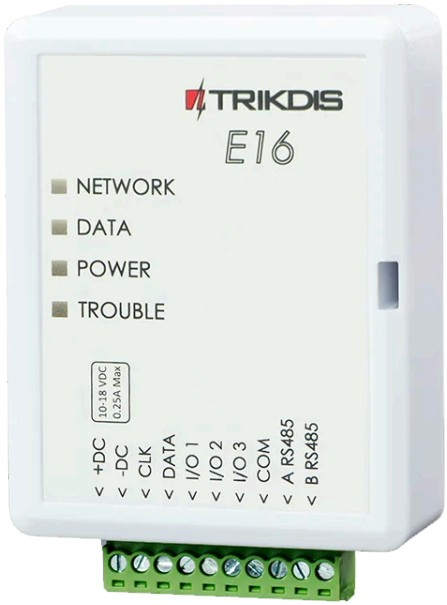
Comunicador E16 – manual de instalación y de usuario

Manual de instalación y de usuario del comunicador Ethernet Trikdis E16: conexión al bus de datos o al puerto serie de la central de alarma, programación de la central, configuración de red en TrikdisConfig, transmisión a la CRA, aplicación Protegus 2.



Edición: 2026-11-17
Versión web siempre actualizada: https://trikdis.es/manual-e16

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Centrales de alarma compatibles
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 Tipo de central y control directo
2.3 Conexión con la aplicación Protegus 2
2.4 Conexión con la CRA

3. Instalación y cableado

3.1 Pasos de la instalación
3.2 Ubicación y red
3.3 Conexión a la central de alarma
3.3.1 DSC PowerSeries
3.3.2 Paradox
3.3.3 UTC Interlogix (Caddx) NetworX
3.3.4 Texecom Premier / Premier Elite
3.3.5 Crow Runner
3.3.6 Pyronix
3.3.7 Honeywell Ademco Vista
3.3.8 InnerRange Inception e Integriti
3.4 Conexión de una zona de 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 del cable Ethernet
3.9 Encendido y primera comprobación
A TRIKDIS átjelző elindítása

4. Programación de la central de alarma

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

5. Control remoto con la aplicación Protegus 2

5.1 Añadir el equipo
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Control directo con el código de teclado

5.3 Armado con zona de interruptor de llave
5.4 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 Restablecer la configuración de fábrica

7. Programación a distancia

8. Comprobación del funcionamiento del comunicador

9. Actualización del firmware

10. Solución de problemas y preguntas frecuentes

11. Normas de seguridad

Ver también

1. Descripción general

El E16 es el **comunicador Ethernet de conexión directa** de Trikdis: no se conecta a la salida de línea telefónica de la central de alarma, sino a su **bus de teclados o a su puerto serie**. Lee los eventos directamente de la central –junto con el número de zona, de partición y de usuario– y los transmite por la red local, a través de una conexión a internet por cable, al receptor de la CRA y a la nube Protegus, a la aplicación del usuario. Funciona con las centrales compatibles de DSC, Paradox, UTC Interlogix (Caddx), Texecom, Pyronix, InnerRange, Honeywell y Crow; en los modelos de **control directo**, el usuario arma y desarma desde la aplicación Protegus 2 con su propio código de teclado, sin necesidad de una zona de interruptor de llave aparte. Para centrales de otras marcas que solo tienen salida de línea telefónica, el adecuado es el comunicador Ethernet E16T (TIP/RING); donde no hay internet por cable, el comunicador de red móvil G16.

1.1 Para qué sirve y cómo funciona

- **Lee la central directamente.** Por el bus de la central, cada evento llega al comunicador al instante, con la numeración propia de la central; no hace falta configurar el marcador telefónico de la central, ni hay marcación Contact ID.
- **Transmite a la CRA.** Envía los eventos por conexión IP a un receptor Trikdis de software o de hardware (protocolo TRK; los receptores Trikdis funcionan con cualquier software de CRA) o a cualquier receptor universal (SIA DC-09 2007/2012, SUR-GARD TL150). Con un receptor SUR-GARD, el comunicador convierte los códigos Contact ID recibidos de la central en códigos SIA; la tabla de conversión está en el anexo de la documentación en inglés de docs.trikdis.com. Por defecto comprueba la conexión cada 30 segundos (el intervalo se puede cambiar, apartado 6.3) y, si hay un fallo, cambia al canal de respaldo; con un canal paralelo, los eventos se pueden enviar a dos receptores a la vez.
- **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 dispositivos conectados (iluminación, puerta, calefacción, ventilación, sistema de riego, etc.). Protegus 2 funciona con las centrales de todos los fabricantes compatibles con el E16.
- **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 ambas. Si las dos están configuradas, envía el evento primero a la CRA y después al usuario.
- **No necesita tarjeta SIM ni contrato de datos móviles.** El equipo usa la conexión a internet que ya existe en el lugar: se conecta al router o al switch con un cable Ethernet, por defecto obtiene la dirección por DHCP y solo establece conexiones salientes, por lo que no hace falta abrir puertos en el router.
- **Tiene entradas y salidas propias.** Tres bornes I/O de doble función se pueden usar como entrada (detector, sabotaje) o como salida controlable (zona de interruptor de llave, relé). Con el expansor iO-8 conectado al bus RS485 se pueden añadir 8 I/O más al sistema.

La estructura del sistema se muestra en la figura siguiente: el bus de la central de alarma se conecta al E16, el E16 accede a internet a través del router y, desde allí, a la nube Protegus y al receptor de la CRA; el usuario ve el sistema en la aplicación Protegus 2.

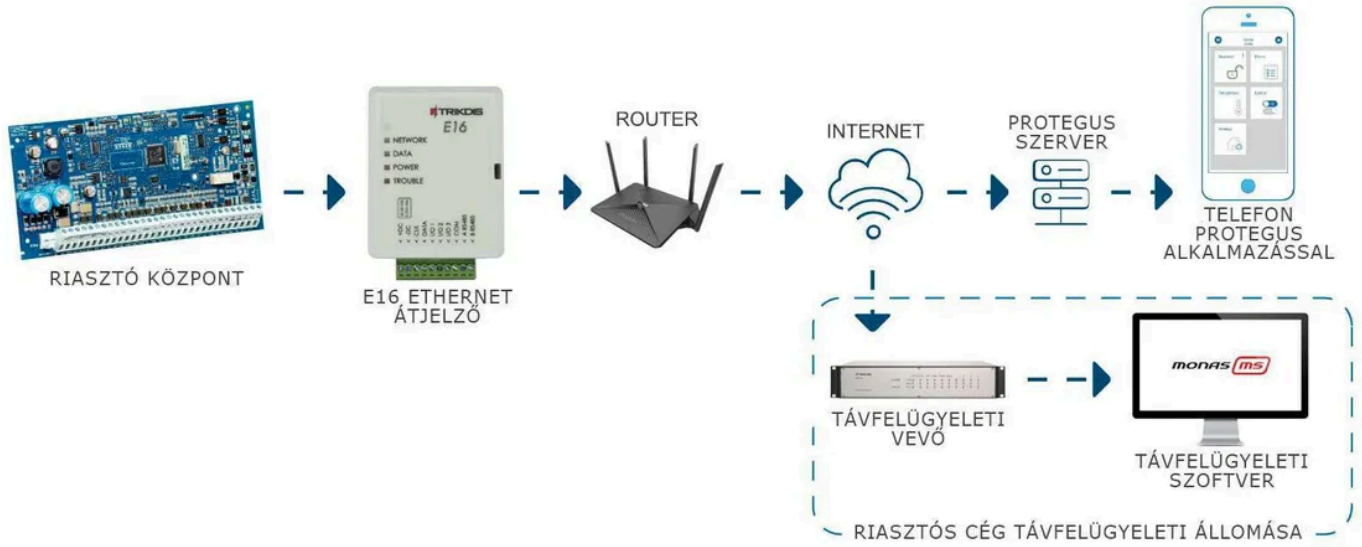


Figura 1. El E16 en el sistema: central de alarma (bus de teclados o puerto serie) → comunicador Ethernet E16 → router → internet → nube Protegus y receptor de la CRA → teléfono del usuario con la aplicación Protegus 2 y software de CRA de la empresa de seguridad.

1.2 Centrales de alarma compatibles

El E16 se puede conectar a las centrales siguientes. En los modelos de **control directo**, el armado y desarmado se hace desde la aplicación con el código de teclado; en los demás, con una zona de interruptor de llave (apartado 3.4). Para el control directo de las centrales Paradox, el firmware de la central debe ser como mínimo **V.4**; en los modelos Paradox más recientes (SP+, MG5050+, EVOHD+) el puerto serie viene bloqueado de fábrica y hay que desbloquearlo antes de usarlo.

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

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

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

Soros port feloldás útmutató

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

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

Además, se puede usar con las centrales **Pyronix MATRIX 424, MATRIX 832, MATRIX 832+, MATRIX 6 y MATRIX 816**, así como con las **Paradox DIGIPLEX NE96 y EVO96**.

La lista cambia de vez en cuando; el estado más actual está en el buscador de compatibilidad. El E16 **no funciona** con las centrales **DSC PowerSeries NEO**: el fabricante de la NEO no permite dispositivos externos en su bus; consulta DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones.

1.3 Características principales

Conexión con la central de alarma

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

Conexión de red

- Conexión Ethernet (IEEE 802.3, 10Base-T, RJ45) a la red local; por defecto obtiene la dirección por DHCP, también se puede configurar una IP fija.
- Solo establece conexiones salientes hacia el receptor y la nube Protegus: no hace falta abrir puertos, ni tener IP pública ni tarjeta SIM.

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, cada uno con su propio receptor de respaldo; con el canal paralelo, los eventos van a dos receptores a la vez.
- Mensajes cifrados (AES-128); memoria de 60 eventos.

Funciones para el usuario

- Aplicación móvil y web Protegus 2: notificaciones, lista de eventos, armado y desarmado, accionamiento de salidas.
- Derechos de usuario de 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.
- Se puede configurar y actualizar a distancia con el programa TrikdisConfig.

1.4 Partes del comunicador

El circuito impreso del E16 va en una caja de plástico blanca; la tapa frontal se puede quitar y el bloque de bornes es extraíble. El conector Ethernet está en el circuito impreso; el cable entra por la abertura de la caja.

