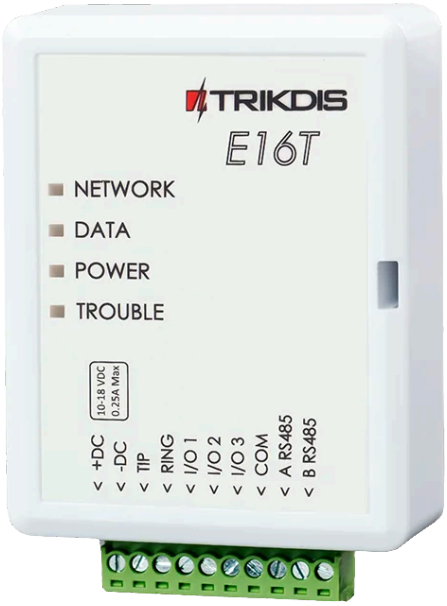
Comunicador E16T – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Ethernet Trikdis E16T: conexión a la central de alarma, configuración de red en TrikdisConfig, transmisión a la CRA, aplicación Protegus 2, comprobación y resolución de averías.



Edición: 2026-11-17
Versión web siempre actualizada: https://trikdis.es/manual-e16t

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 de los LED
1.7 Datos técnicos

2. Puesta en marcha rápida con TrikdisConfig

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

3. Instalación y conexión

3.1 Pasos de la instalación
3.2 Ubicación y red
3.3 Conexión a la central de alarma
3.3.1 Si está justificado: supervisión de línea
3.4 Conexión de una zona de interruptor de llave
3.5 Conexión de entradas
3.6 Conexión del cable Ethernet
3.7 Conexión de una salida con relé
3.8 Conexión del módulo de expansión iO-8
3.9 Encendido y primera comprobación
A TRIKDIS átjelző elindítása

4. Programación de la central de alarma

4.1 Programación del marcador de Honeywell Vista
4.2 Centrales de otros fabricantes

5. Control a distancia con la aplicación Protegus 2

5.1 Añadir el equipo
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Armado y desarmado con una salida
5.3 Armado y desarmado desde la aplicación

6. 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 Ethernet settings
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Restablecimiento de la configuración de fábrica

7. Programación a distancia

8. Comprobación del funcionamiento del comunicador

9. Actualización del firmware

10. Resolución de averías y preguntas frecuentes

11. Normas de seguridad

Ver también

1. Descripción general

El E16T es el **comunicador Ethernet universal** 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 «marca», envía el mensaje Contact ID con tonos DTMF, y el E16T descuelga la línea, decodifica el mensaje y lo transmite a través de la red local, por la conexión a internet por cable, al receptor de la CRA y a la nube Protegus, a la aplicación del usuario. Así se puede usar con **centrales de cualquier marca** que tengan un marcador Contact ID: no hace falta cambiar la central, solo configurar su marcador. El E16T funciona por internet por cable, sin tarjeta SIM y sin suscripción.

1.1 Para qué sirve y cómo funciona

- **Transmite a la CRA.** Envía los eventos por conexión IP a un receptor Trikdis de software o de hardware (protocolo TRK; estos receptores funcionan con cualquier software de CRA) o a cualquier receptor universal (SIA DC-09 2007/2012, SUR-GARD TL150). Por defecto comprueba la conexión cada 30 segundos (envía una señal de vida, PING, al receptor; el intervalo se puede cambiar) y, si hay un fallo, cambia 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 controlar los dispositivos conectados (iluminación, puerta, ventilación, calefacción, riego, etc.). La aplicación funciona con la central de alarma de cualquier fabricante a la que esté conectado el E16T.
- **Juntos 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 están configurados los dos, el evento se envía primero a la CRA y después al usuario.
- **Tiene sus propias entradas y salidas.** Los tres bornes de E/S de doble función se pueden usar como entradas (detector, sabotaje) o como salidas controlables (zona de interruptor de llave, relé). Con el módulo de expansión iO-8 conectado al bus RS485 se pueden añadir 8 E/S más al sistema.
- **Sin suscripción.** El E16T usa la conexión a internet que ya hay en la instalación: no necesita tarjeta SIM, contrato móvil ni antena, y la intensidad de la señal móvil no importa.

La figura siguiente muestra la estructura del sistema: la salida de línea telefónica de la central se conecta al E16T, el E16T llega a internet a través del router local y desde allí al receptor de la CRA y a la nube Protegus, y el usuario ve el sistema en la aplicación Protegus 2.

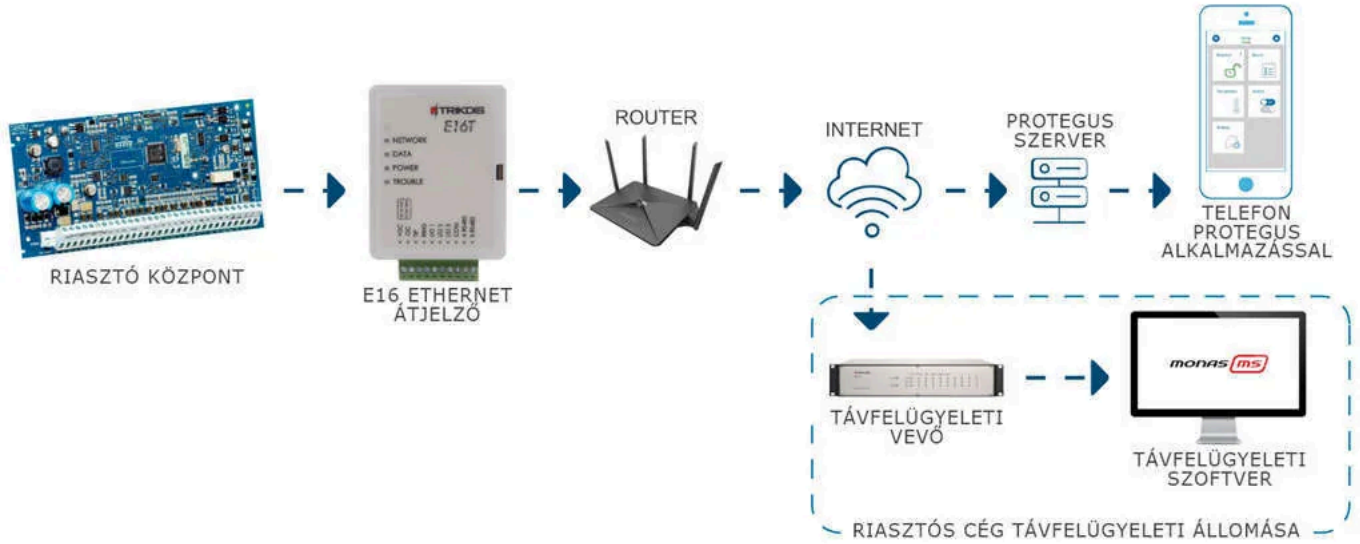


Figura 1. El lugar del E16T en el sistema: central de alarma → E16T → router → internet → receptor de la CRA y nube Protegus → aplicación Protegus 2.

1.2 Versiones

Este manual está hecho para la **versión de hardware actual del E16T, la v2** (TrikdisConfig la muestra con el nombre **E16T_2000**), pero **también sirve para el E16T anterior**: la conexión, la configuración y el funcionamiento son en gran parte iguales. Las diferencias se resumen en la tabla siguiente; donde el texto da el dato de la v2, en la versión anterior ten en cuenta este.

	E16T anterior	**E16T v2 (actual)**
Entradas/salidas	2 entradas de tipo seleccionable (T-1/IN1, R-1/IN2 – NC, NO, EOL; también sirven para supervisar la línea telefónica) + 1 salida de colector abierto (OUT, máx. 0,15 A, hasta 30 V; se controla desde la aplicación Protegus)	3 bornes de E/S de doble función (I/O 1, I/O 2, I/O 3); cada uno se puede usar como entrada (tipos NC, NO, EOL, DEOL) o como salida de colector abierto (máx. 0,15 A)
Consumo	hasta 0,5 A	100 mA nominal, hasta 250 mA durante el envío
LED	NETWORK, DATA, POWER, TROUBLE, LINE (el LINE se enciende en verde mientras la central «ha descolgado», es decir, marca; las indicaciones distintas de los demás LED se enumeran en la nota al final del apartado 1.6)	NETWORK, DATA, POWER, TROUBLE
Memoria de eventos	100 mensajes	60 mensajes
Dimensiones	88 × 62 × 25 mm	88 × 65 × 26 mm

La versión de hardware se ve en la barra de estado de TrikdisConfig (**HW**) y en la etiqueta de la parte trasera del equipo.

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 E16T transmite la información completa del evento (código, partición, zona o usuario).

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: puede enviar a dos receptores a la vez, cada uno con su propio canal de respaldo.
- Comunicación cifrada y protegida con contraseña; memoria de 60 eventos.

Funciones para el usuario

- Aplicación móvil y web Protegus 2: notificaciones, lista de eventos, armado y desarmado, control de salidas.
- Derechos de usuario en varios 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 – para la configuración del equipo, para el administrador de la CRA y para el instalador.
- Se puede configurar y actualizar a distancia con el programa TrikdisConfig.

1.4 Partes del comunicador

El circuito impreso del E16T va en una caja de plástico blanca; la tapa frontal se puede quitar y la regleta de bornes es extraíble. El conector de red (RJ45) está en el borde superior del circuito impreso y se accede a él por una abertura de la caja.

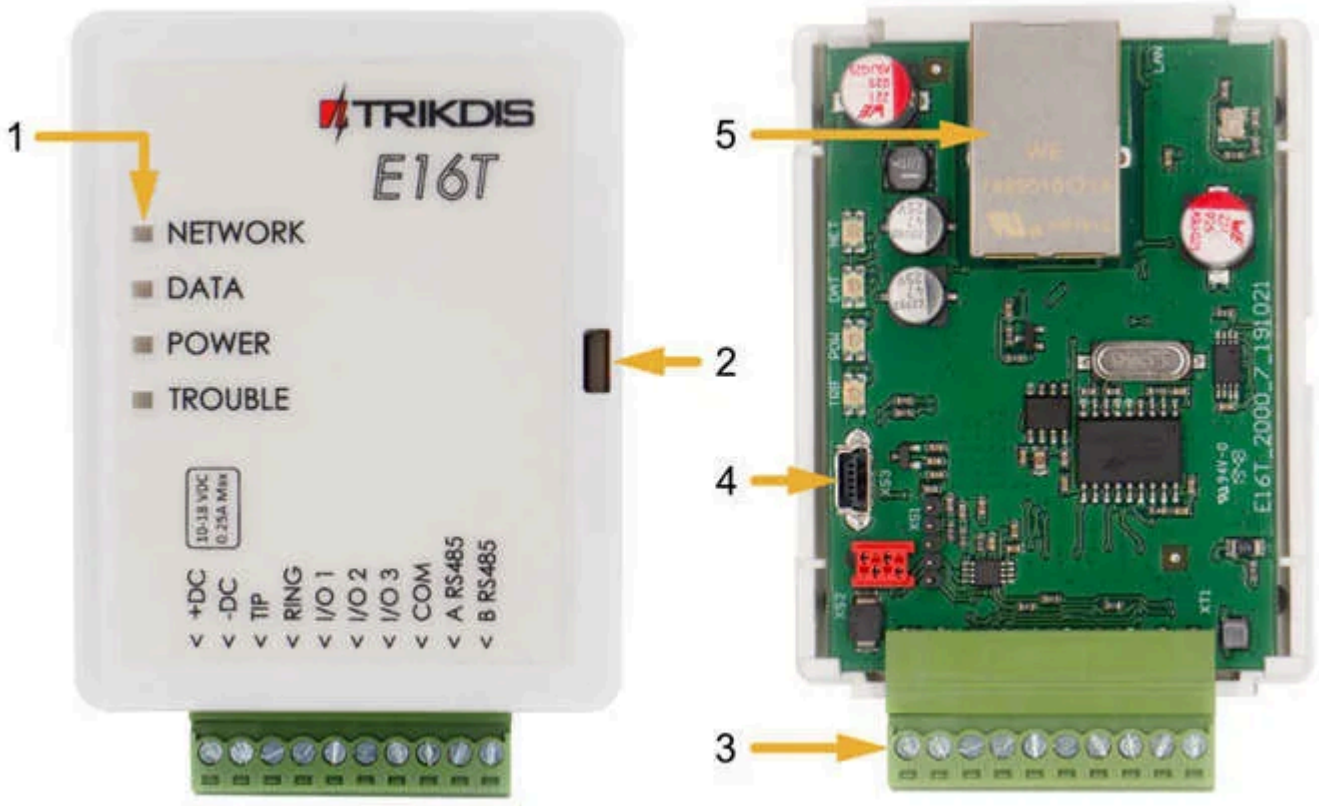


Figura 2. Partes del E16T, por delante y con la caja abierta.

