciben tanto la CRA como Protegus 2.

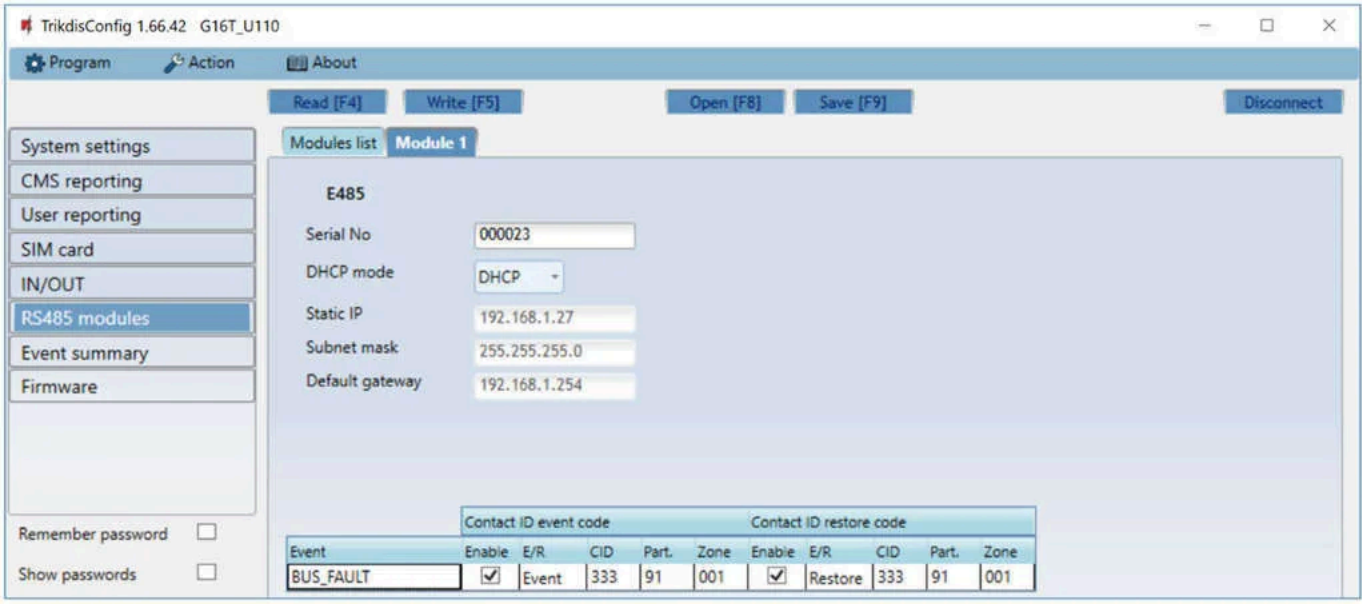


Figura 35. TrikdisConfig – RS485 modules, pestaña del módulo E485.

Para que el W485 y el E485 funcionen, la conexión del G16T con la CRA y/o con Protegus debe estar configurada (apartados 2.2 y 2.3) y, por defecto, el G16T también debe tener una tarjeta SIM (si hace falta, también puede funcionar sin SIM: Trikdis lo añadió más tarde, a petición).

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**.

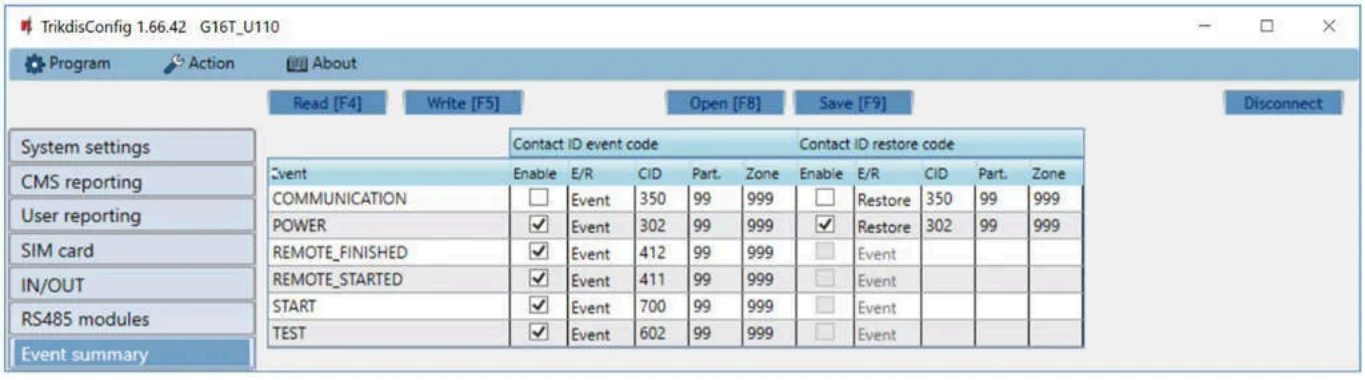


Figura 36. TrikdisConfig – página Event summary: los mensajes internos del dispositivo.