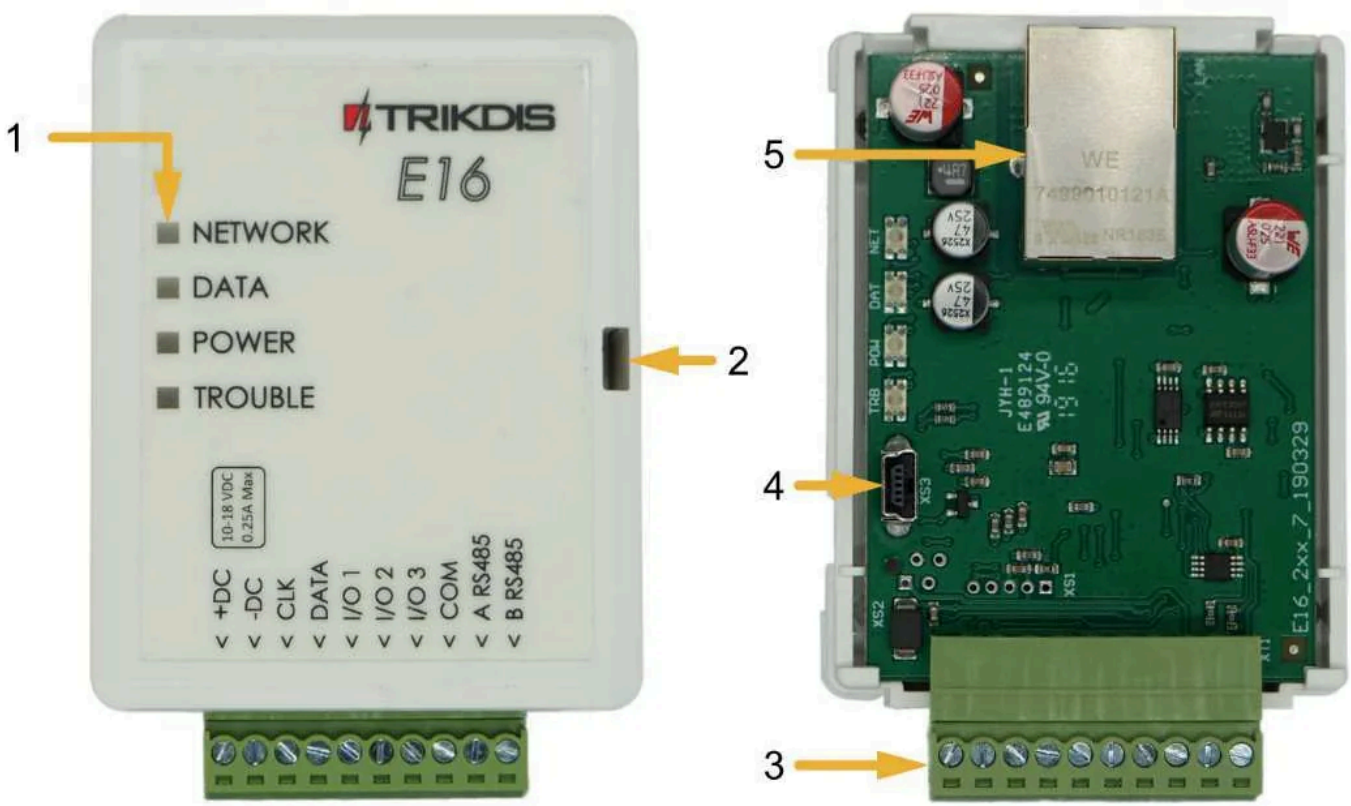


Figura 2. Partes del E16, vistas de frente y con la caja abierta.

- 1 Indicadores LED (NETWORK, DATA, POWER, TROUBLE)
- 2 Ranura para retirar la tapa frontal
- 3 Bloque de bornes extraíble
- 4 Conector USB Mini-B para la programación
- 5 Conector Ethernet (RJ45)

El bloque de bornes es extraíble: así el equipo 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 el equipo al ordenador.

1.5 Bornes

Borne	Función
+DC	Alimentación, +10–18 V DC
–DC	Alimentación, negativo
CLK	Línea de reloj / serie del bus de la central
DATA	Línea de datos del bus de la central

Borne	Función
I/O 1	Entrada/salida 1 (por defecto: entrada, NO)
I/O 2	Entrada/salida 2 (por defecto: entrada, NO)
I/O 3	Entrada/salida 3 (por defecto: salida)
COM	Punto común (negativo) de entradas y salidas
A RS485	Hilo A del bus RS485
B RS485	Hilo B del bus RS485

La serigrafía de los bornes aparece también en la tapa frontal, así que no hace falta quitarla para el cableado. A qué borne de la central van CLK y DATA depende del fabricante: los esquemas de conexión están en el apartado 3.3.

1.6 Indicaciones de los LED

Los LED de la tapa frontal son la herramienta más importante para la puesta en marcha y la solución de problemas. Léelos en conjunto: POWER indica la alimentación, NETWORK la conexión de red, DATA el tráfico de datos y TROUBLE los fallos.

NETWORK – conexión de red

Indicación	Significado
apagado	No hay conexión con la red (falta el cable, el router o la dirección IP; el LED TROUBLE indica cuál)
verde fijo	Conectado a la red

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 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 – alimentación

Indicación	Significado
apagado	No hay alimentación, o la alimentación está desconectada

Indicación	Significado
verde fijo	Encendido, la tensión de alimentación es correcta
amarillo fijo	Tensión de alimentación inadecuada (11,5 V como máximo)
verde fijo, amarillo intermitente	Listo para la programación (cable USB conectado)
amarillo fijo (durante la programación)	No hay conexión con el ordenador

TROUBLE – fallo

Indicación	Significado
apagado	Sin fallos
1 destello rojo	No hay conexión física con la red (PHY link): el cable no está conectado o el puerto del router / switch no está activo
2 destellos rojos	Error de DHCP: el equipo no ha obtenido dirección IP
3 destellos rojos	Error de DNS: no puede resolver el nombre de dominio del receptor o de la nube Protegus
6 destellos rojos	No hay conexión con el receptor de la CRA y/o con el servidor Protegus (la causa también puede ser la conexión a internet o el cortafuegos)
7 destellos rojos	Se ha perdido la conexión con la central de alarma (conexión por bus o serie)
rojo intermitente (durante la programación)	Error de memoria
rojo fijo (durante la programación)	Firmware dañado

1.7 Datos técnicos

Parámetro	Valor
Conexión con la central de alarma	bus de teclados o puerto serie, según el tipo de central (4 hilos: +DC, −DC, CLK, DATA)
Conexión de red	Ethernet, IEEE 802.3, 10Base-T, conector RJ45
Configuración de red	DHCP (por defecto) o dirección IP fija, máscara de subred, puerta de enlace, DNS
Entradas/salidas	3 I/O de doble función: como entrada NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (resistencia de fin de línea de 2,2 kΩ); como salida de colector abierto (OC), máx. 0,15 A / 30 V DC
Ampliación	hasta 4 expansores iO-8 en el bus RS485 (+8 I/O por expansor)
Tensión de alimentación	10–18 V DC
Consumo	100 mA nominal (en reposo); hasta 250 mA durante el envío
Protocolos de transmisión	TRK, DC-09_2007, DC-09_2012, TL150
Cifrado de mensajes	AES-128
Memoria de eventos	60 mensajes
Programación	TrikdisConfig (Windows) por cable USB Mini-B o a distancia

Parámetro	Valor
Condiciones 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 E16 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 · cable de al menos 4 hilos para el bus de la central – para el puerto serie Paradox, cable **CRP2** o **CRP2B**; para el puerto serie Texecom, cable **CRP4** · destornillador plano de 2,5 mm · cable Ethernet (CAT-5 o superior, máximo 100 m) hasta el router o el switch · manual de instalación de la central de alarma. Los cables y accesorios se compran por separado al distribuidor.

1. Descarga e instala el programa 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 E16. Introduce un destornillador plano en la ranura del borde superior de la tapa y, haciendo palanca hacia abajo, suelta la tapa con cuidado. La figura siguiente muestra la apertura y la posición del conector USB.

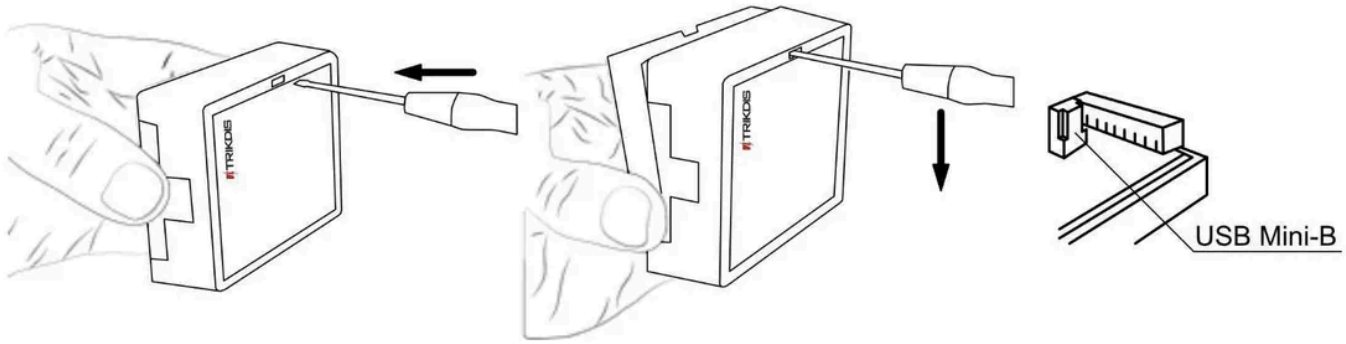


Figura 3. Apertura de la tapa frontal con un destornillador plano (izquierda, centro) y posición del conector USB Mini-B en el circuito impreso (derecha).

3. Conecta el E16 al ordenador con un cable USB Mini-B. El USB da alimentación suficiente para la programación; no hace falta una fuente aparte.

Advertencia

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

4. 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`).

2.2 Tipo de central y control directo

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

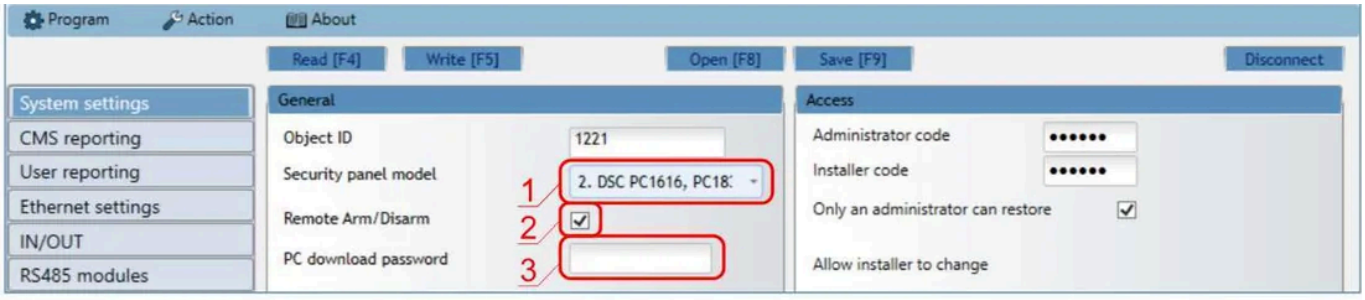


Figura 4. TrikdisConfig – página System settings, grupo General.

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

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

2.3 Conexión con la aplicación Protegus 2

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



Figura 5. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

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

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).

El E16 solo establece conexiones **salientes** hacia la nube Protegus y el receptor, por lo que no hace falta abrir ni redirigir puertos en el router. En una red de empresa filtrada por cortafuegos, acuerda el tráfico saliente con el administrador de red (apartado 3.2).

Si el equipo solo funciona con Protegus 2, sin CRA, la configuración ya está lista: pulsa el botón **Write [F5]** (escribir), espera la confirmación y desconecta el cable USB. Si también transmite a una CRA, sigue con el apartado 2.4.

2.4 Conexión con la CRA

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

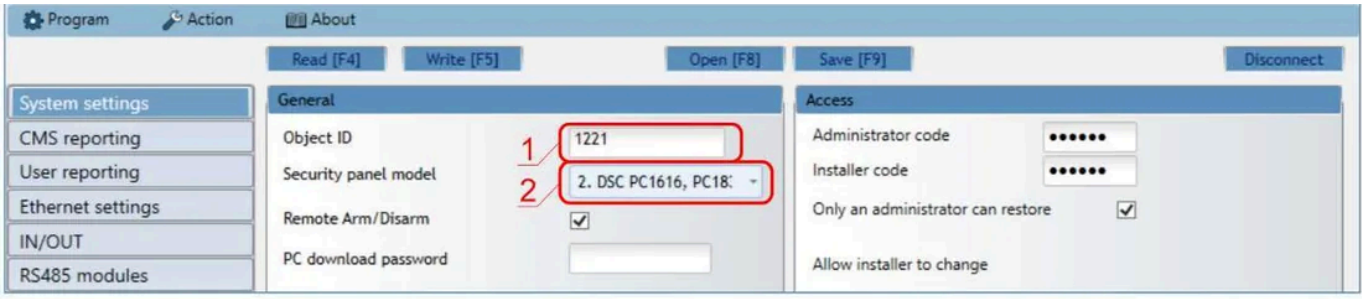


Figura 6. TrikdisConfig – página System settings, grupo General.