- 1 Indicadores LED (NETWORK, DATA, POWER, TROUBLE)
- 2 Ranura para quitar la tapa frontal (en el borde superior de la tapa)
- 3 Regleta de bornes extraíble
- 4 Conector USB Mini-B para la programación
- 5 Conector Ethernet (RJ45)

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

1.5 Bornes

Borne	Función
+DC	Alimentación, +10–18 V CC
–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 (iO-8 y otros módulos de expansión de la serie iO)
B 485	Hilo B del bus RS485

Los nombres de los bornes también están impresos en la tapa frontal, así que no hace falta quitarla para hacer el cableado.

1.6 Indicaciones de los LED

Los LED de la tapa frontal son las herramientas más importantes para la puesta en marcha y la búsqueda de averías. Léelos juntos: el POWER muestra la alimentación, el NETWORK la conexión de red, el DATA los mensajes pendientes de envío y el TROUBLE las averías.

NETWORK – conexión de red

Indicación	Significado
apagado	No hay conexión de red (no hay cable, el puerto no está activo o no ha recibido dirección IP)
verde fijo	Conectado a la red local: la conexión llega hasta el router. Si también hay acceso a internet lo indica el LED DATA (ver más abajo).

DATA – tráfico de datos

Indicación	Significado
apagado	No hay mensajes pendientes de envío
verde fijo	Hay mensajes pendientes de envío en la memoria
verde intermitente	Envío o recepción de 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	No hay alimentación, o la alimentación está desconectada
verde fijo	Encendido, la tensión de alimentación es correcta
amarillo fijo	Tensión de alimentación incorrecta (11,5 V o menos)
verde fijo, amarillo intermitente	Listo para programar (cable USB conectado)
amarillo fijo (durante la programación)	No hay conexión con el ordenador

TROUBLE – avería

Indicación	Significado
apagado	No hay avería

Indicación	Significado
1 destello rojo	No hay conexión física de red (enlace PHY): cable, conector o puerto del router/switch
2 destellos rojos	Error de DHCP: el equipo no ha recibido dirección IP
3 destellos rojos	Error de DNS: la resolución de nombres no funciona
6 destellos rojos	No hay conexión con el receptor de la CRA
7 destellos rojos	Se ha perdido la conexión con la central de alarma
rojo intermitente (durante la programación)	Error de memoria
rojo fijo (durante la programación)	Firmware dañado

E16T anterior

Los LED del E16T anterior indican en parte otras cosas: el **DATA** se enciende en amarillo si hay un evento pendiente de envío en la memoria y parpadea en verde mientras la central transmite un mensaje al comunicador; el **POWER** parpadea en verde si la alimentación está encendida y la tensión es correcta, y parpadea en amarillo si la tensión no es suficiente (11,5 V o menos); la luz roja fija del **TROUBLE** indica un fallo de la conexión de red (LAN), y apagado significa que no hay avería; el **LINE** se enciende en verde mientras la central «ha descolgado» (apartado 1.2).

1.7 Datos técnicos

Parámetro	Valor
Conexión con la central de alarma	línea telefónica por cable (TIP/RING), Contact ID, DTMF
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 CC
Ampliación	por el bus RS485: módulo de expansión iO-8 (+8 E/S) y otros módulos de la serie iO, hasta 4 módulos
Conexión de red	Ethernet, IEEE 802.3, 10Base-T, conector RJ45
Configuración de red	DHCP (de fábrica) o dirección IP fija
Tensión de alimentación	10–18 V CC
Consumo	100 mA nominal; hasta 250 mA durante el envío
Protocolos de transmisión	TRK, DC-09_2007, DC-09_2012, TL150
Memoria de eventos	60 mensajes
Programación	TrikdisConfig (Windows) por cable USB Mini-B o a distancia
Entorno de funcionamiento	−10 … +50 °C, humedad relativa máx. 80 % (a +20 °C)
Dimensiones	88 × 65 × 26 mm
Peso	80 g

2. Puesta en marcha rápida con TrikdisConfig

Toda la configuración del E16T 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 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 (para la configuración) · cable de al menos 4 hilos hasta la central · destornillador plano de 2,5 mm · cable Ethernet (CAT-5 o superior, máximo 100 m) hasta el router o el switch · un puerto de red libre · si en la red no hay DHCP: la dirección IP fija, la máscara, la puerta de enlace y el DNS que te dé el administrador de red · el manual de instalación de la central de alarma. Lo que falte se puede pedir aparte al distribuidor local.

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

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

2. Abre la tapa frontal del E16T y conéctalo al ordenador. Introduce un destornillador plano en la ranura del borde superior de la tapa y, haciendo palanca hacia abajo, suelta la tapa con cuidado; después conecta el cable USB Mini-B. El USB da alimentación suficiente para la programación; no hace falta una fuente aparte.

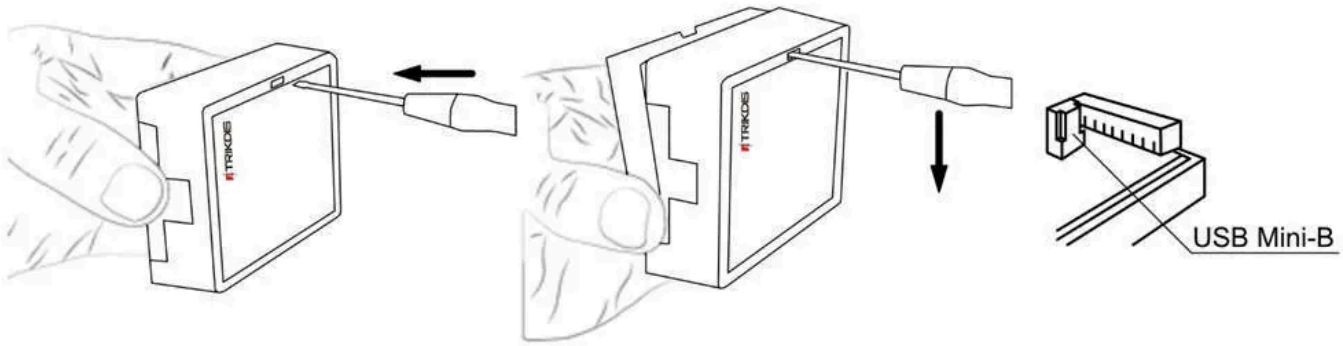


Figura 3. Apertura de la tapa frontal y conexión al ordenador con un cable USB Mini-B.

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

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

Los dos apartados siguientes describen qué hay que configurar para que la central de alarma se pueda controlar desde la aplicación Protegus 2 (2.2) y para que el comunicador envíe los eventos a la CRA (2.3).

2.2 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 4. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- 1 **Enable connection** – márcalo: habilita la conexión con la nube 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 **System settings**, comprueba el tipo de interfaz de la central de alarma.

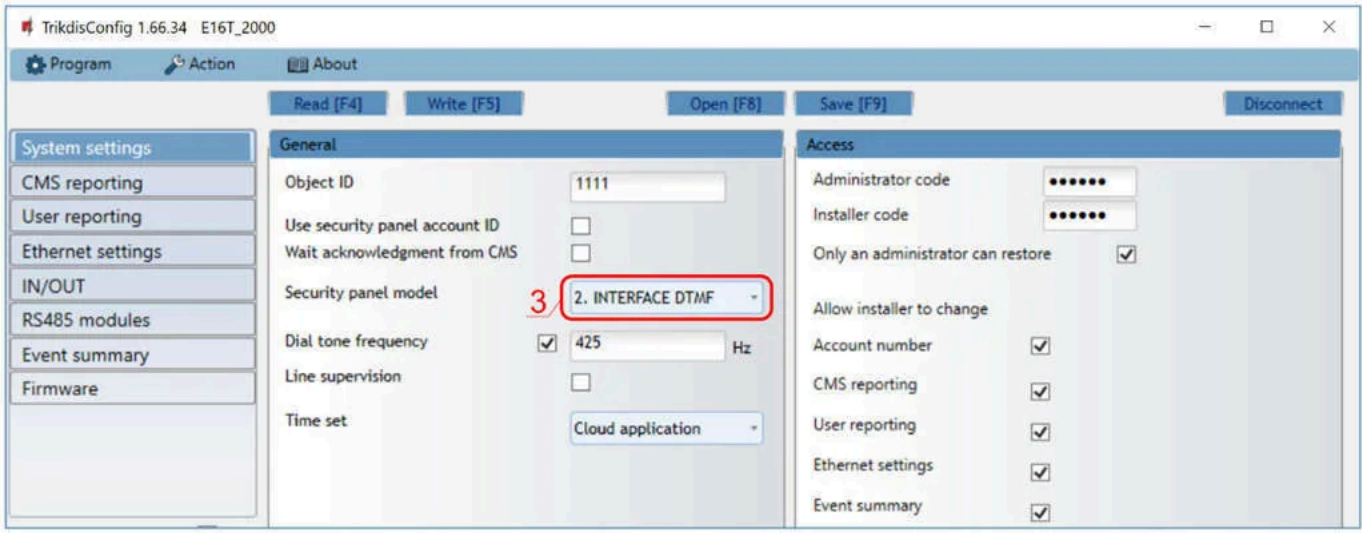


Figura 5. TrikdisConfig – página System settings, grupo General.

- 3 **Security panel model** – debe quedar en **2. INTERFACE DTMF** (la conexión por línea telefónica con marcación DTMF).

Para la configuración de red, en la página **Ethernet settings** viene marcado de fábrica **Use DHCP**: el equipo obtiene automáticamente la dirección IP del router y, en la mayoría de los casos, no hay que hacer nada más. Si en la red no hay DHCP o hay que usar una dirección fija, introduce aquí la configuración manual (apartado 6.5).

Si usas el equipo solo con Protegus 2, sin CRA, la configuración ya está lista: pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB.

No olvides activar y configurar el marcador telefónico de la central de alarma; si no, la central no enviará eventos. La configuración de la central se describe en el capítulo 4.

2.3 Conexión con la CRA

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

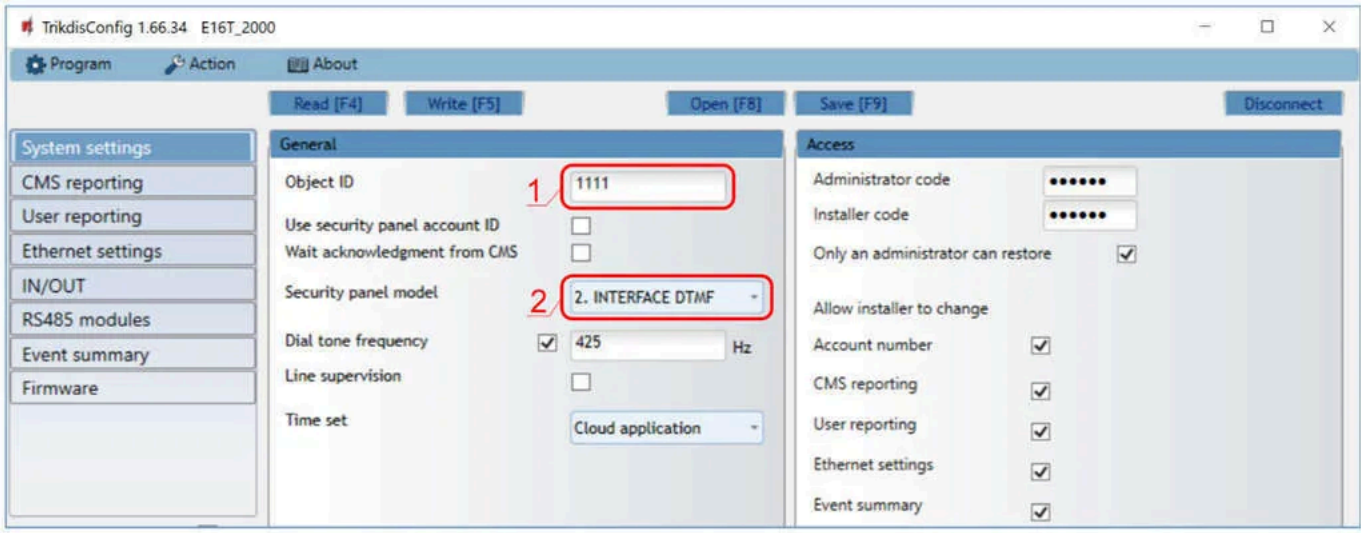


Figura 6. TrikdisConfig – página System settings, grupo General.