6.9 Restablecer los ajustes de fábrica

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

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

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.

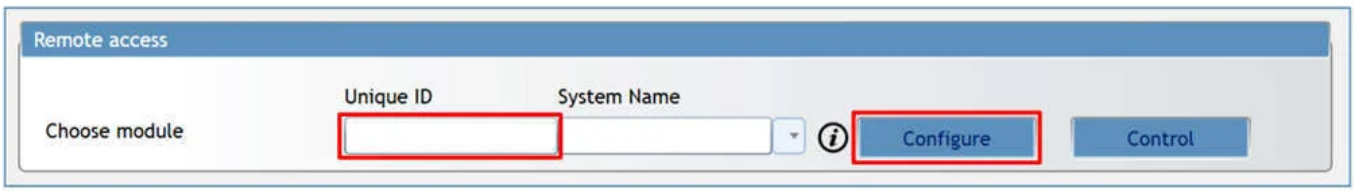


Figura 37. TrikdisConfig – Remote access: el identificador del dispositivo, el nombre del sistema y el botón Configure.

La habilitación de la nube de Protegus se describe en el apartado 6.4.

8. Comprobación del funcionamiento del comunicador

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

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

1. **Provoca un evento.** Arma y luego desarma el sistema desde el teclado o, con el sistema armado, viola una zona para que se produzca una alarma.
2. **Comprueba la recepción.** Mira si el evento ha aparecido en el software de la CRA y/o en la lista de eventos de la aplicación Protegus 2, con el número de partición y de zona correctos.
3. **Entradas.** Activa el detector conectado a una entrada propia del comunicador y comprueba el evento correspondiente.
4. **Salidas.** Activa la salida desde la aplicación Protegus 2 y comprueba que el dispositivo conectado (relé, zona de interruptor de llave) realmente se acciona.
5. **Armado remoto.** Si la central se puede controlar a distancia, ármala y desármala también desde la aplicación Protegus 2.

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.

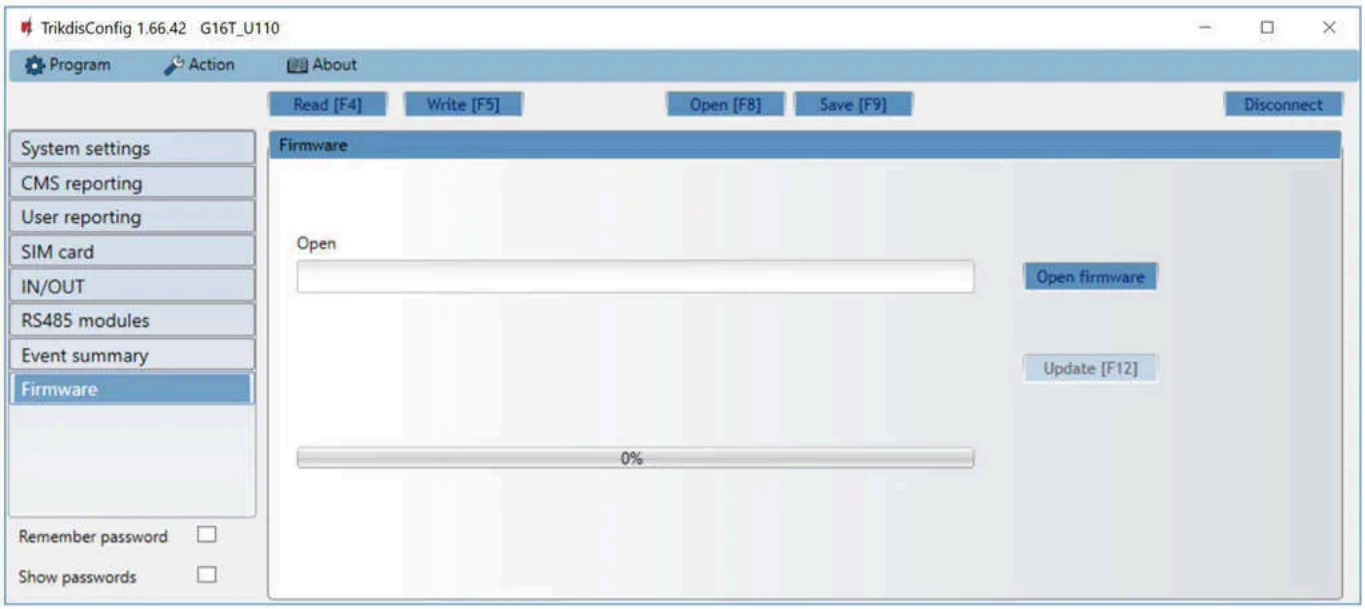


Figura 38. TrikdisConfig – página Firmware: Open firmware y Update [F12].