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

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

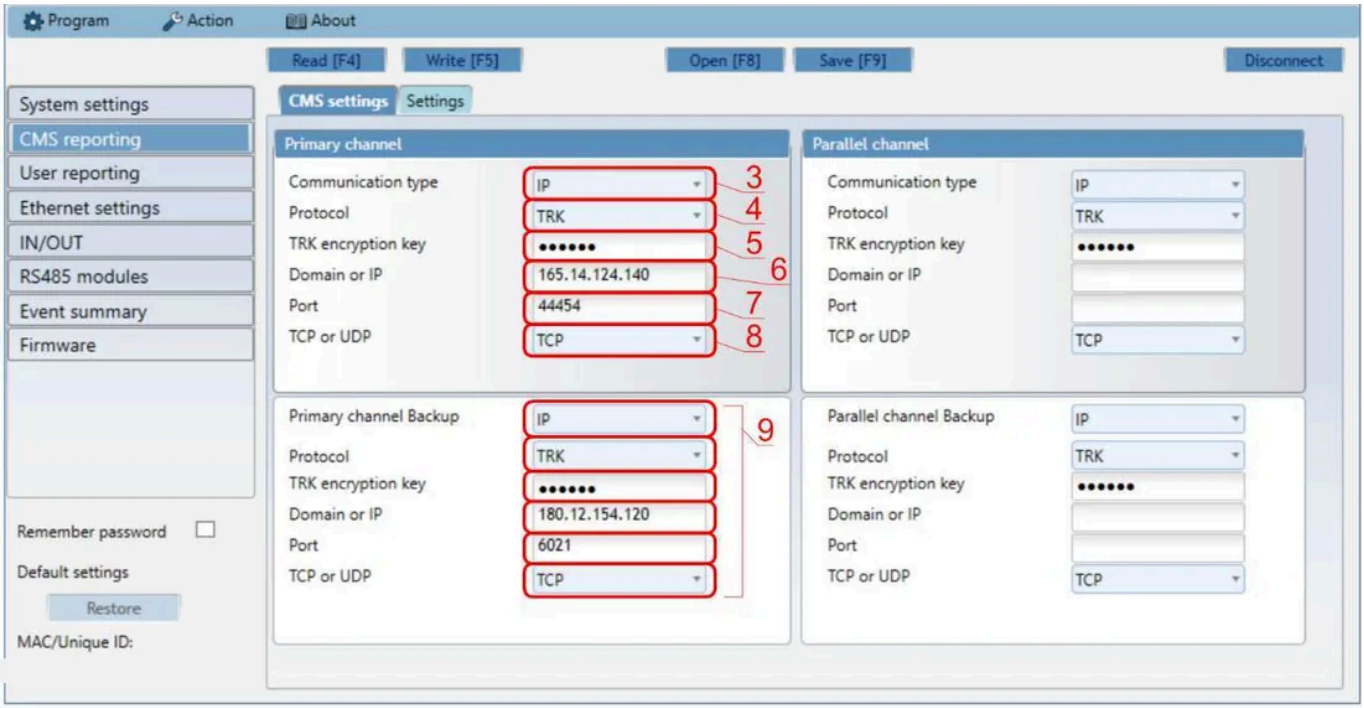


Figura 7. TrikdisConfig – CMS reporting, pestaña CMS settings.

- 3 **Communication type** – **IP** (en el E16 es la única opción).
- 4 **Protocol** – **TRK** para receptor Trikdis, **DC-09_2007** o **DC-09_2012** para receptor universal, **TL150** para receptor SURGARD.
- 5 **TRK encryption key** – la clave de cifrado de 6 dígitos configurada en el receptor.
- 6 **Domain or IP** – el nombre de dominio o la dirección IP del receptor.
- 7 **Port** – el número de puerto del receptor.
- 8 **TCP or UDP** – el protocolo de transmisión; se ajusta a la configuración del receptor.
- 9 **Primary channel Backup** – canal de respaldo para cuando falla el principal; rellénalo de la misma manera, se recomienda configurarlo.

También se recomienda configurar el **Parallel channel** (canal paralelo) y su canal de respaldo si los eventos deben llegar a dos receptores.

Con el protocolo **DC-09**, introduce en la pestaña **Settings** también el número de abonado, de línea y de receptor DC-09. Si indicas el receptor con un nombre de dominio, en la página **Ethernet settings** debe haber una dirección DNS que funcione (por defecto, el servidor de nombres público de Google).

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 cableado

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 apartado 2.1) y extrae el bloque 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 el bloque de bornes.
5. Conecta el cable Ethernet al conector RJ45 (apartado 3.8).
6. Vuelve a colocar la tapa frontal.

3.2 Ubicación y red

- Instala el comunicador en un lugar **seco e interior**, a ser posible cerca de la caja de la central de alarma, para que el cable del bus sea corto. Una caja metálica no le afecta: el E16 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 E16 se alimenta de la central de alarma, así que durante un corte de corriente sigue funcionando con la batería de la central; el router y el módem, en cambio, normalmente no, y sin ellos no hay internet. Si esto no es aceptable para el sistema, alimenta también los equipos de red con un SAI, o elige un comunicador de red móvil (G16).

3.3 Conexión a la central de alarma

El E16 se conecta a la central con **un máximo de cuatro hilos** (en el bus de Caddx y de Pyronix no se usa CLK): a los bornes **+DC** y **–DC** va la alimentación auxiliar de 12 V de la central (AUX), y a los bornes **CLK** y **DATA** los dos hilos de datos del bus de teclados o del puerto serie de la central. Qué borne de la central es cada uno depende del fabricante: conecta según los esquemas siguientes. Para las centrales con puerto serie (Paradox, Texecom) existe un cable original: un extremo encaja en el conector de la central y el otro se conecta al bloque de bornes del E16.

Durante el envío, el E16 puede consumir hasta 250 mA. Comprueba que la salida AUX de la central lo soporta junto con los demás dispositivos conectados. Como la alimentación la da la central, durante un corte de corriente la batería de la central alimenta también al comunicador. La mayoría de las centrales no se dañan si

se invierten los hilos de un dispositivo conectado al bus, pero invertir **+DC y −DC** puede destruir el comunicador: comprueba la polaridad antes de conectar.

Después del cableado hay que seleccionar el tipo de la central conectada en el campo **System settings** → **Security panel model** de TrikdisConfig (apartado 2.2); con algunos fabricantes también hay que configurar la central (capítulo 4).

3.3.1 DSC PowerSeries

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

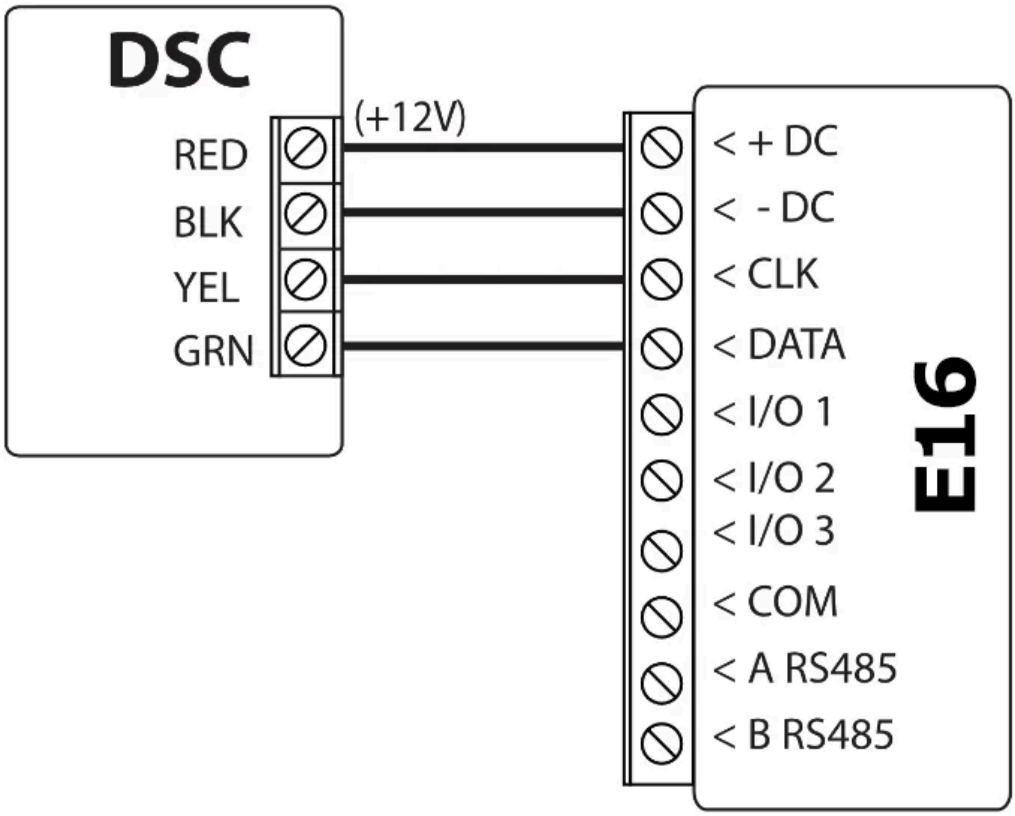


Figura 8. Conexión al Keybus de una central DSC PowerSeries (bus de teclados, «Keypad bus»): RED → +DC (+12 V), BLK → −DC, YEL → CLK, GRN → DATA.

3.3.2 Paradox

El comunicador se conecta al **puerto serie** (SERIAL) de las centrales Paradox con el cable original **CRP2** o **CRP2B**; el extremo del lado de la central encaja en el conector serie y el otro extremo se conecta al bloque de bornes del E16. Los 4 pines del conector: **4** → +DC (+12 V), **3** → −DC, **2** → CLK, **1** → DATA. Los colores de los hilos de los dos cables son distintos: el esquema muestra la asignación de colores de ambos. Marcado del conector serie de Paradox: AUX+ (→ +DC), GND (→ −DC), Tx (→ CLK), Rx (→ DATA).