- 1 **Object ID** – el número 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** – debe quedar en **2. INTERFACE DTMF**.

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

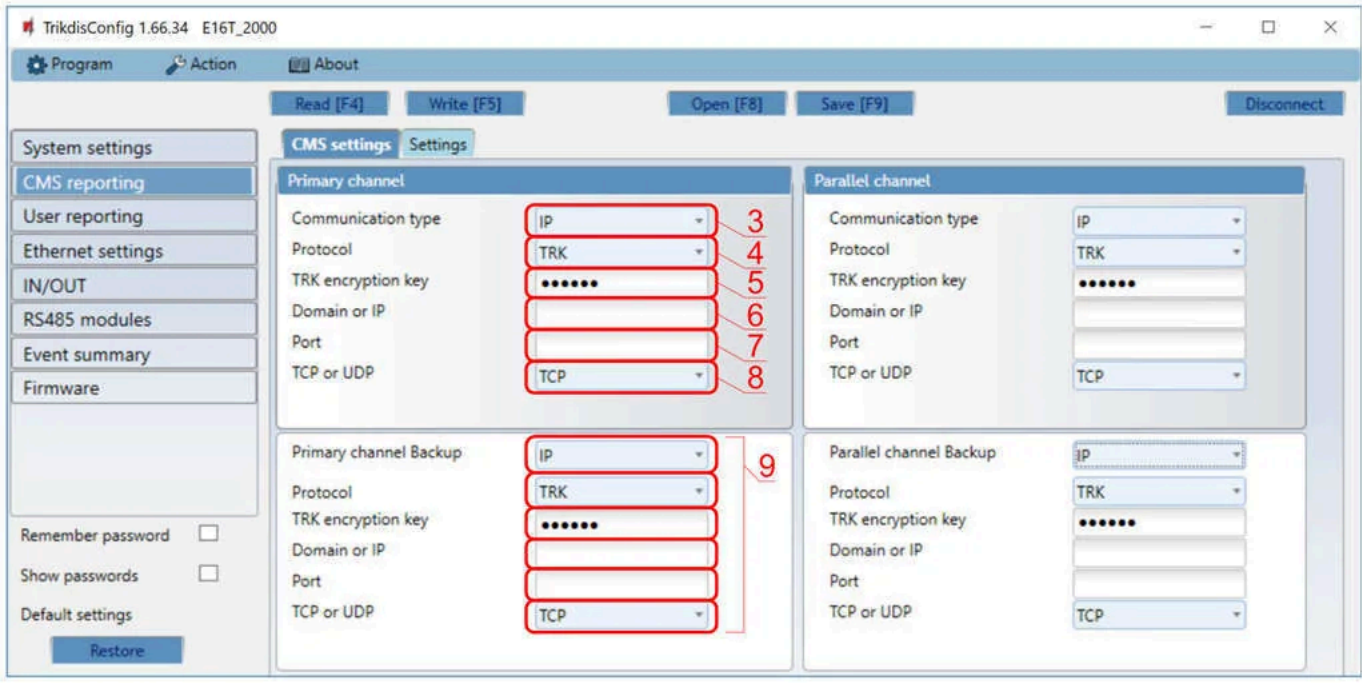


Figura 7. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 3 **Communication type** – **IP** (en el E16T es la única opción).
- 4 **Protocol** – **TRK** para un receptor Trikdis, **DC-09_2007** o **DC-09_2012** para un receptor universal, **TL150** para un receptor SUR-GARD.
- 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 transporte; se ajusta a la configuración del receptor.
- 9 **Primary channel Backup** – canal de respaldo para cuando falle el principal; se rellena igual, y se recomienda configurarlo.

Con el protocolo **DC-09**, en la pestaña **Settings** introduce también el número de objeto, de línea y de receptor DC-09 (apartado 6.3); con DC-09_2012 también se puede activar el cifrado con la clave DC-09 configurada en el receptor (nota del apartado 6.3). Para comprobar la conexión, el intervalo de la señal de vida (PING) se ajusta en esa misma pestaña **Settings** (**IP ping period**, de fábrica 30 s). Si has indicado el receptor con un nombre de dominio, para la resolución de nombres también hace falta el ajuste DNS de la página **Ethernet settings** (de fábrica lleva el DNS público de Google). En el E16T anterior los campos tienen otros nombres (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**); la correspondencia está en la nota del apartado 6.3.

Si el usuario también usa la aplicación Protegus 2, haz también los ajustes del apartado 2.2 (**User reporting** → **PROTEGUS Cloud**). 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 el cableado.

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. Saca el circuito impreso de la base: abre el cierre de la esquina.
3. Fija la base con tornillos en el lugar elegido.
4. Vuelve a colocar el circuito impreso en la base y vuelve a enchufar la regleta de bornes.
5. Conecta el cable Ethernet al conector RJ45 (apartado 3.6).
6. Vuelve a colocar la tapa frontal.

3.2 Ubicación y red

- 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. Una caja metálica no le molesta: el E16T no tiene antena.
- El cable Ethernet (CAT-5 o superior) hasta el router o el switch puede medir **como máximo 100 m**.
- Mantén el comunicador y los cables alejados del transformador de la central y de los cables de red eléctrica.

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.

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

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

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

Corte de corriente

El E16T se alimenta de la central de alarma, así que durante un corte de corriente sigue funcionando con la batería de la central; en cambio, el router y el módem normalmente no, y sin ellos no hay internet. Si para el sistema esto no es aceptable, alimenta también los equipos de red con un SAI o elige un comunicador de red móvil (G16T).

3.3 Conexión a la central de alarma

El E16T se conecta a la salida de línea telefónica (TIP/RING) de la central y se alimenta 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.

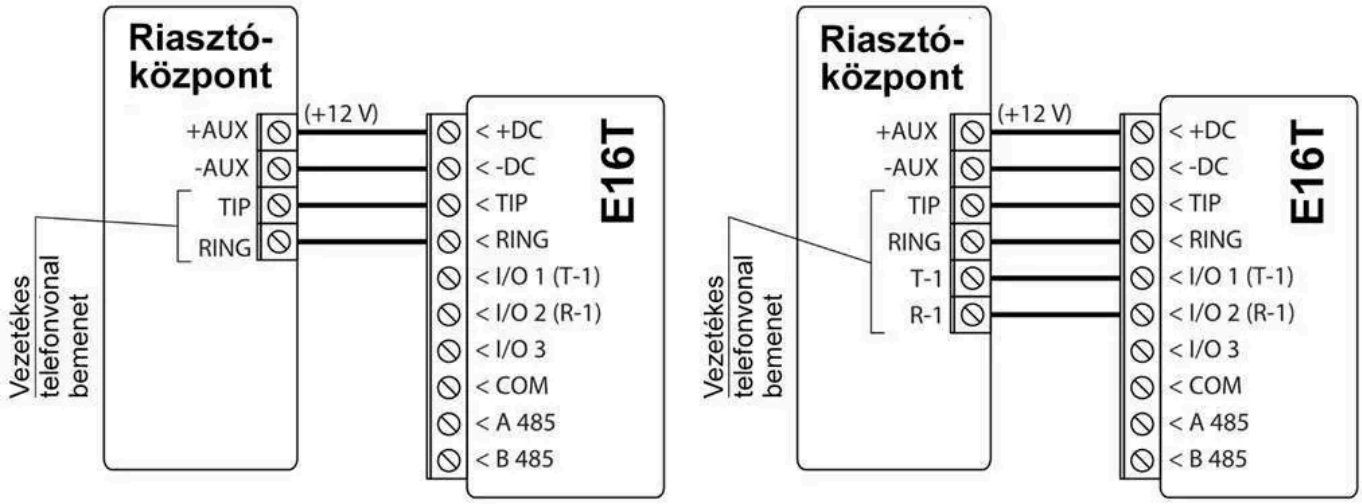


Figura 8. Conexión a la salida de línea telefónica de la central: a la izquierda la conexión normal, a la derecha la conexión con supervisión de línea.

Durante el envío, el E16T consume como máximo 250 mA. 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 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 una zona de interruptor de llave

Si quieres armar y desarmar la central a distancia desde la aplicación Protegus 2, configura uno de los bornes de E/S 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 E16T tiene tres bornes de E/S, se pueden manejar hasta tres particiones, cada una con su propia salida.

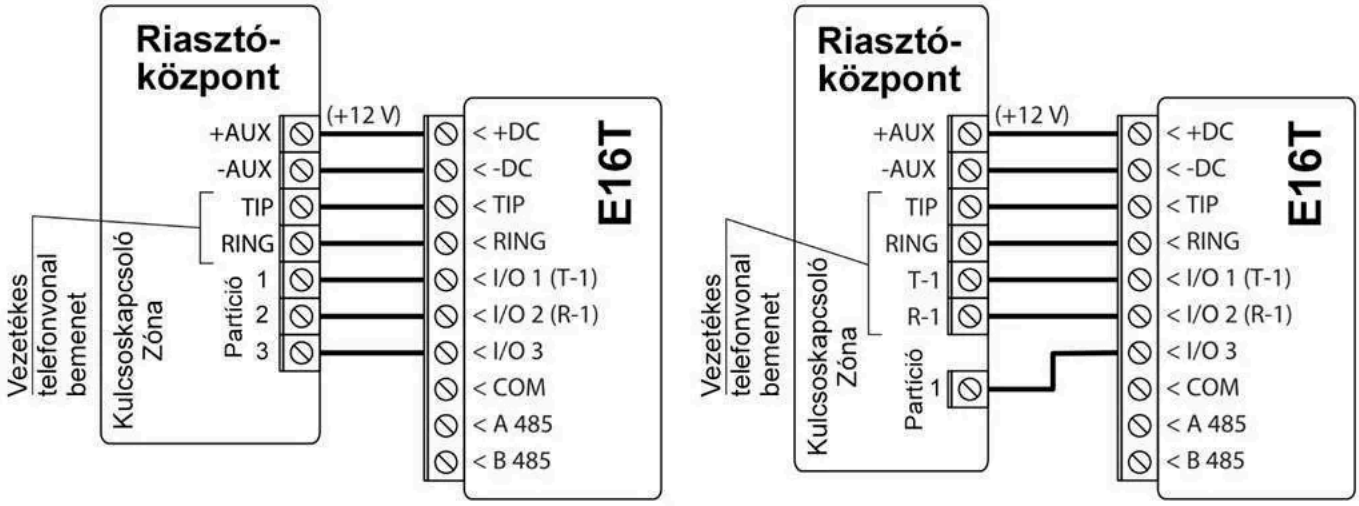


Figura 9. Armado y desarmado con una zona de interruptor de llave: a la izquierda la conexión normal, a la derecha la conexión con supervisión de línea (en este caso queda I/O 3 para el interruptor de llave).

La zona de interruptor de llave puede ser de impulso o de dos estados (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.

E16T anterior

En el E16T anterior (2 entradas + OUT), el tipo y el modo de la salida se configuran en el grupo **System settings** → **Output** de TrikdisConfig: para el armado con interruptor de llave, **OUT type** debe ser **Remote Control** y **OUT mode**, **Pulse** (con duración del impulso) o **Level**, según el tipo de zona de la central.