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 descarga el archivo a mano y ábrelo en la página Firmware.

10. Resolución de problemas y preguntas frecuentes

Las preguntas y averías más frecuentes, partiendo de las indicaciones 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 = no hay APN, 4 = no puede conectarse a la red GSM, 5 = no puede conectarse a la red de datos.
2. Comprueba que la tarjeta SIM está activa, tiene servicio de datos y está bien asentada en la ranura.
3. Si la petición del PIN está activada en la tarjeta, introduce el PIN en la página **SIM card**, o desactiva la petición del PIN con un teléfono.
4. Comprueba la antena: está enroscada, no está dentro de una caja metálica y el nivel de señal es adecuado (apartados 1.6 y 3.2).

Hay red, pero la CRA no recibe eventos

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

1. Los 6 destellos del LED **TROUBLE** indican que no hay conexión con el receptor: comprueba la dirección y el puerto del receptor, el ajuste TCP/UDP y la clave de cifrado (**CMS reporting**).

2. Si el receptor está indicado con un nombre de dominio, comprueba el ajuste de DNS (**CMS reporting → Settings**).
3. Comprueba que el plan de datos de la tarjeta SIM no bloquea el puerto necesario (algunas tarjetas M2M solo permiten determinadas direcciones).

La central no envía los eventos al comunicador

1. El marcador de la central debe estar activado, en modo DTMF, con formato Contact ID y con número de teléfono introducido (capítulo 4).
2. Comprueba la conexión TIP/RING; los 7 destellos del LED **TROUBLE** indican que falta la conexión con la central (si está conectado con supervisión de línea).
3. Si la central espera tono de llamada y no inicia la llamada, desactiva en ella la detección del tono de llamada.
4. Si la central indica un «error de comunicación» aunque el evento haya llegado, comprueba el ajuste **Wait acknowledgment from CMS** (apartado 6.2).

Protegus 2 no ve el dispositivo

1. En la página **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 dispositivo; una vez creado el sistema, ya no se puede modificar en el dispositivo.
3. Escribe el IMEI exactamente, copiándolo 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 en verde, y el LED DATA se apaga después de un evento).

No puedo acceder a distancia con TrikdisConfig

1. El dispositivo debe estar en línea (LED NETWORK en verde), y la conexión con Protegus debe estar habilitada.
2. **CMS reporting → Settings → IP ping period** no debe ser superior a 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 G16T con módem 2G (G16T_G410) no tiene bus RS485; los módulos iO-8, W485 y E485 solo se pueden conectar a la versión 4G (G16T_E120). Para el módulo W485 y E485, por defecto, el G16T también debe tener una tarjeta SIM; si hace falta, también puede funcionar sin SIM (una mejora que Trikdis añadió más tarde, a petición).

Tengo un dispositivo 2G: ¿hasta cuándo funcionará?

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

¿Cuántos datos consume el dispositivo?

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

11. Normas 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.

- El montaje y el mantenimiento de equipos de seguridad solo los puede realizar un instalador cualificado.
- Antes de la instalación, lee el manual; no seguir las instrucciones puede provocar un funcionamiento incorrecto o una avería.
- Antes del cableado, en cada conexión eléctrica y antes de cualquier reparación, desconecta el equipo de la alimentación.
- Los fallos debidos a una instalación o un uso inadecuados, así como las modificaciones y reparaciones no autorizadas por Trikdis, anulan la garantía.
- Respeta las normas locales de gestión de residuos: no tires el aparato averiado ni sus componentes a la basura doméstica.

Ver también

- Armado a distancia con interruptor de llave desde la aplicación Protegus 2 – los detalles y las trampas del armado con interruptor de llave.
- Llega la versión de hardware 4 de los comunicadores GSM G16 y G16T – qué ha cambiado respecto a la versión anterior.
- Novedades del comunicador G16T v3 – la presentación del producto.
- Documentación en inglés: docs.trikdis.com.

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

Productos relacionados

Trikdis G16T 4G GSM comunicador inteligente (TIP-RING)

Trikdis G16T 2G GSM comunicador inteligente (TIP-RING)

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-g16t