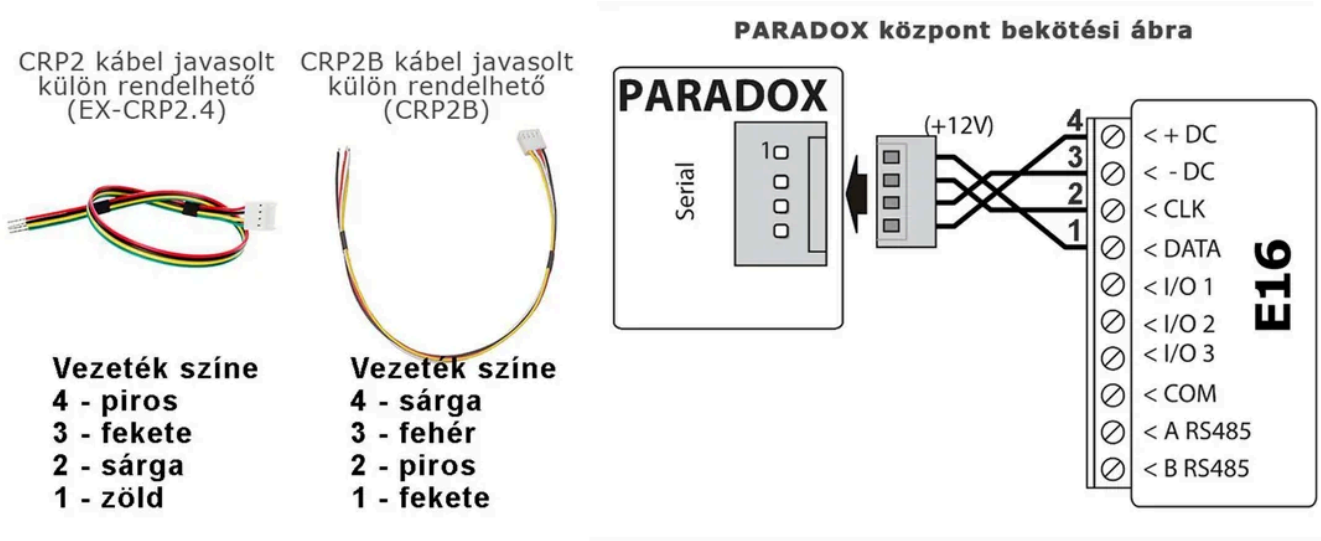


Figura 9. Conexión al puerto serie de una central Paradox con el cable CRP2 (EX-CRP2.4) o CRP2B. CRP2: 4 rojo → +DC, 3 negro → −DC, 2 amarillo → CLK, 1 verde → DATA. CRP2B: 4 amarillo → +DC, 3 blanco → −DC, 2 rojo → CLK, 1 negro → DATA.

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

3.3.3 UTC Interlogix (Caddx) NetworX

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

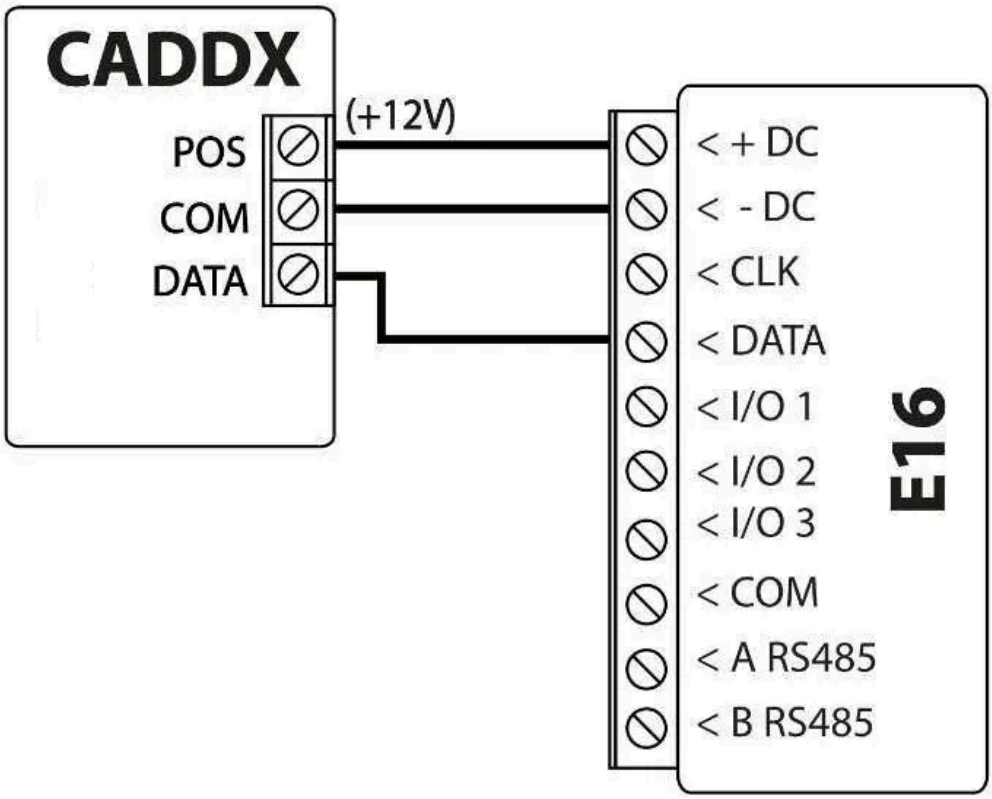


Figura 10. Conexión al bus de teclados de una central Caddx NetworX («Keypad bus»): POS → +DC (+12 V), COM → −DC, DATA → DATA; CLK queda libre.

3.3.4 Texecom Premier / Premier Elite

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

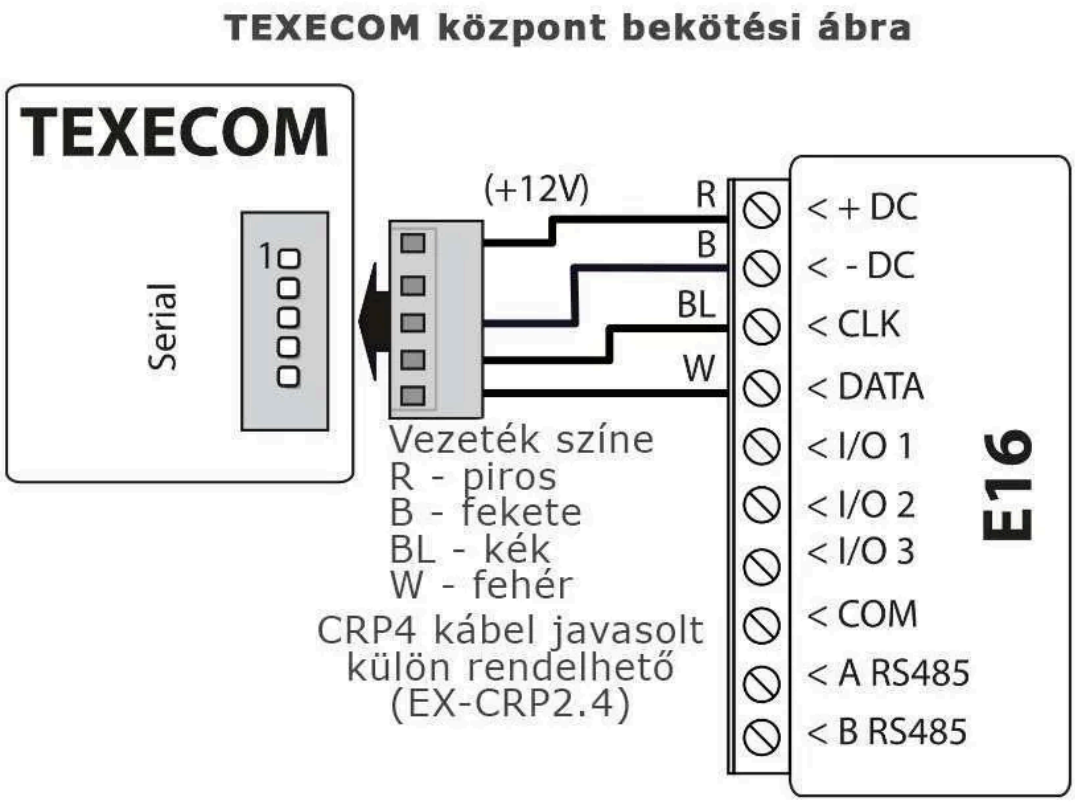


Figura 11. Conexión al puerto serie de una central Texecom con el cable CRP4: rojo → +DC, negro → −DC, azul → CLK, blanco → DATA.

3.3.5 Crow Runner

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

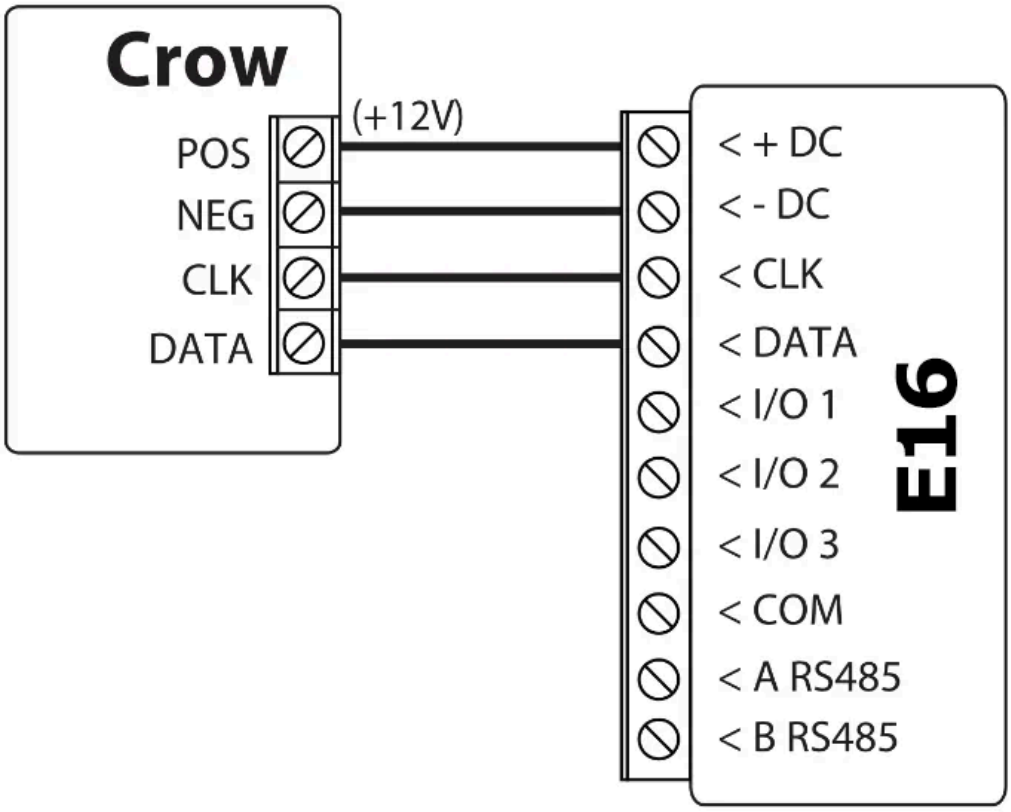


Figura 12. Conexión al bus de teclados de una central Crow Runner 4/8 o Runner 8/16 («Keypad bus»): POS → +DC, NEG → −DC, CLK → CLK, DATA → DATA.

3.3.6 Pyronix

Bus de teclados de las centrales Pyronix: **+AUX** → +DC, **−AUX** → −DC, **KD** → DATA. El borne **CLK** no se usa. Después del cableado y de la configuración del comunicador, desconecta la alimentación de la central y reiníciala para que acepte el comunicador (apartado 4.5).