3.5 Conexión de entradas

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

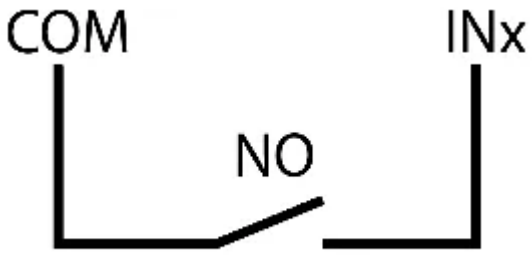


Figura 10. NO – circuito normalmente abierto: cerrado – alarma, abierto – reposo.

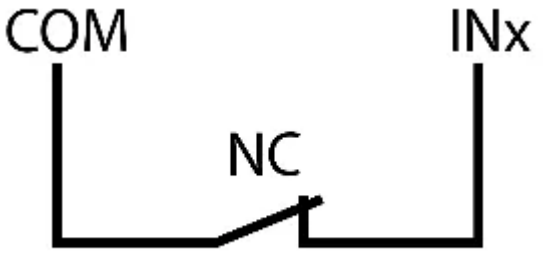


Figura 11. NC – circuito normalmente cerrado: abierto – alarma, cerrado – reposo.

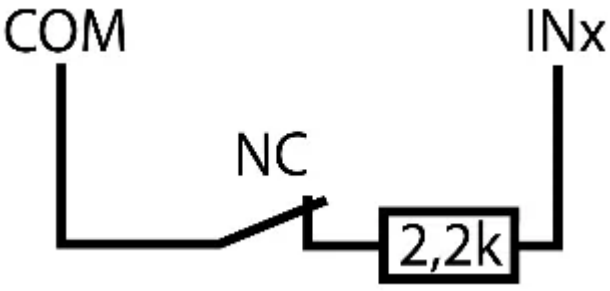


Figura 12. NC/EOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto – alarma, 2,2 kΩ – reposo.

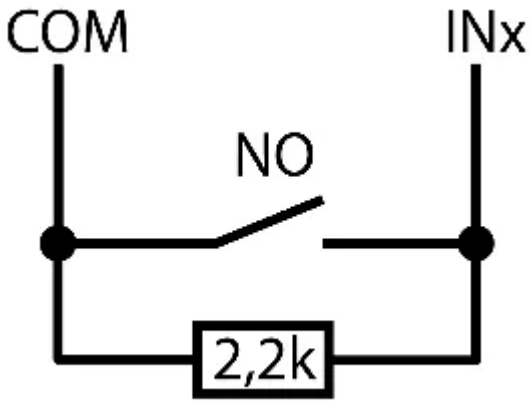


Figura 13. NO/EOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ: cortocircuito o circuito abierto – alarma, 2,2 kΩ – reposo.

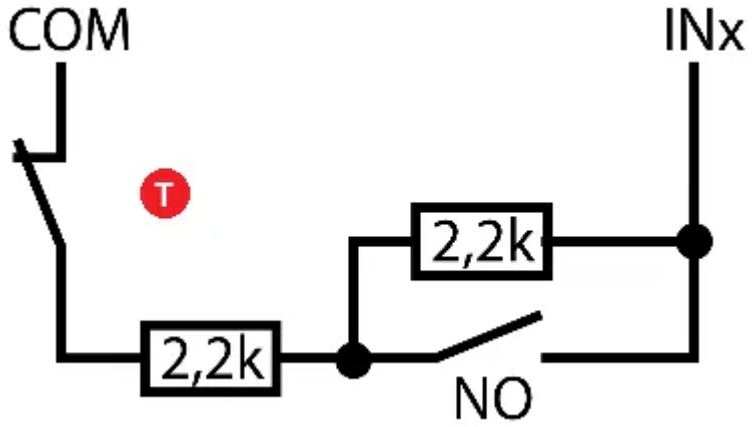


Figura 14. NO/DEOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto – sabotaje, 2,2 kΩ – alarma, 3,3–5,5 kΩ – reposo.

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

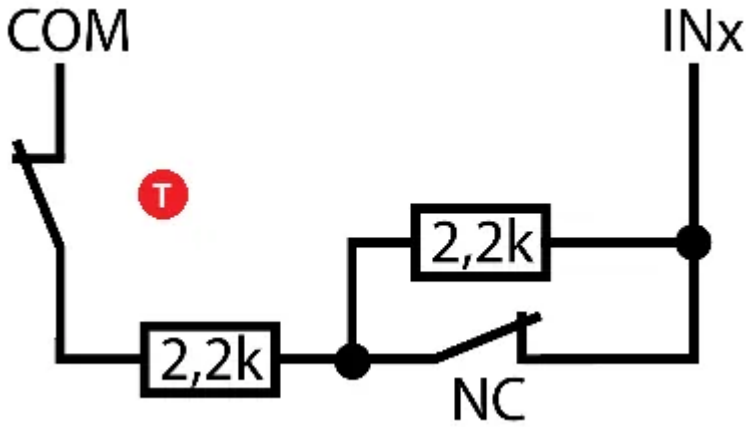


Figura 15. NC/DEOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o circuito abierto – sabotaje, 2,2 kΩ – reposo, 3,3–5,5 kΩ – alarma.

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

E16T anterior

Las dos entradas (IN1, IN2) del E16T anterior (2 entradas + OUT) admiten circuitos de tipo NO, NC o EOL; el ajuste de fábrica es NO. Allí el tipo de entrada no se configura en IN/OUT, sino en la página **Event summary** de TrikdisConfig (nota del apartado 6.6). La conexión es la misma: conecta la entrada según el tipo elegido (NO, NC, EOL).

3.6 Conexión del cable Ethernet

Conecta un extremo del cable Ethernet al conector RJ45 del circuito impreso del E16T y el otro a un puerto libre del router o del switch. Hace falta un cable normal, de conexión directa (patch); el cable entra por la abertura superior de la caja. Tras el encendido, la luz verde del LED **NETWORK** indica que se ha establecido la conexión de red.

3.7 Conexión de una salida con relé

Como salidas, los bornes de E/S son salidas de colector abierto (OC): en estado activo llevan a negativo la carga conectada, con un máximo de 0,15 A y hasta 30 V CC. Los consumos mayores o los equipos de tensión de red conéctalos **a través de un relé**: un extremo de la bobina del relé va a +DC y el otro al borne de E/S. Un LED indicador también se puede conectar directamente a la salida: desde +DC, a través de una resistencia en serie de 2,2 kΩ, al LED, y la otra pata del LED al borne de E/S (en el E16T anterior, al borne OUT).

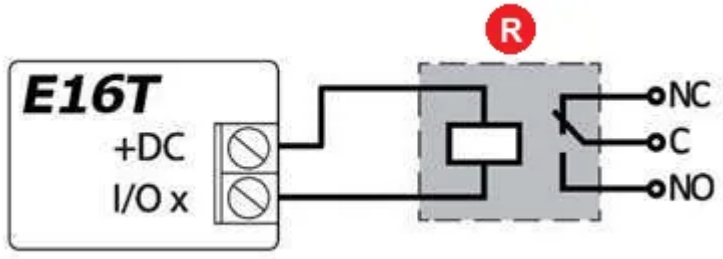


Figura 16. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne I/O x, y los contactos (NC, C, NO) conmutan la carga.

- R relé («Relay»)

Las salidas se controlan desde la aplicación Protegus 2 (capítulo 5).

3.8 Conexión del módulo de expansión iO-8

Si hacen falta más entradas o salidas, al bus RS485 del E16T se pueden conectar hasta cuatro módulos de expansión **iO-8**; cada uno añade 8 E/S de doble función más. 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 bus RS485 puede medir como máximo 100 m; es un máximo teórico, ver la nota del apartado 3.2. El módulo hay que añadirlo en la página **RS485 modules** de TrikdisConfig (apartado 6.7). Al mismo bus se pueden conectar también los demás miembros de la serie iO (iO, iO-WL, iO-LO, LO-MOD); los módulos W485 y E485 no son para el E16T, ya que el propio E16T es un equipo de internet por cable.

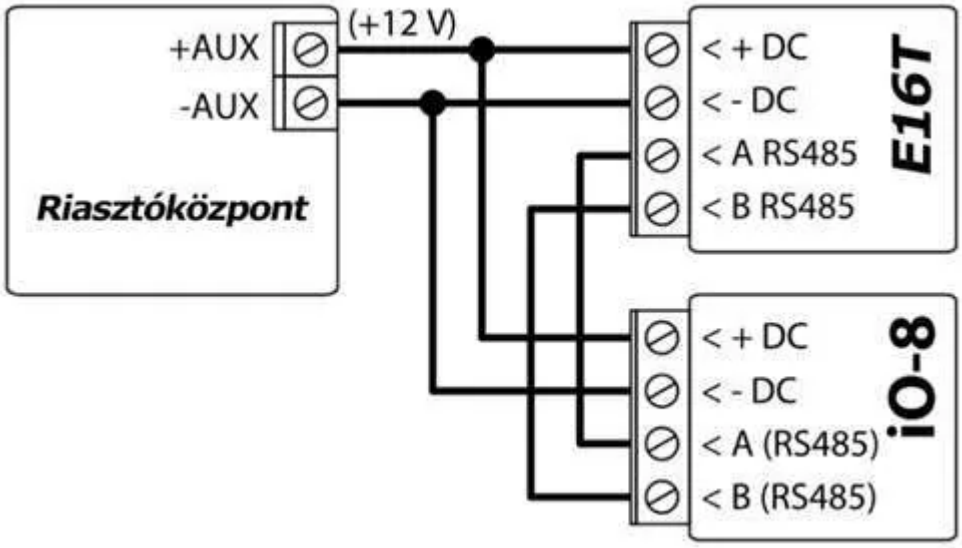


Figura 17. Conexión del módulo de expansión iO-8 al bus RS485 del E16T; la alimentación, desde la salida AUX de la central de alarma.

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

- **POWER** en verde fijo – la alimentación es correcta;
- **NETWORK** en verde fijo – conectado a la red local;
- **TROUBLE** apagado.

Si el TROUBLE parpadea, el número de destellos indica la causa (apartado 1.6): 1 = no hay conexión física (cable, puerto), 2 = no ha recibido dirección IP (DHCP), 3 = error de DNS, 6 = no llega al receptor. 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 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 telefónico, el número de teléfono del receptor, el modo de marcación (DTMF) y el formato de comunicación (Contact ID). Si la central espera tono de línea (dial tone) antes de marcar, lo da el E16T; si aun así no se inicia la llamada, desactiva en la central la detección del tono de línea («marcar sin tono de línea» 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 notificaciones de los eventos, puede armar y desarmar, y puede controlar las salidas del comunicador.

5.1 Añadir el equipo

Antes de añadir el equipo, comprueba lo siguiente:

1. El E16T está conectado a la red y tiene salida a internet: el LED **NETWORK** está en verde fijo y el LED **DATA** se apaga después de un evento o de un informe de prueba.
2. En la página **User reporting** → **PROTEGUS Cloud** de TrikdisConfig (apartado 6.4) está marcado **Enable connection**, es decir, la nube Protegus está habilitada, y está configurado el **Protegus Cloud access code** (una vez creado el sistema, ya no se puede modificar).
3. El LED **POWER** está en verde fijo.