3.3.7 Honeywell Ademco Vista

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

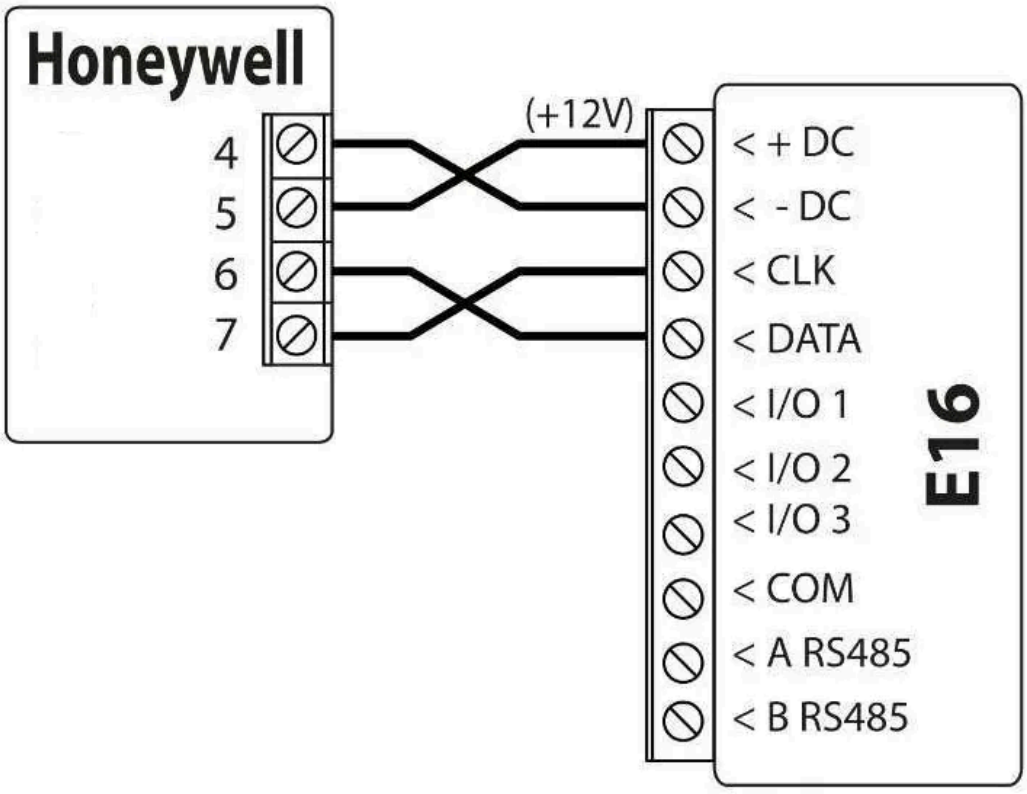


Figura 13. Conexión al bus de teclados de una central Honeywell Vista-20 / Vista-48 («Keypad bus»): 5 → +DC (+12 V), 4 → −DC, 7 → CLK, 6 → DATA.

3.3.8 InnerRange Inception e Integriti

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

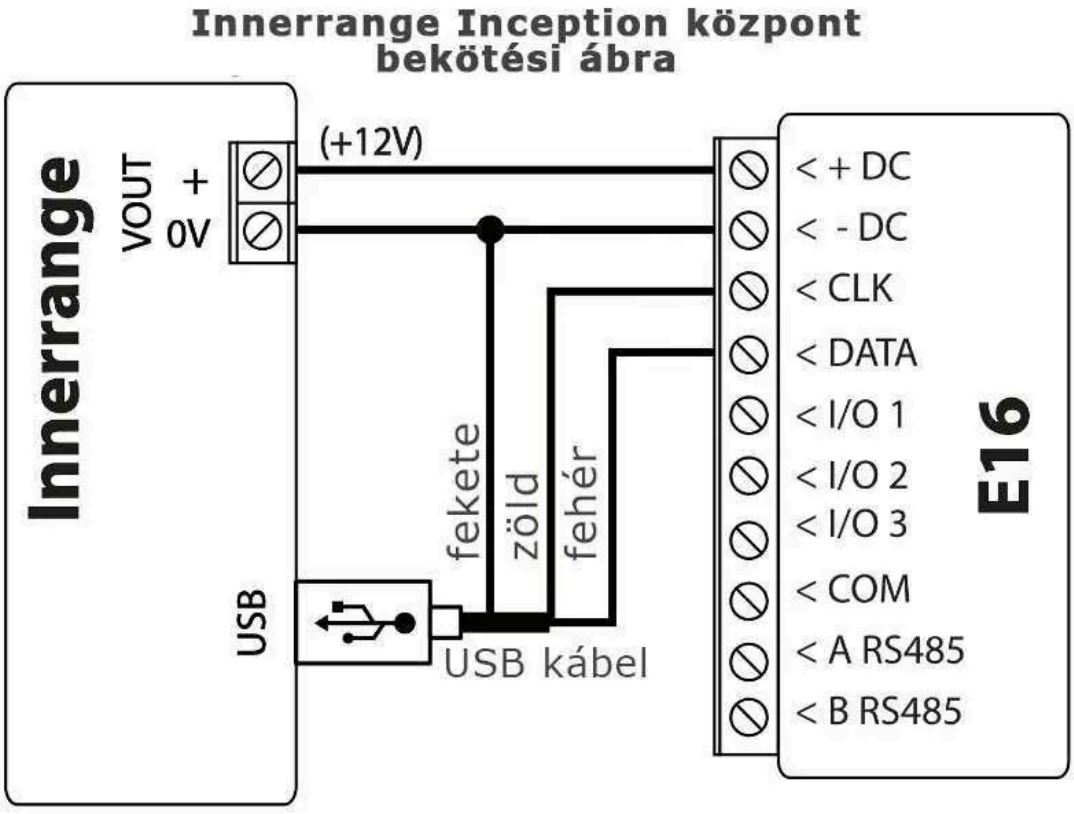


Figura 14. Conexión a una central InnerRange Inception: alimentación desde los bornes VOUT + y 0V, datos desde el puerto USB con el cable 993030USB (negro → 0V, verde → CLK, blanco → DATA).

A la central **Integriti** se conecta en el puerto 0 (Port 0) con el cable INTG-996795: **+DET** (+13 V) → +DC, **GND** (5) → −DC, **Rx** (3) → CLK, **Tx** (2) → DATA. El puerto serie de la central hay que configurarlo con el protocolo Trikdis (apartado 4.7).

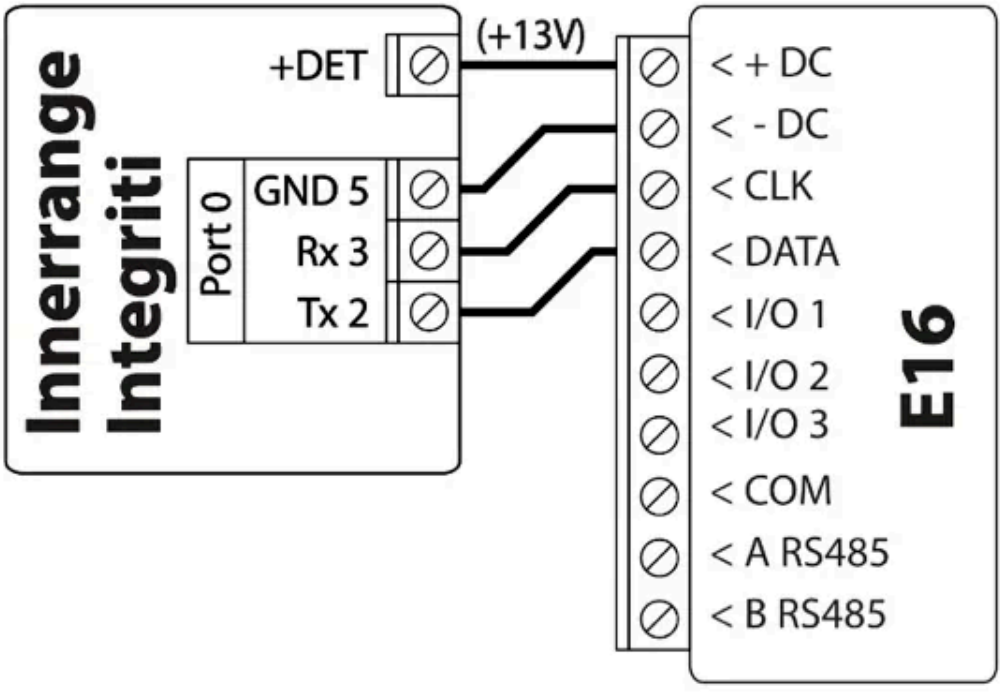


Figura 15. Conexión a una central InnerRange Integriti con el cable Inner Range de referencia INTG-996795: +DET (+13 V) → +DC, Port 0 GND (5) → −DC, Rx (3) → CLK, Tx (2) → DATA.

3.4 Conexión de una zona de interruptor de llave

Si la central no es de los modelos de control directo, o no quieres usar el control directo, el armado y desarmado a distancia se resuelve con una **zona de interruptor de llave**: configuras uno de los bornes I/O del comunicador como **salida** (página IN/OUT, apartado 6.6) y lo conectas 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 E16 tiene tres bornes I/O, se pueden controlar hasta tres particiones, cada una con su salida.

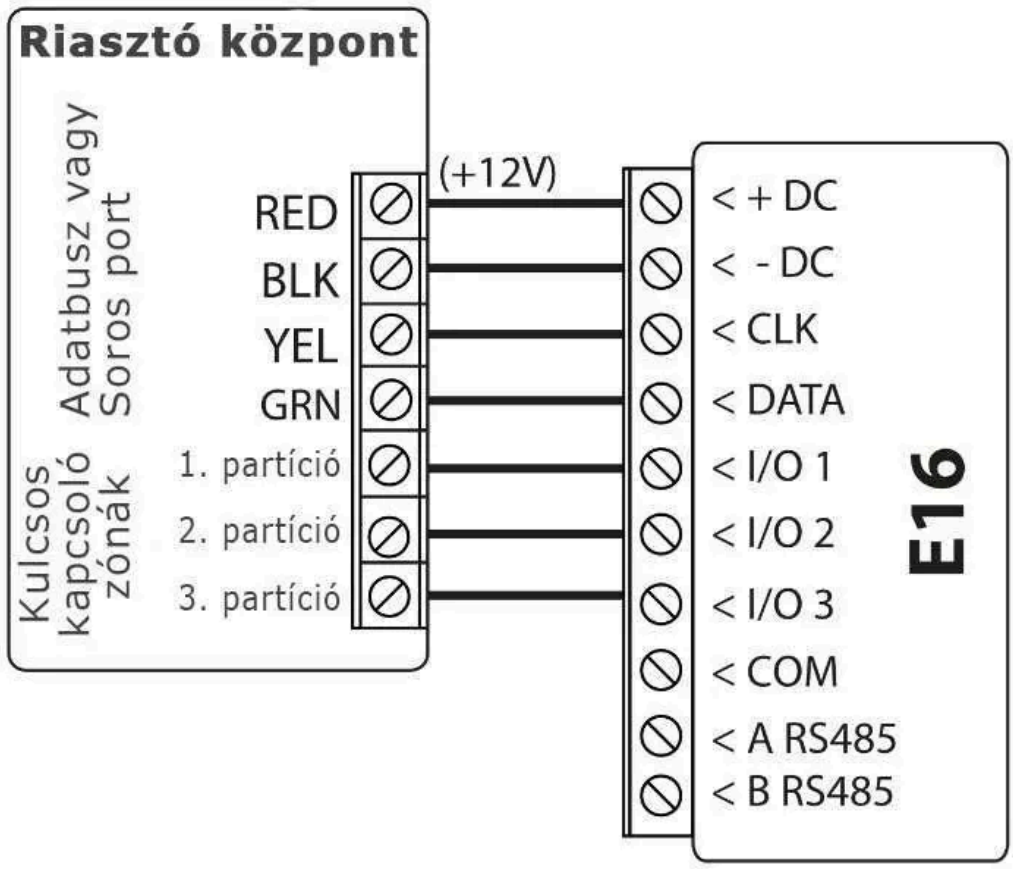


Figura 16. Armado y desarmado con zona de interruptor de llave: el comunicador lee los eventos del bus de la central, y las salidas I/O 1–3 accionan la zona de interruptor de llave de las particiones 1–3 de la central.

- En la página **System settings** de TrikdisConfig, **Remote Arm/Disarm** debe quedar **sin marcar**: las dos cosas no se pueden usar a la vez.
- La zona de interruptor de llave puede ser por impulso o biestable; en la aplicación Protegus 2 hay que configurar el mismo modo (apartado 5.3).

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 también se pueden usar como entradas para recibir otros detectores (p. ej., contacto de sabotaje, 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 NO, NC, NC/EOL, NO/EOL, NO/DEOL y NC/DEOL con resistencia de fin de línea de 2,2 kΩ; en los tipos DEOL, también con el circuito de sabotaje conectado.

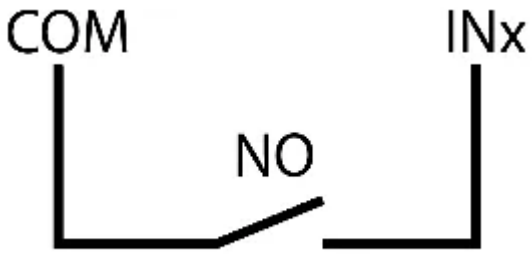


Figura 17. NO – circuito normalmente abierto: cerrado – alarma, abierto – reposo.

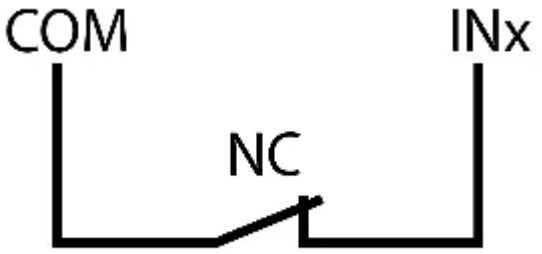


Figura 18. NC – circuito normalmente cerrado: abierto – alarma, cerrado – reposo.

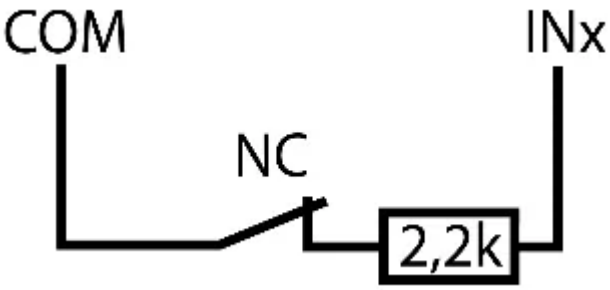


Figura 19. NC/EOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

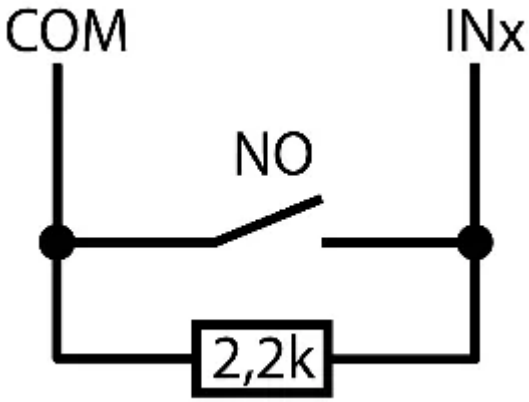


Figura 20. NO/EOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ: cortocircuito o corte – alarma, 2,2 kΩ – reposo.

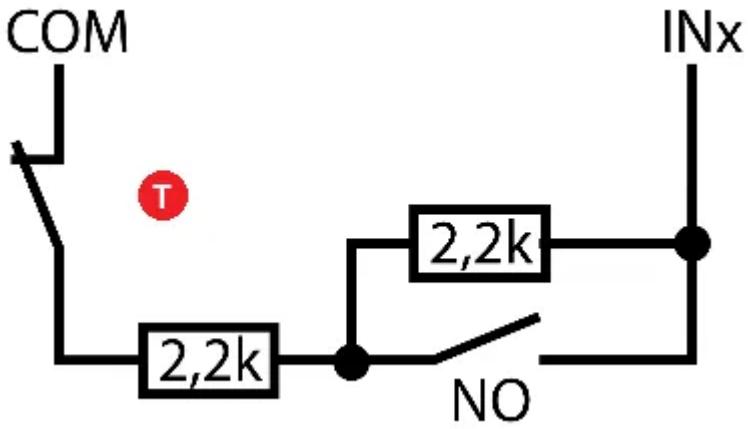


Figura 21. NO/DEOL – circuito normalmente abierto con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o corte – sabotaje, 2,2 kΩ – alarma, 3,3–5,5 kΩ – reposo.

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

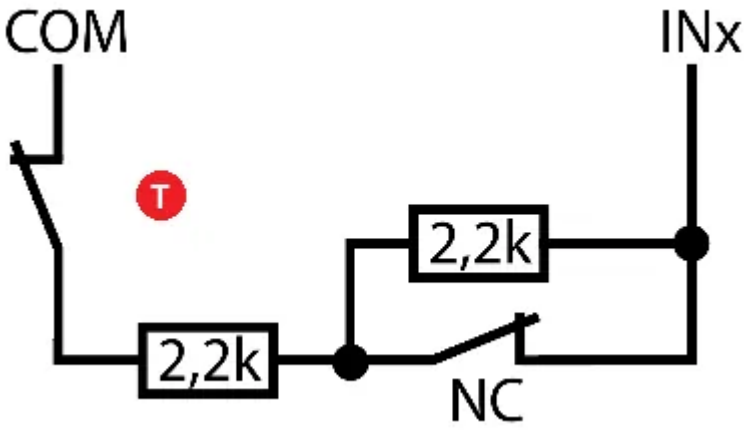


Figura 22. NC/DEOL – circuito normalmente cerrado con resistencia de fin de línea de 2,2 kΩ y detección de sabotaje: cortocircuito o corte – sabotaje, 2,2 kΩ – reposo, 3,3–5,5 kΩ – alarma.

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

3.6 Conexión de una salida con relé

Como salidas, los bornes I/O son de colector abierto (OC): en estado activo llevan la carga conectada al negativo, con un máximo de 0,15 A y hasta 30 V DC. Con los contactos del relé puedes encender y apagar distintos aparatos eléctricos. Los consumos mayores o los equipos a tensión de red conéctalos **a través de un relé**: un extremo de la bobina del relé va a +DC y el otro al borne I/O. El borne I/O usado hay que configurarlo como salida (**OUT**) en la página **IN/OUT** de TrikdisConfig (apartado 6.6).

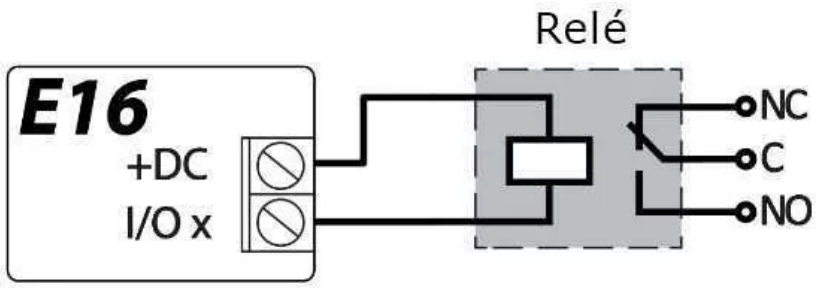


Figura 23. Conexión de un relé a la salida del comunicador: la bobina va entre +DC y el borne I/O x, y los contactos (NC, C, NO) conmutan la carga.

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

3.7 Conexión del expansor iO-8

Si hacen falta más entradas o salidas, al bus RS485 del E16 se pueden conectar expansores **iO-8**; cada uno añade 8 I/O de doble función más. Conecta los bornes A RS485 y B RS485 con los bornes A y B del módulo, y toma la alimentación del módulo de la salida AUX de 12 V de la central. El módulo hay que darlo de alta en la página **RS485 modules** de TrikdisConfig (apartado 6.7); los eventos de las entradas van a la CRA y a Protegus 2, y las salidas se pueden accionar desde la aplicación.

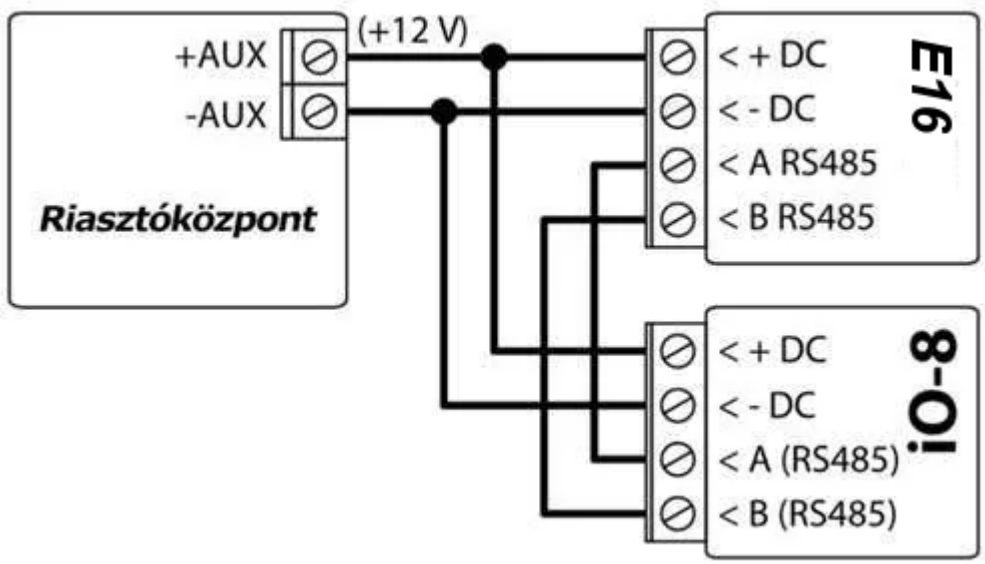


Figura 24. Conexión de un expansor iO-8 al bus RS485 del E16 (A RS485 → A, B RS485 → B); ambos equipos se alimentan de la salida AUX de la central de alarma (+12 V).

3.8 Conexión del cable Ethernet

Conecta un extremo del cable Ethernet al conector RJ45 del circuito impreso del E16 y el otro a un puerto libre del router o del switch. Hace falta un cable convencional de conexión directa (patch); el cable entra por la abertura de la caja. Tras el encendido, la luz verde del LED **NETWORK** indica que se ha establecido la conexión de red.

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 debes ver lo siguiente:

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

Cualquier otra combinación de LED indica algún fallo; identifica la causa con la tabla de LED del apartado 1.6. Si TROUBLE parpadea, el número de destellos indica la causa (apartado 1.6): 1 = no hay conexión física (cable, puerto), 2 = no ha obtenido dirección IP (DHCP), 3 = error de DNS, 6 = no llega al receptor o a la nube

Protegus. Los **7 destellos** indican que falta la conexión con la central: comprueba los hilos CLK y DATA, el tipo de central seleccionado y –donde haga falta– la programación de la central (capítulo 4). Si no se enciende ningún LED, comprueba la alimentación y el cableado.

4. Programación de la central de alarma

Este capítulo describe, por fabricante, qué hay que configurar en la central de alarma para que el E16 lea los eventos y, donde sea posible, controle la central a distancia. En la mayoría de las centrales no hay que programar nada para leer los eventos; para el **control directo**, marca la opción **Remote Arm/Disarm** en la página **System settings** de TrikdisConfig y, en centrales Paradox o Texecom, introduce también la contraseña PC o UDL de la central en el campo **Security panel PC download password** (apartados 2.2 y 6.2).

Si controlas la central no directamente, sino mediante una zona de interruptor de llave (apartado 3.4), **Remote Arm/Disarm** debe quedar sin marcar, y este capítulo solo se aplica a los ajustes necesarios para leer los eventos.