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

A rendszer létrehozása a Protegus 2 alkalmazásban

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

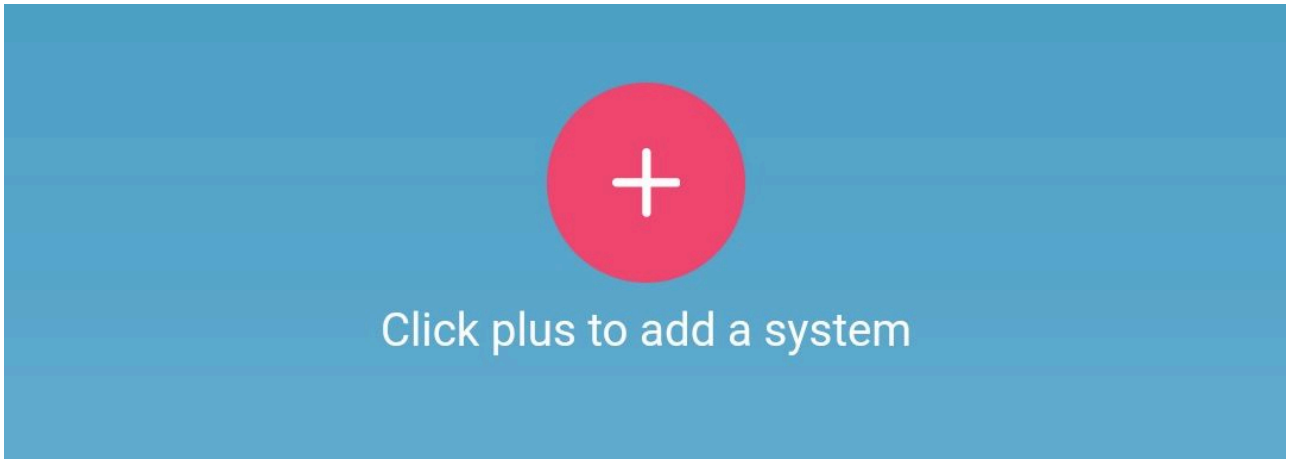








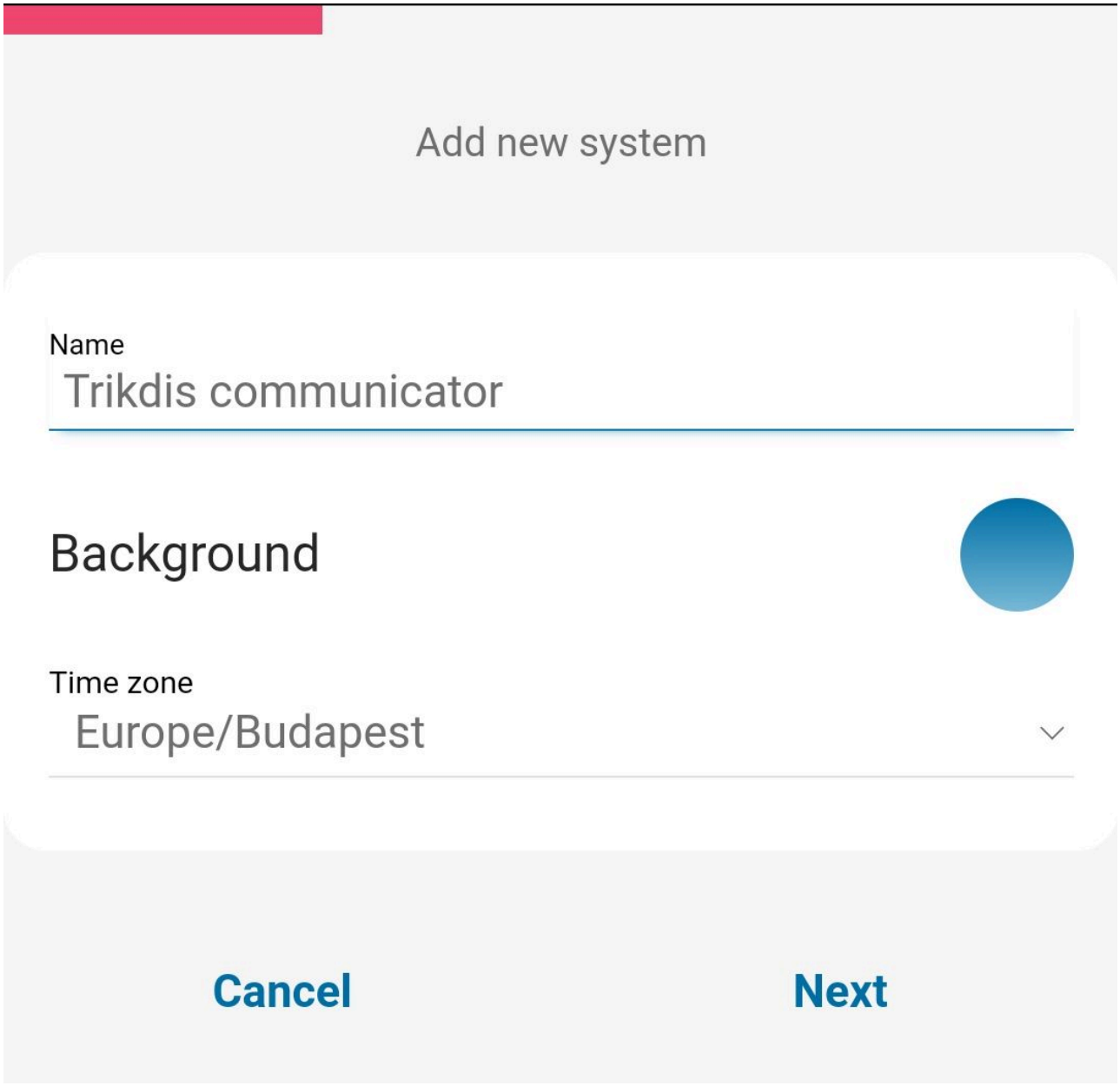
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



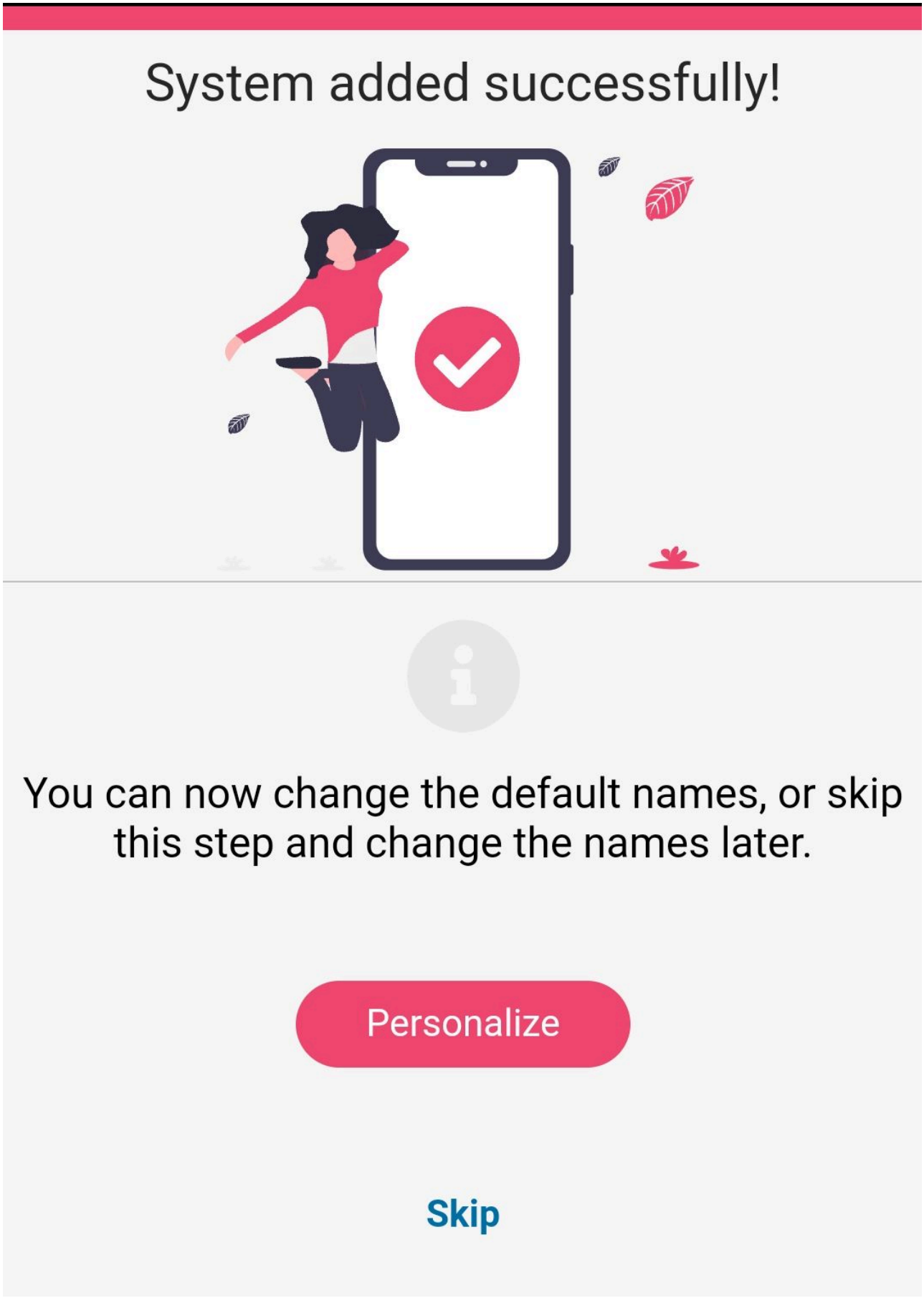
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



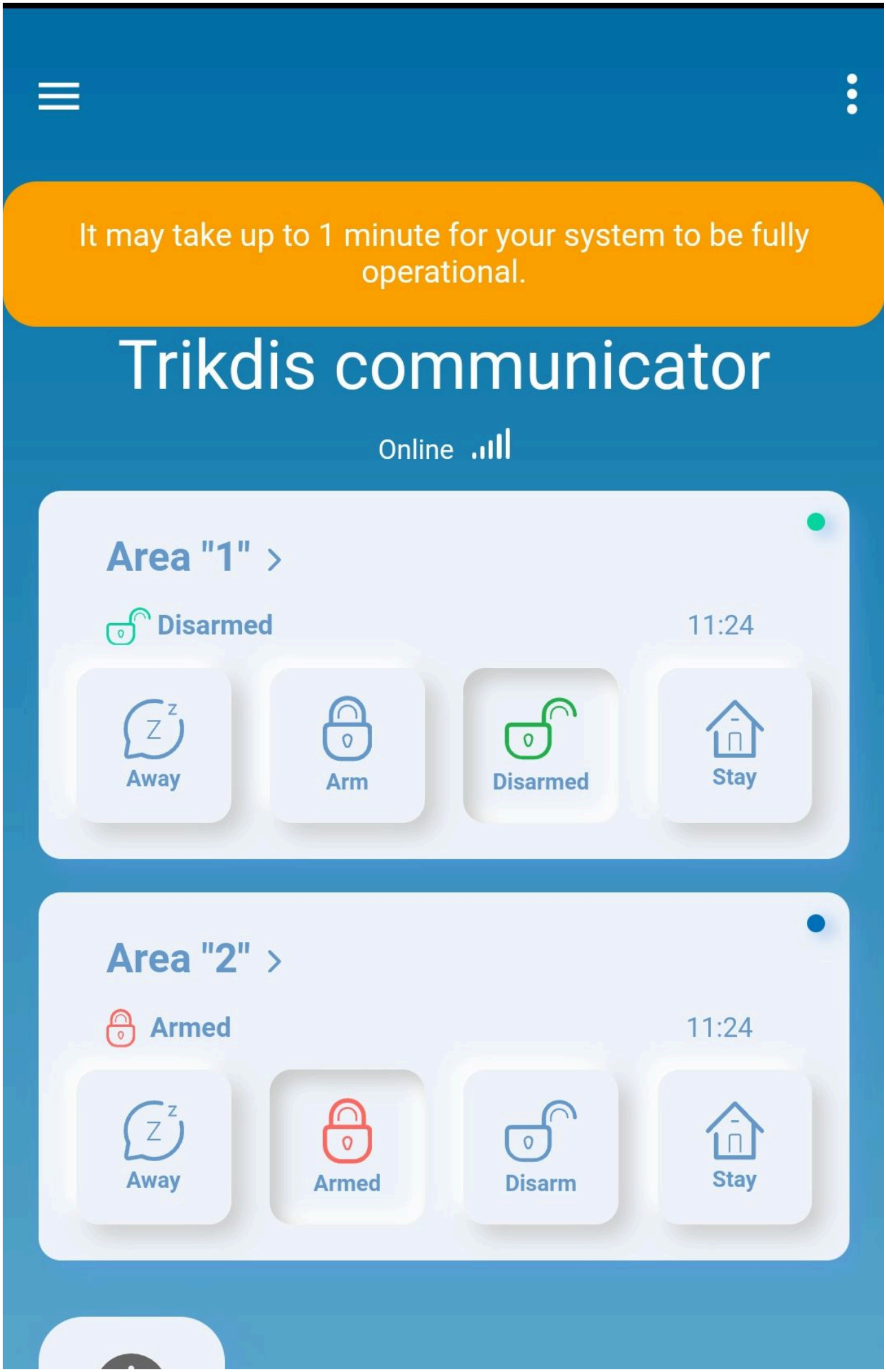
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



En el E16T, el identificador único del equipo es la **dirección MAC**: se puede leer en la caja y en la parte trasera del equipo, y también la muestra TrikdisConfig (**MAC / Unique ID**).

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.

6. TrikdisConfig – la configuración en detalle

En la ventana de TrikdisConfig se ven, a la izquierda, la lista de páginas (System settings, CMS reporting, User reporting, Ethernet settings, IN/OUT, RS485 modules, Event summary, Firmware), arriba, la barra de botones (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**) y, abajo, la barra de estado. Este capítulo repasa, página por página, la configuración del E16T.

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 18. Barra de estado de TrikdisConfig con un E16T leído: a la izquierda, el botón de restablecimiento de fábrica y el MAC / Unique ID; abajo, el estado, el tipo, el número de serie, las versiones, el modo de conexión y el nivel de acceso.

Tras **Read [F4]**, el programa lee y muestra la configuración que hay en el equipo; en el campo **Device** debe aparecer el tipo de equipo (E16T; en la v2, **E16T_2000**). Haz la configuración según las descripciones de las páginas que siguen.

6.2 System settings

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

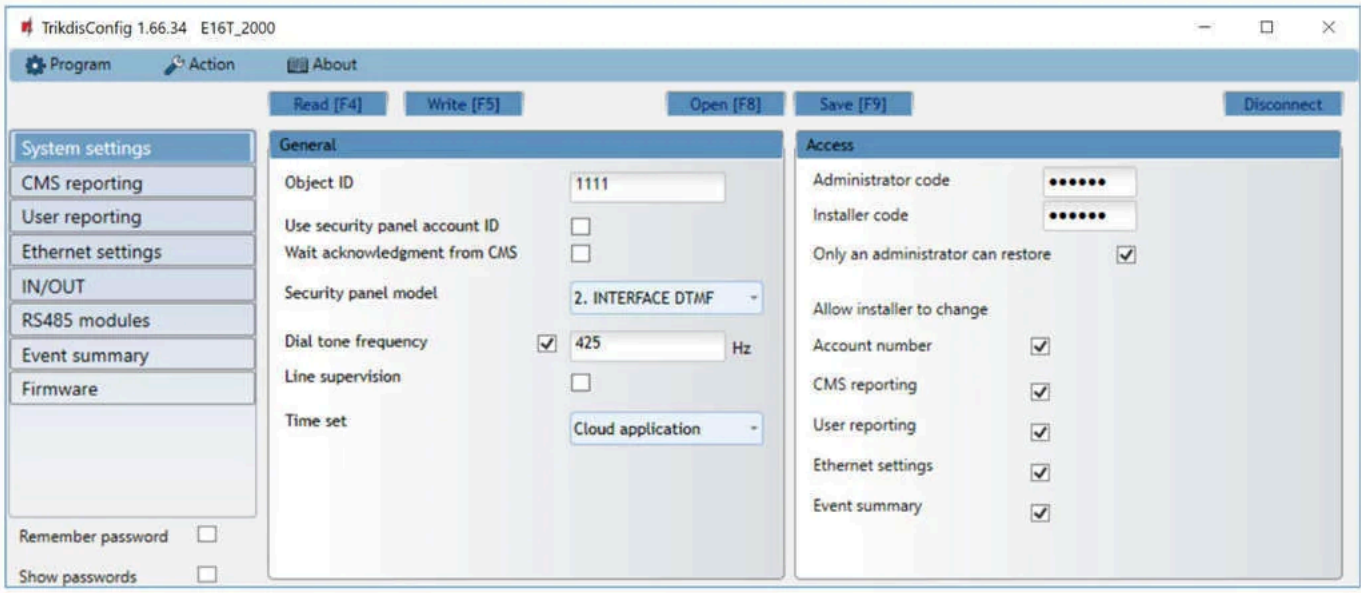


Figura 19. TrikdisConfig – página System settings: grupos General y Access.

- **Object ID** – el número de abonado que te da la CRA (4 caracteres hexadecimales: 0–9, A–F; no se pueden usar `FFFE` ni `FFFF`). Es obligatorio si el equipo también transmite a una CRA.
- **Use security panel account ID** – si lo marcas, el comunicador no usa su propio Object ID, sino el número de abonado que envía la central en el mensaje Contact ID. Es útil si varias particiones transmiten con números de abonado distintos.
- **Wait acknowledgment from CMS** – si lo marcas, 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; por defecto **2. INTERFACE DTMF**. Con él activas o desactivas la interfaz de línea telefónica DTMF del comunicador.
- **Dial tone frequency** – la frecuencia del tono de línea que el E16T da a la central (por defecto 425 Hz, el tono de línea habitual en la mayoría de los países europeos, también en España).
- **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).
- **Time set** – la fuente del reloj del equipo (por defecto **Cloud application**, la nube Protegus).

E16T anterior

En el E16T anterior, la página System settings tiene además otros grupos:

- **General → Test period** – el informe de prueba periódico se envía con el intervalo indicado aquí (en la v2 está en la pestaña **CMS reporting → Settings**).
- Grupo **Ethernet settings** (en la v2 es una página aparte, apartado 6.5): **Internal MAC** – el identificador único del equipo, la dirección MAC; **Use DHCP** – si lo marcas, el equipo se registra automáticamente en la red; si el registro automático no funciona, rellena a mano los campos **Internal IP address**, **Mask** (máscara de subred), **Gateway** (puerta de enlace) y **DNS**.

- Grupo **Output** (en la v2, la página IN/OUT, apartado 6.6): **OUT type** – el funcionamiento de la salida, de la lista: Disabled (desactivada), LAN OK (la red funciona), Communication Trouble (fallo de comunicación), Remote Control (control a distancia desde la aplicación Protegus); **Inverted** – si lo marcas, la salida funciona al revés; **OUT mode**: **Pulse** – la salida permanece en el nuevo estado durante el tiempo indicado en el campo **Pulse Time** (en segundos), **Level** – el estado se mantiene hasta la orden siguiente; **Pulse time** – la duración del impulso en segundos; en el modo Pulse, la salida se activa durante ese tiempo.

En el grupo **Access** se gestionan 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 IP. Los eventos pueden ir por varios canales: el canal **principal** y el **paralelo** funcionan a la vez (a dos receptores a la vez), y cada uno tiene un canal de **respaldo**, que entra en funcionamiento si se corta el canal correspondiente. La comunicación está cifrada y protegida con contraseña; para recibirla y transmitirla al software de la CRA hace falta un receptor Trikdis (receptor de software IPcom para Windows o Linux, receptor de hardware IP/SMS RL14, receptor multicanal RM14) o un receptor universal que admita los protocolos DC-09 / TL150.

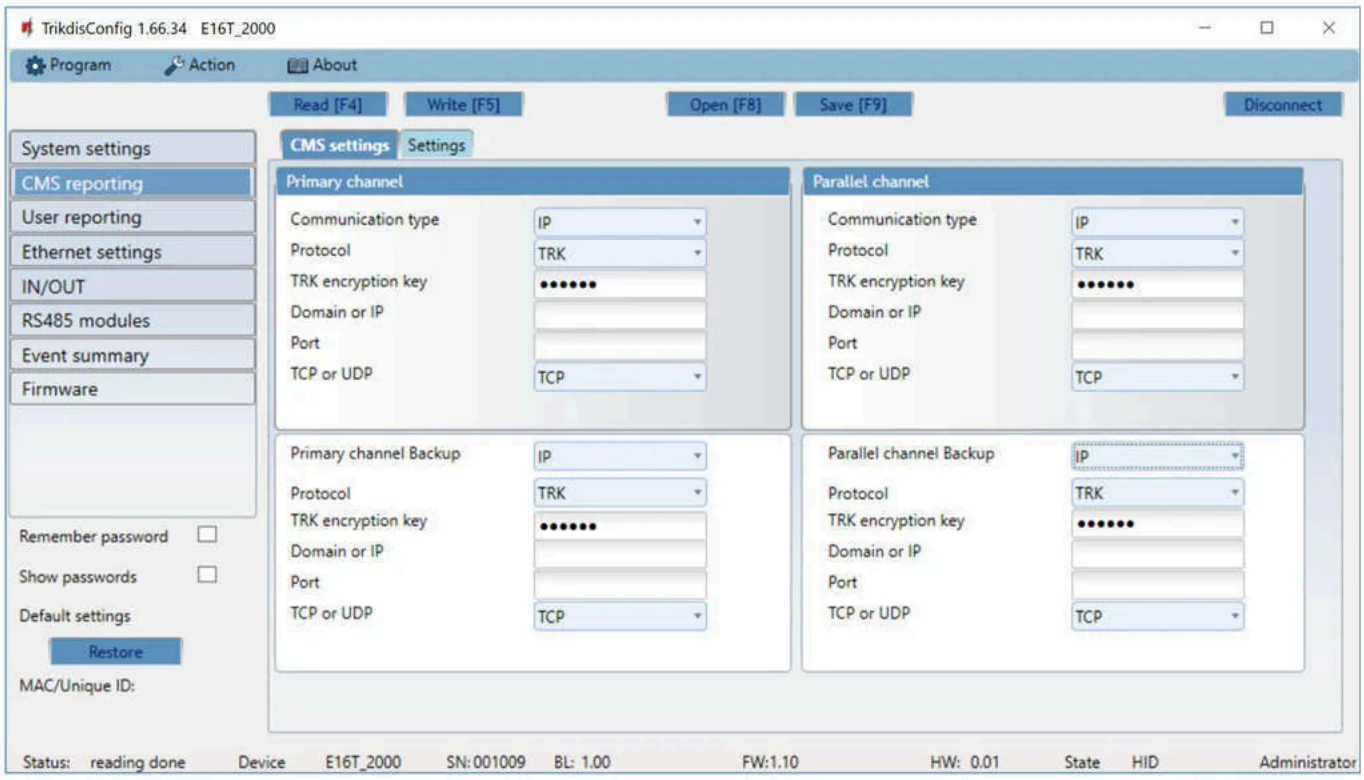


Figura 20. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal, de respaldo y paralelo.

Primary channel – canal principal

- **Communication type** – en el E16T solo se puede elegir **IP**.
- **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 del receptor (nombre de dominio o dirección IP) y su número de puerto de red.
- **TCP or UDP** – el protocolo de transporte con el que envía los eventos (según la configuración del receptor).

Primary channel Backup – canal de respaldo. Se encarga de la comunicación si el canal principal no funciona; su configuración es igual que la anterior. También en un equipo por cable conviene configurarlo, por ejemplo con una segunda dirección o un segundo puerto del receptor, porque el canal de respaldo también salva los fallos del lado del receptor.

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.

E16T anterior

En el E16T anterior, TrikdisConfig muestra lo mismo en la pestaña **CMS Reporting** de la ventana **Reporting**, con otros nombres de campo:

- Grupo **Primary**: **Enable** – si lo marcas, el canal principal hacia la CRA está activo; **Remote Host** – el nombre de dominio o la dirección IP del receptor; **Remote Port** – el número de puerto de red del receptor; **TCP or UDP** – el protocolo de transporte; **PING Time** – actívalo e indica el tiempo entre

señales de vida (valor de fábrica 30); hace falta para supervisar la conexión; **Encryption key** – clave de cifrado de 6 dígitos, la misma en el comunicador y en el receptor.