4.1 DSC

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

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

4.2 Paradox

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

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

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

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

Errores típicos y su solución

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

4.3 Texecom

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

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

Desde el teclado:

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

4.4 UTC Interlogix (Caddx)

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

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

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

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

4.5 Crow y Pyronix

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

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

4.6 Honeywell Ademco Vista

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

Entrada en la programación – de dos maneras:

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

Ajustes:

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

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

4.7 InnerRange Inception e Integriti

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

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

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

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

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

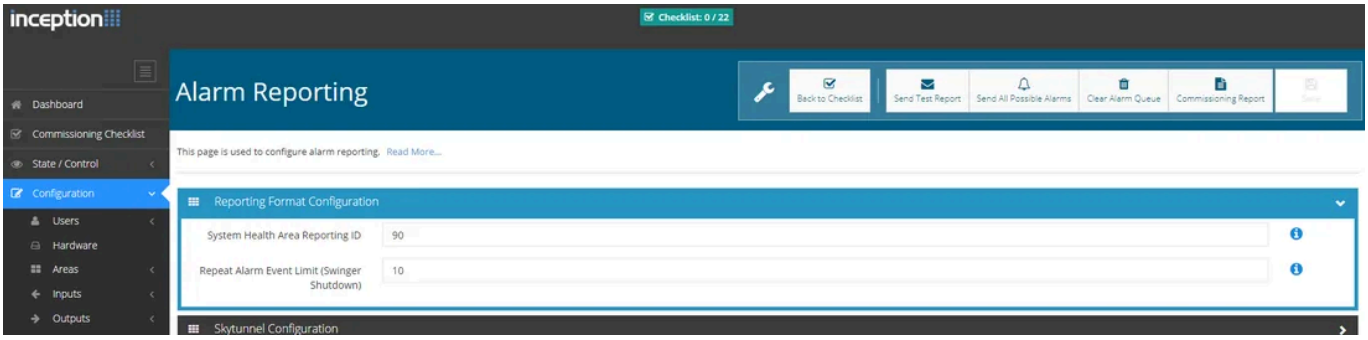


Figura 25. Interfaz web de Inception – Configuration → General → Alarm Reporting.



Figura 26. Inception – 3rd Party Device Configuration.

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

5. Control remoto 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 accionar las salidas del comunicador. Con el E16, el armado se puede hacer de dos maneras: en las centrales de **control directo**, el usuario usa su propio **código de teclado**; en las centrales conectadas con una zona de interruptor de llave, se hace con una **salida** del comunicador.

5.1 Añadir el equipo

Antes de añadir el equipo, comprueba lo siguiente:

1. El E16 está conectado a la red y tiene acceso a internet: el LED **NETWORK** está verde fijo y el LED **TROUBLE** no parpadea.
2. En la página **User reporting** → **PROTEGUS Cloud** de TrikdisConfig está marcado **Enable connection** y está configurado el **Protegus Cloud access code** (una vez creado el sistema, ya no se puede modificar).
3. El LED **POWER** está verde fijo.

El LED DATA es la forma más sencilla de comprobar Internet. El LED DATA se ilumina cuando en la memoria del dispositivo hay un mensaje pendiente de envío. El verde del LED NETWORK solo indica que la conexión de red se ha establecido –en un dispositivo de red móvil, que se ha registrado en la red del operador; en uno Ethernet, que la conexión hasta el router funciona–, pero no que el dispositivo también

salga a Internet. Si el LED NETWORK está en verde, pero el LED DATA sigue encendido de forma continua tras un evento o un informe de prueba, la conexión a Internet no funciona: el mensaje no puede salir. En red móvil lo más habitual es que fallen el APN o el servicio de datos de la tarjeta SIM; en Ethernet, el router, el cortafuegos o el DNS. Si el LED DATA se apaga, el mensaje se ha enviado y la conexión de datos está bien.

A rendszer létrehozása a Protegus 2 alkalmazásban

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

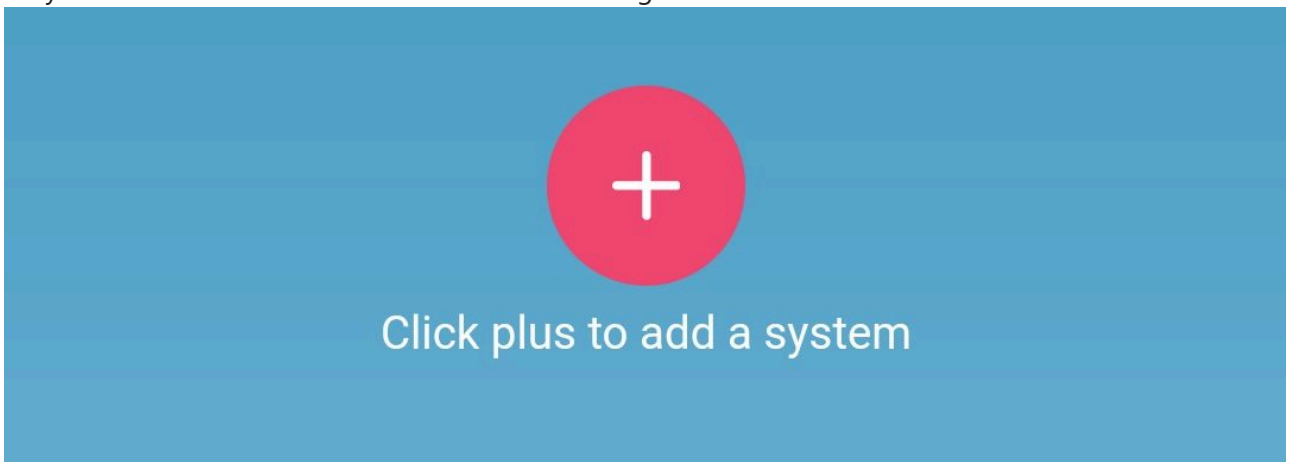
protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

WEB APP protegus
intelligent security & control

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

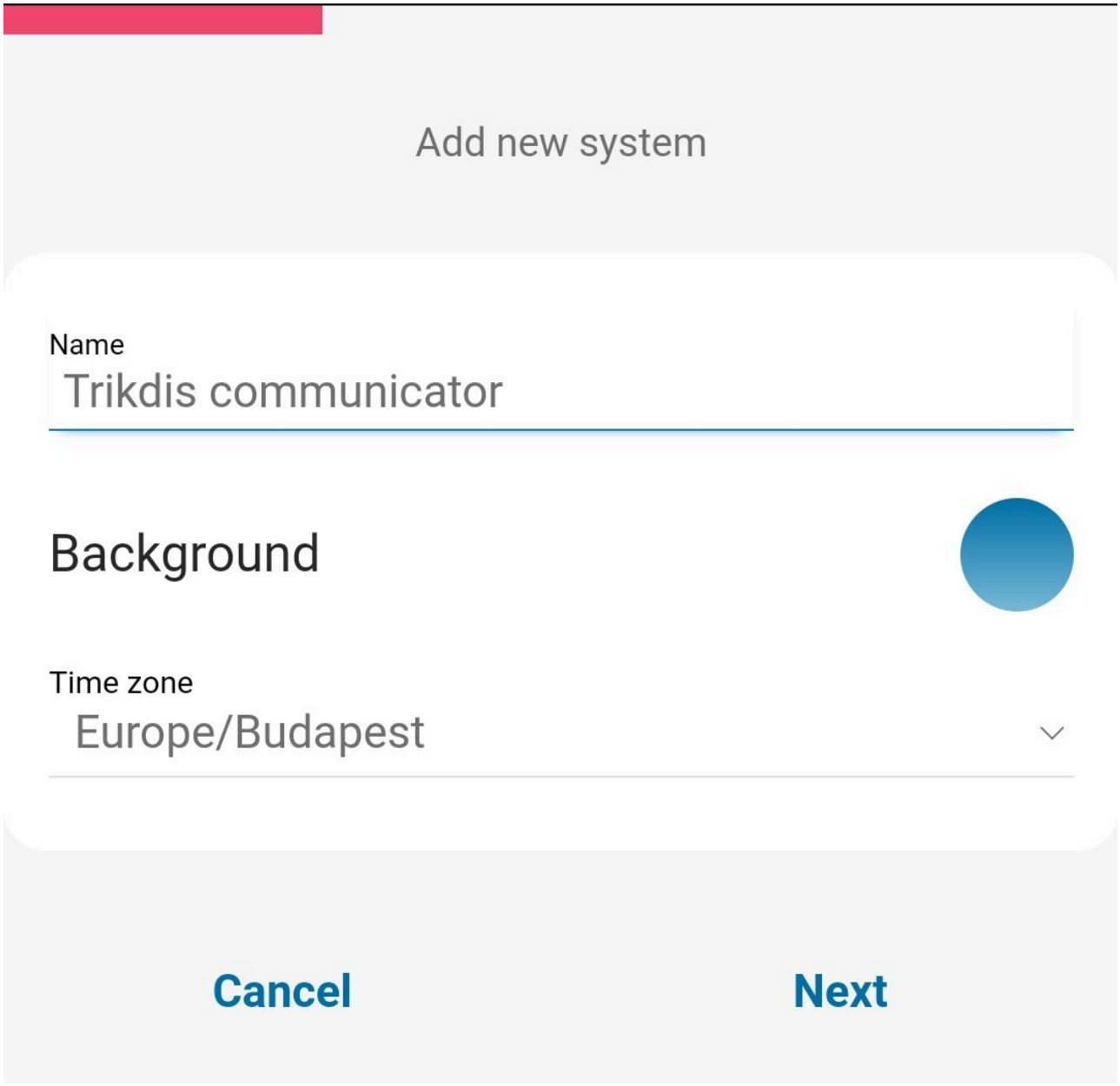


5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán

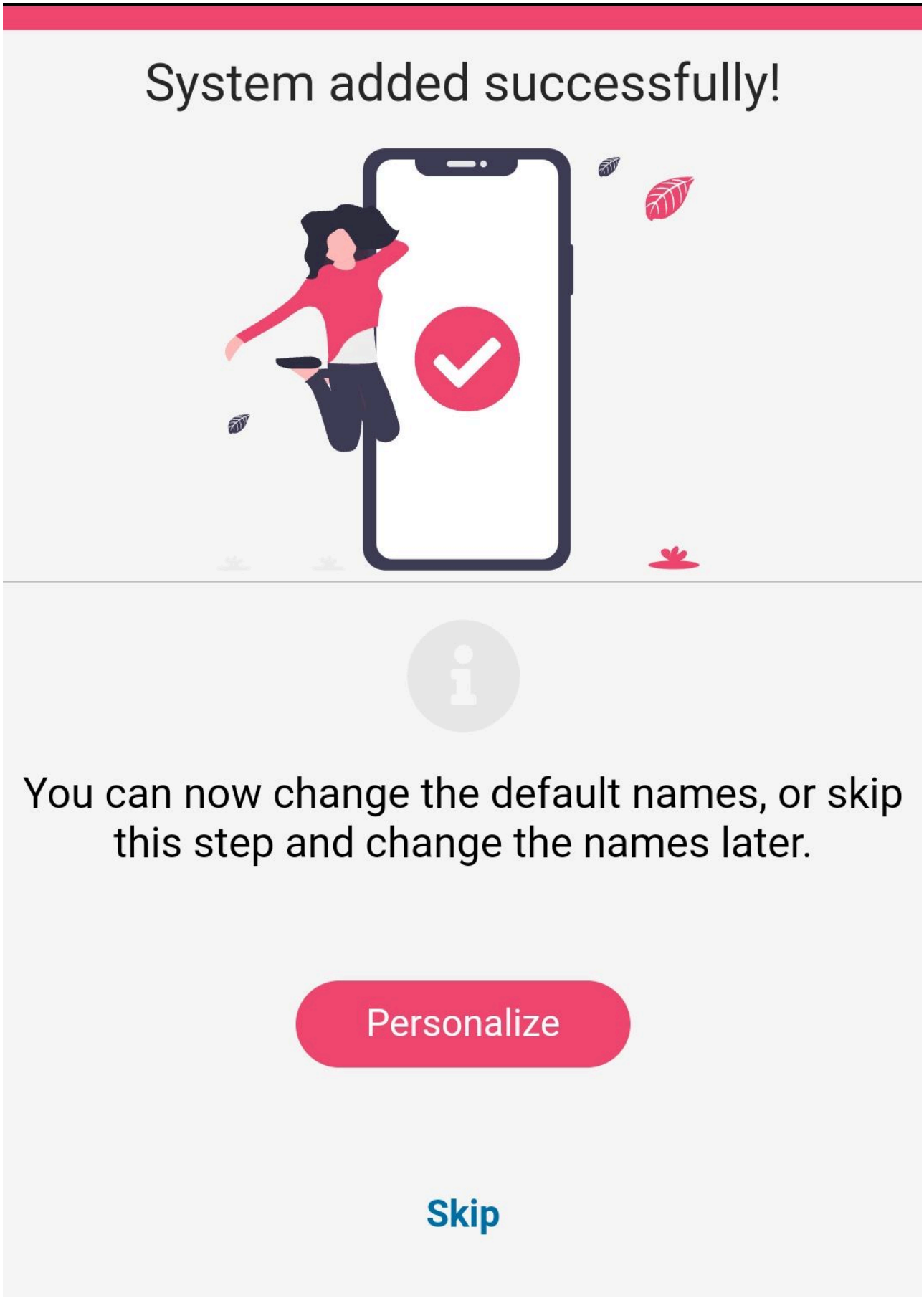
- Az eszköz papírdobozán
- A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