- Grupo **Backup**: **Enable** – activa el canal de respaldo, que envía si se corta la conexión principal; los demás campos son iguales que en el principal.
- Grupo **Settings**: **TCP protocol** – la codificación del envío: TRK (para receptor Trikdis), DC-09_2007 o DC-09_2012 (para receptor universal).
- Grupo **SIA IP parameter** – solo se puede modificar si en el campo **TCP protocol** está DC-09_2007 o DC-09_2012: **Encryption enabled** – con DC-09_2012 se puede activar el cifrado; **DC09-2012 encryption key** – la clave de cifrado configurada en el receptor; **DC09-2012 receiver No.** – el número del receptor; **DC-09 line No.** – el número de línea del receptor; **Use time stamp** – si lo marcas, el mensaje incluye también la hora (marca de tiempo).

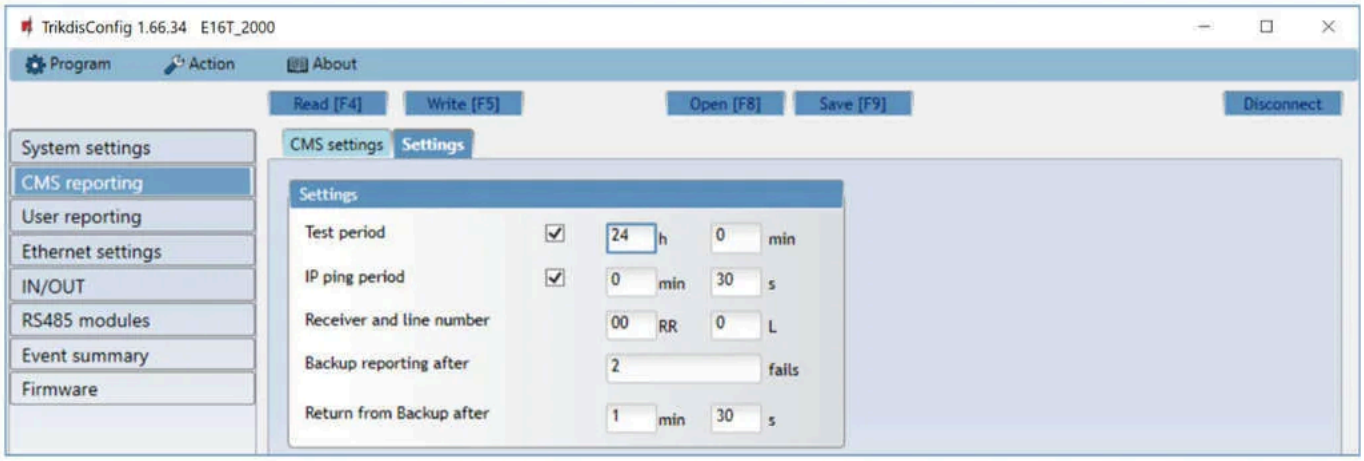


Figura 21. TrikdisConfig – CMS reporting, pestaña Settings: informe de prueba, PING, número de receptor y de línea (Receiver and line number: RR = número de receptor, L = número de línea) y temporizaciones del canal de respaldo.

En la pestaña **Settings** se configuran las temporizaciones y el número de receptor y de línea; el grupo DC-09 solo hace falta si envías con el protocolo DC-09 (en la captura de pantalla de 2022 todavía no aparece).

- **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.

6.4 User reporting

En la pestaña **PROTEGUS Cloud** se habilita el servicio Protegus. El E16T no tiene notificaciones ni control por SMS, por eso en esta página solo está esta pestaña.

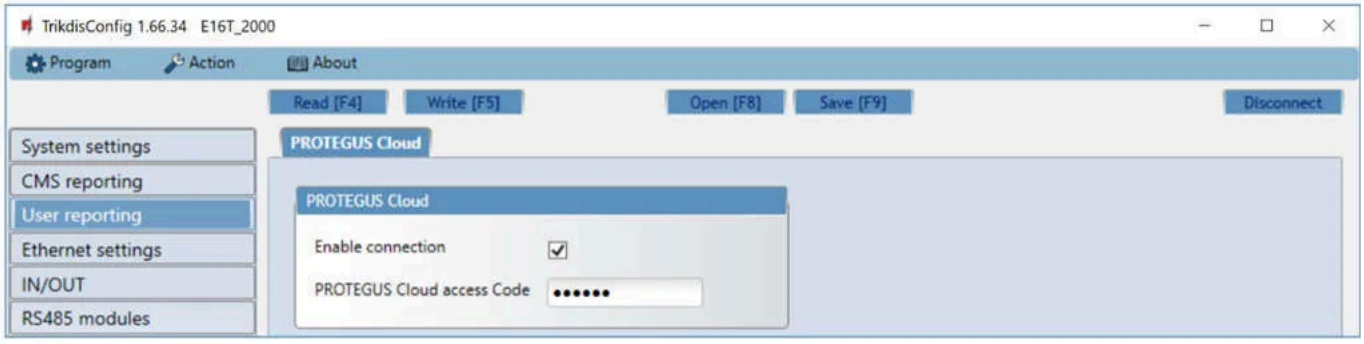


Figura 22. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

- **Enable connection** – habilita la conexión con la nube Protegus y el acceso a distancia de TrikdisConfig.
- **Protegus Cloud access code** – código de 6 dígitos para la conexión con Protegus (de fábrica `123456`). Si lo has cambiado, es el que hay que introducir al añadir el sistema en Protegus 2. Solo se puede configurar antes de crear el sistema en Protegus 2; después ya no se puede modificar.

6.5 Ethernet settings

Aquí indicas cómo se conecta el E16T a la red local.



Figura 23. TrikdisConfig – página Ethernet settings; de fábrica está activado el DHCP.

- **Use DHCP** – marcado, el dispositivo obtiene automáticamente la dirección IP, la máscara de subred y la puerta de enlace del servidor DHCP del router. Es el ajuste de fábrica y en la mayoría de los casos no hay que hacer nada más. Si en la red no hay DHCP, si el registro automático en la red falla o si el administrador de red pide una dirección fija, desmarca la casilla y rellena a mano los campos siguientes y los servidores de nombres:
- **Static IP** – dirección IP fija del dispositivo en la red local (una dirección que no use ningún otro dispositivo y que quede fuera del rango DHCP).
- **Subnet mask** – máscara de subred de la red.
- **Default gateway** – puerta de enlace predeterminada, normalmente la dirección del router. Con una puerta de enlace incorrecta, el dispositivo llega a la red local, pero no a Internet.

- **DNS 1, DNS 2** – servidores de nombres; a través de ellos el dispositivo encuentra la nube Protegus y el receptor indicado con nombre de dominio. De fábrica está configurado el DNS público de Google; si la red solo permite hacia fuera su propio servidor de nombres, escribe aquí la dirección del DNS local. 3 destellos del LED TROUBLE indican un error de DNS.

El identificador único del dispositivo, la dirección MAC (en el programa, **Internal MAC**), en la ventana más reciente de TrikdisConfig no aparece en esta página, sino en la parte inferior de la ventana, en el campo **MAC / Unique ID** de la barra de estado.

El dispositivo solo establece conexiones **salientes** hacia el receptor y la nube Protegus, por lo que en el router no hace falta abrir ni redirigir puertos, ni tampoco una IP pública fija.

En el E16T anterior, la dirección MAC aparece en el campo **Internal MAC** del grupo Ethernet settings de la página **System settings** (nota del apartado 6.2).

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).

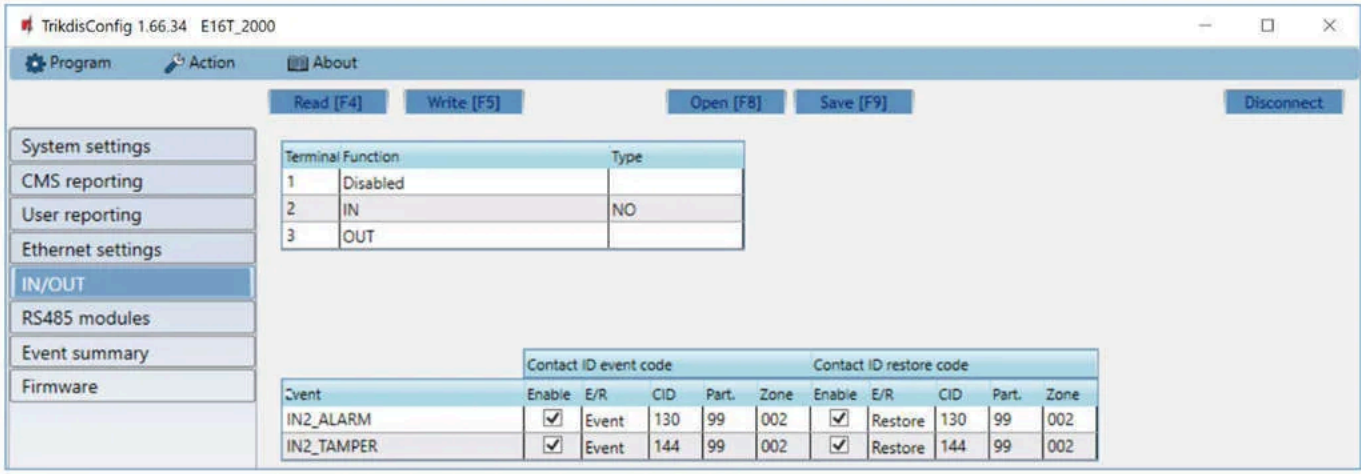


Figura 24. TrikdisConfig – página IN/OUT: función de los bornes de E/S y eventos de las entradas.

Cuando se activa el detector conectado a una entrada, el comunicador envía un evento propio (**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.

E16T anterior

En el E16T anterior no hay página IN/OUT: el tipo y los eventos de las dos entradas se configuran en el grupo **Input description** de la página **Event summary**. **Partition** – el número de partición; **Contact ID** – el código de evento (puede quedar el valor de fábrica); cuando se activa la entrada, envía este código a Protegus

y a la CRA; **Zone No.** – el número de zona, que va en los mensajes; **Type** – el tipo de entrada (NO, NC, EOL); **Enable / Alarm** – si lo marcas, transmite cuando se activa la entrada (evento); **Enable / Restore** – si lo marcas, transmite cuando la entrada se restaura. La configuración de la salida está en el grupo **System settings** → **Output** (nota del apartado 6.2).

6.7 RS485 modules

El iO-8 y los demás módulos de expansión de la serie iO conectados al bus RS485 hay que añadirlos en la pestaña **Modules list**.

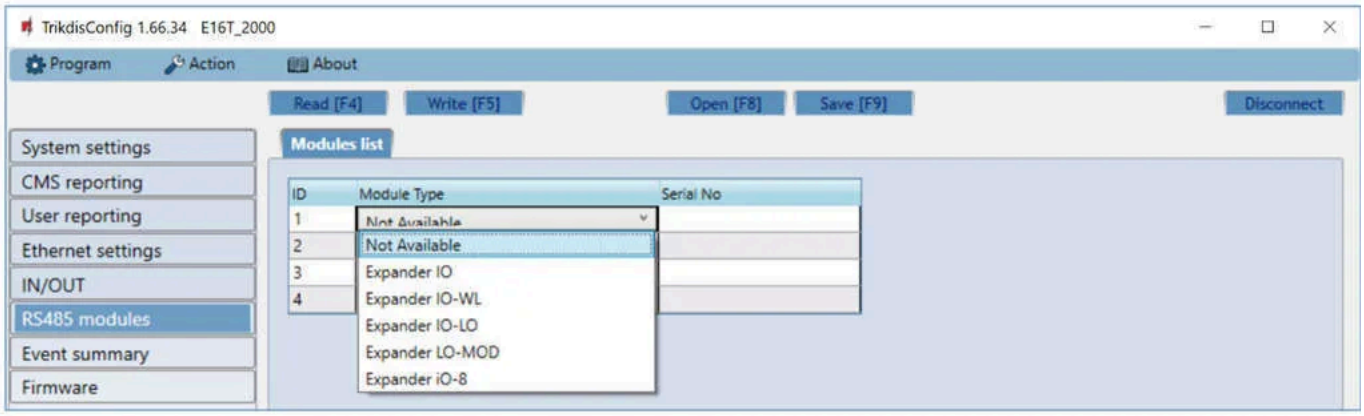


Figura 25. TrikdisConfig – RS485 modules, pestaña Modules list: los tipos de módulo disponibles.

- **Module Type** – el tipo del módulo conectado, de la lista (Expander iO-8, IO, IO-WL, IO-LO, LO-MOD).
- **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, numerada, del módulo.

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

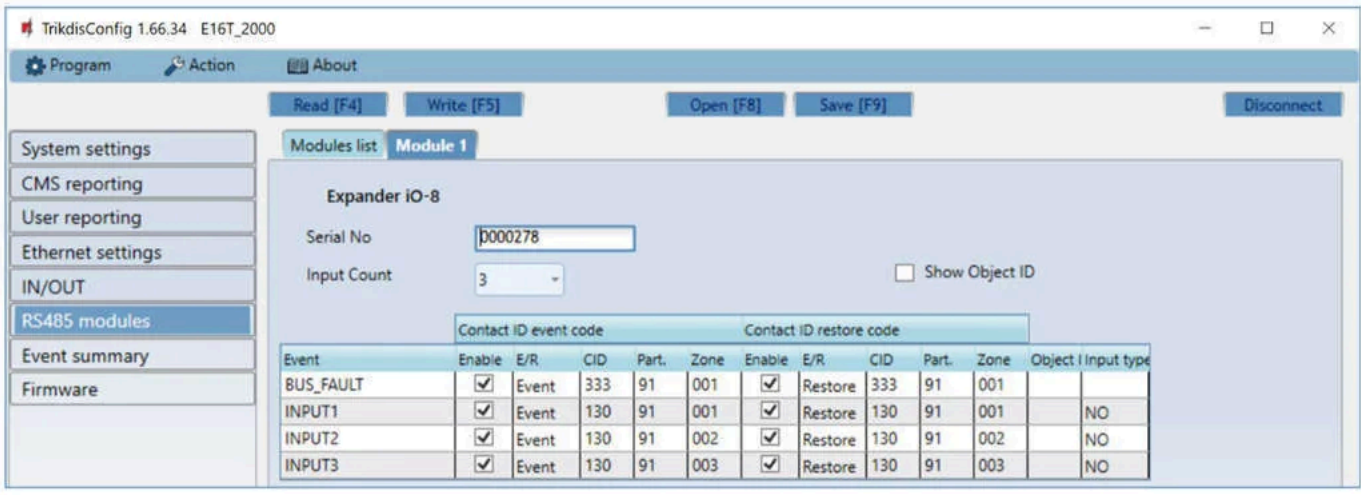


Figura 26. TrikdisConfig – RS485 modules, pestaña del módulo iO-8.

- **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 control de un dispositivo) se configura en la aplicación Protegus 2.

- En la tabla puedes asignar códigos 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**). 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 número de abonado distinto del del comunicador.

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**.

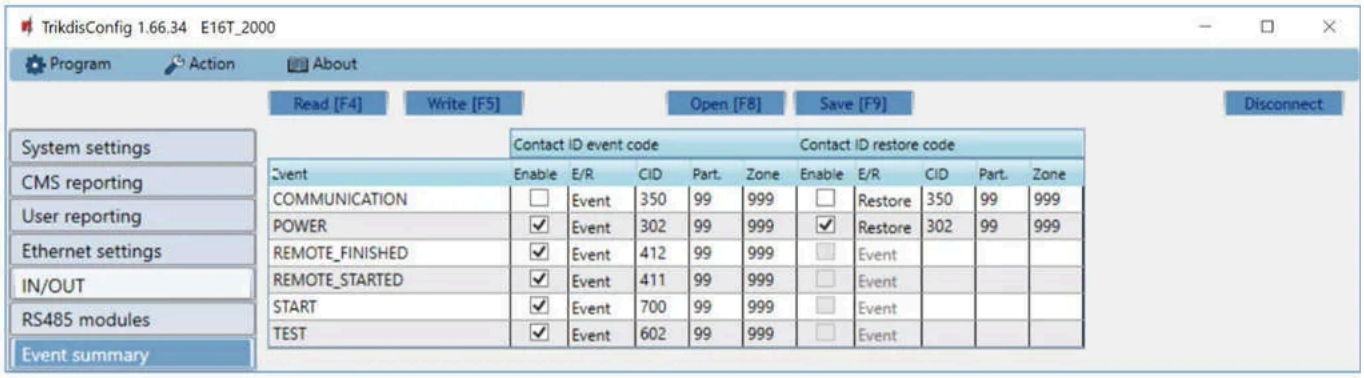


Figura 27. TrikdisConfig – página Event summary: los mensajes internos del equipo.

En el E16T anterior, la configuración de las entradas también está en esta página (nota del apartado 6.6).

6.9 Restablecimiento de 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.

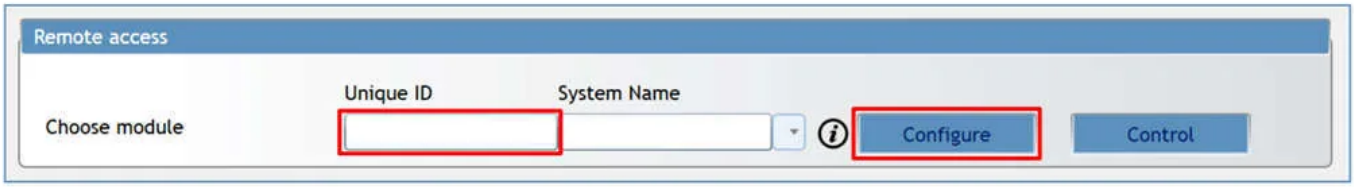


Figura 28. TrikdisConfig – Remote access: el identificador del equipo (en el E16T, la dirección MAC), el nombre del sistema y el botón Configure.

La habilitación del servicio Protegus se describe en el apartado 6.4 y la descarga de TrikdisConfig, en el apartado 2.1.

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.

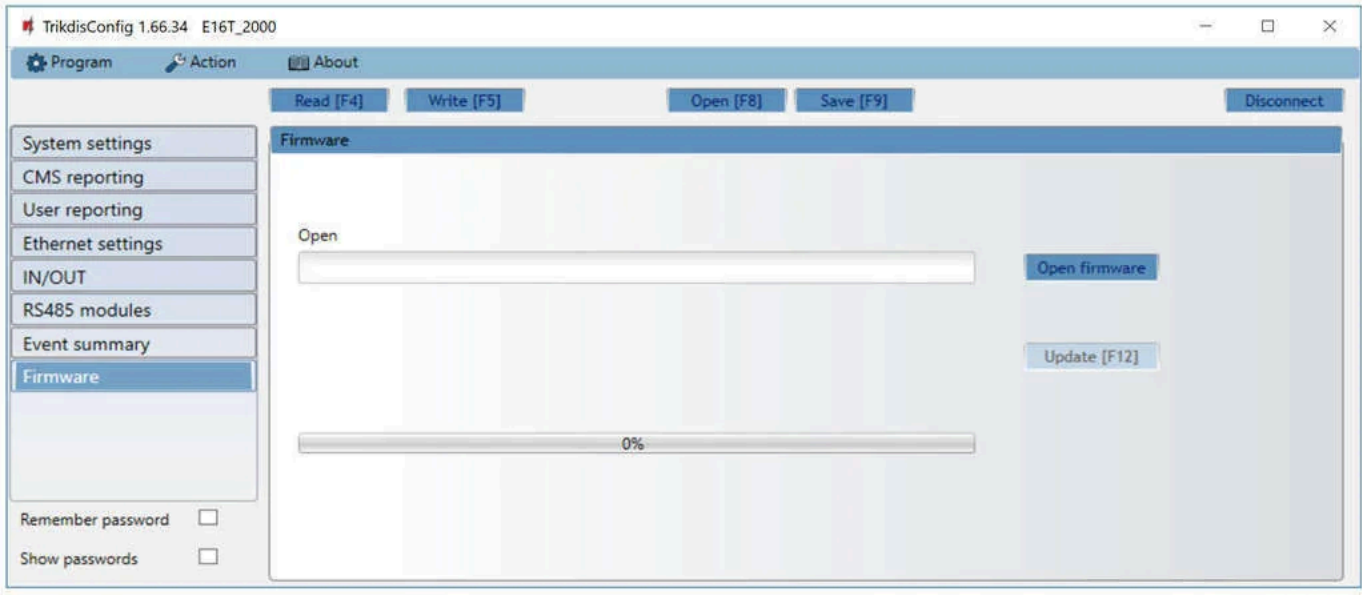


Figura 29. TrikdisConfig – página Firmware: Open firmware y Update [F12].

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 averías y preguntas frecuentes

Las preguntas y averías más frecuentes, partiendo de las indicaciones de los LED. Si la respuesta remite a un 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 conexión física, 2 = no ha recibido dirección IP (DHCP), 3 = error de DNS.
2. **Con 1 destello**, comprueba el cable y los conectores (si el RJ45 está bien encajado, hasta el clic), el puerto del router o del switch (si está activo y no está deshabilitado), y prueba con otro cable u otro puerto.
3. **Con 2 destellos**, en la red no hay servidor DHCP o no responde: actívalo en el router o asigna al equipo una dirección IP fija, una máscara y una puerta de enlace en la página **Ethernet settings** (apartado 6.5).
4. **Con 3 destellos**, la resolución de nombres no funciona: comprueba los campos DNS 1 / DNS 2 (de fábrica, el DNS público de Google) y que la red permita el tráfico DNS saliente.

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 la configuración DNS (**Ethernet settings**).
3. Con dirección IP fija, comprueba la puerta de enlace (**Default gateway**): con una puerta de enlace incorrecta, el equipo llega a la red local, pero no a internet.
4. En una red de empresa o filtrada, el cortafuegos puede bloquear la conexión saliente al puerto del receptor; acuérdalo con el administrador de red (apartado 3.2).

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 un 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 línea y no inicia la llamada, desactiva en ella la detección del tono de línea.
4. Si la central indica «fallo de comunicación» aunque el evento haya llegado, comprueba el ajuste **Wait acknowledgment from CMS** (apartado 6.2).

Protegus 2 no ve el equipo

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 equipo; una vez creado el sistema, ya no se puede modificar en el equipo.
3. Escribe la dirección MAC con exactitud, tal como aparece en la caja o en la parte trasera, o escanea el código QR de la etiqueta con la aplicación; así no hay errores de escritura.
4. La conexión a internet debe funcionar: el LED NETWORK está en verde y el LED DATA se apaga después de un evento. Para llegar a la nube Protegus también hace falta un DNS que funcione (**Ethernet settings**).

No puedo entrar a distancia con TrikdisConfig

1. El equipo debe estar en línea (LED NETWORK en verde, el LED DATA se apaga después de un evento) y la conexión 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 a distancia.
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.

¿Hace falta una dirección IP fija o redirigir puertos en el router?

No. El propio E16T inicia la conexión saliente hacia el receptor y la nube Protegus, por lo que no hacen falta ni una dirección IP pública fija, ni DNS dinámico, ni redirección de puertos. En la red local sirve la dirección obtenida por DHCP; asigna una dirección local fija solo si en la red no hay DHCP o si lo pide el administrador de red (apartado 6.5).

¿Funciona por WiFi?

No: el E16T solo admite conexión de red por cable (RJ45). Si cerca de la central no hay cable de red, se puede montar un puente WiFi hasta el router, o elegir el comunicador de red móvil G16T.

¿Qué pasa durante un corte de corriente?

El comunicador se alimenta de la batería de la central, pero si el router y el módem se quedan sin corriente, no hay internet y los eventos esperan en la memoria (el LED DATA está encendido). El equipo los envía cuando vuelve internet. Si la interrupción no es aceptable, la solución es un SAI para los equipos de red o un comunicador de red móvil (apartado 3.2).

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.

- La instalación y el mantenimiento del equipo 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 averías.
- Antes del cableado, en cada conexión eléctrica y antes de cualquier intervención de servicio, desconecta el equipo de la alimentación.
- Los fallos derivados de una instalación o un uso inadecuados, así como las modificaciones y reparaciones no autorizadas por el fabricante, anulan la garantía.
- Respeta la normativa local sobre residuos: no tires el equipo averiado ni sus componentes con 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.
- Documentación técnica: docs.trikdis.com.

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

Productos relacionados

Trikdis E16T Ethernet comunicador universal - módulo IP

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-e16t