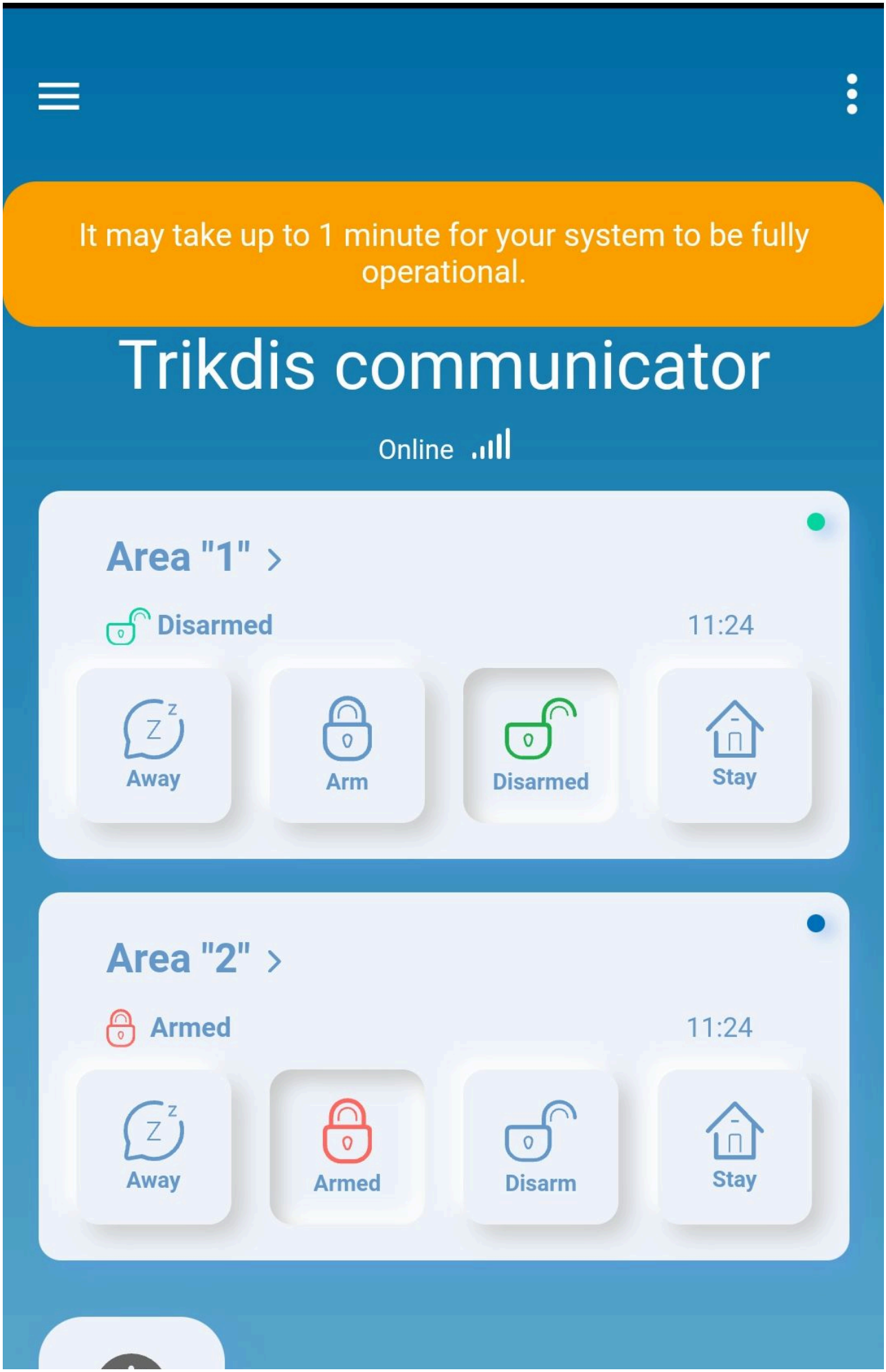
6. Add meg a rendszer nevét és válassz idozónát



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 E16, el identificador único del equipo es la **dirección MAC (Unique ID)**: figura en la caja y en la base del equipo, y también la muestra la barra de estado de TrikdisConfig (apartado 6.1). Es lo que hay que introducir en la aplicación como identificador del equipo al crear el sistema.

5.2 Control directo con el código de teclado

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

- Para ello, según el fabricante, hay que configurar la central (Paradox: contraseña PC; Texecom: contraseña UDL; en las Caddx, Honeywell e InnerRange, la habilitación del bus o del puerto serie, necesaria ya para leer los eventos): consulta el capítulo 4.
- El código de teclado lo comprueba la central, y el registro de eventos de la central anota al usuario, no al comunicador.
- En una central Paradox, el código del usuario **no puede ser el código maestro**; después de cambiar un código, reinicia el comunicador (apartado 4.2).
- En una central DSC PowerSeries, la aplicación muestra también el estado de las zonas y permite anular zonas; los detalles están en el artículo sobre el control directo de DSC (el artículo trata del G16, pero vale igual para el E16).

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

5.3 Armado con zona de interruptor de llave

Si la central no admite control directo, o no quieres usarla así, conectas una salida del comunicador a la zona de interruptor de llave de la central (apartado 3.4), en TrikdisConfig **Remote Arm/Disarm** queda sin marcar y en Protegus 2 asignas la salida a la partición.

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

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

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

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

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

5.4 Armado y desarmado desde la aplicación

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

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

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

El E16 no tiene control ni notificaciones por SMS: el armado, el desarmado y el accionamiento de las salidas se hacen desde la aplicación Protegus 2, y las notificaciones llegan como mensajes push.

6. TrikdisConfig – la configuración en detalle

En la parte izquierda de la ventana de TrikdisConfig está la lista de páginas (System settings, CMS reporting, User reporting, 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 recorre, página por página, la configuración del E16.

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 27. Barra de estado de TrikdisConfig con un E16 leído: dirección MAC (Unique ID, en blanco en la imagen), estado, tipo (E16_1100), número de serie, versiones, modo de conexión y nivel de acceso.

En el E16, el identificador único del equipo es la **dirección MAC**: es la que pide Protegus 2 al crear el sistema y TrikdisConfig para el acceso remoto (Unique ID). La misma dirección figura también en la caja y en la base del equipo.

6.2 System settings

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

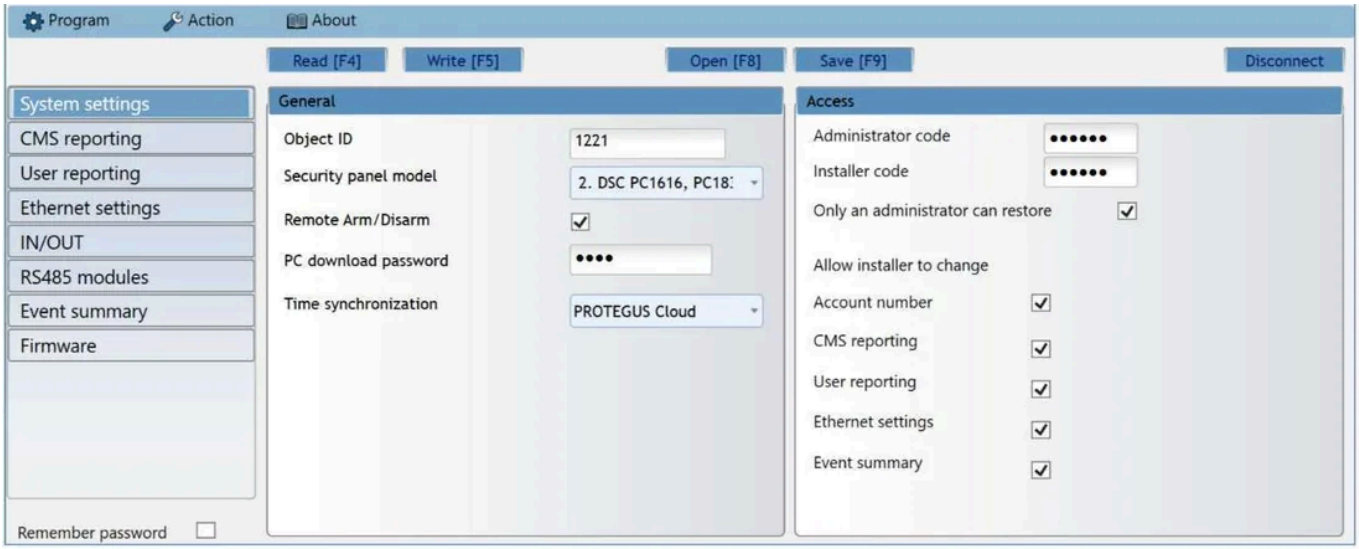


Figura 28. TrikdisConfig – página System settings: grupos General y Access.

- **Object ID** – el número de abonado facilitado por la CRA (4 caracteres hexadecimales, 0–9, A–F). Es obligatorio si el equipo también transmite a una CRA; no se pueden usar `FFFE` ni `FFFF`.
- **Security panel model** – el tipo de central de alarma conectada, de la lista. De él depende cómo lee el comunicador el bus, así que elige el tipo exacto de la central conectada.
- **Remote Arm/Disarm** – marcado, el comunicador controla la central directamente: el usuario arma y desarma desde Protegus 2 con su código de teclado. Solo aparece en los modelos de central de control directo; según el fabricante, requiere configuración en la central (capítulo 4). Con armado por zona de interruptor de llave, déjalo sin marcar.
- **Security panel PC download password** – para el control directo de centrales Paradox y Texecom, la contraseña PC o UDL de la central (4 caracteres); debe coincidir con la configurada en la central (apartados 4.2 y 4.3).
- **Time synchronization** – la fuente del reloj del equipo (por defecto **PROTEGUS Cloud**, la nube 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 IP. Los eventos pueden ir por varios canales: el canal **principal** y el **paralelo** funcionan a la vez (a dos receptores simultáneamente) y cada uno tiene un canal de **respaldo**, que entra en funcionamiento si se interrumpe el canal correspondiente. La comunicación está cifrada y protegida con contraseña; para recibir los eventos y pasarlos 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 el protocolo DC-09 / TL150.

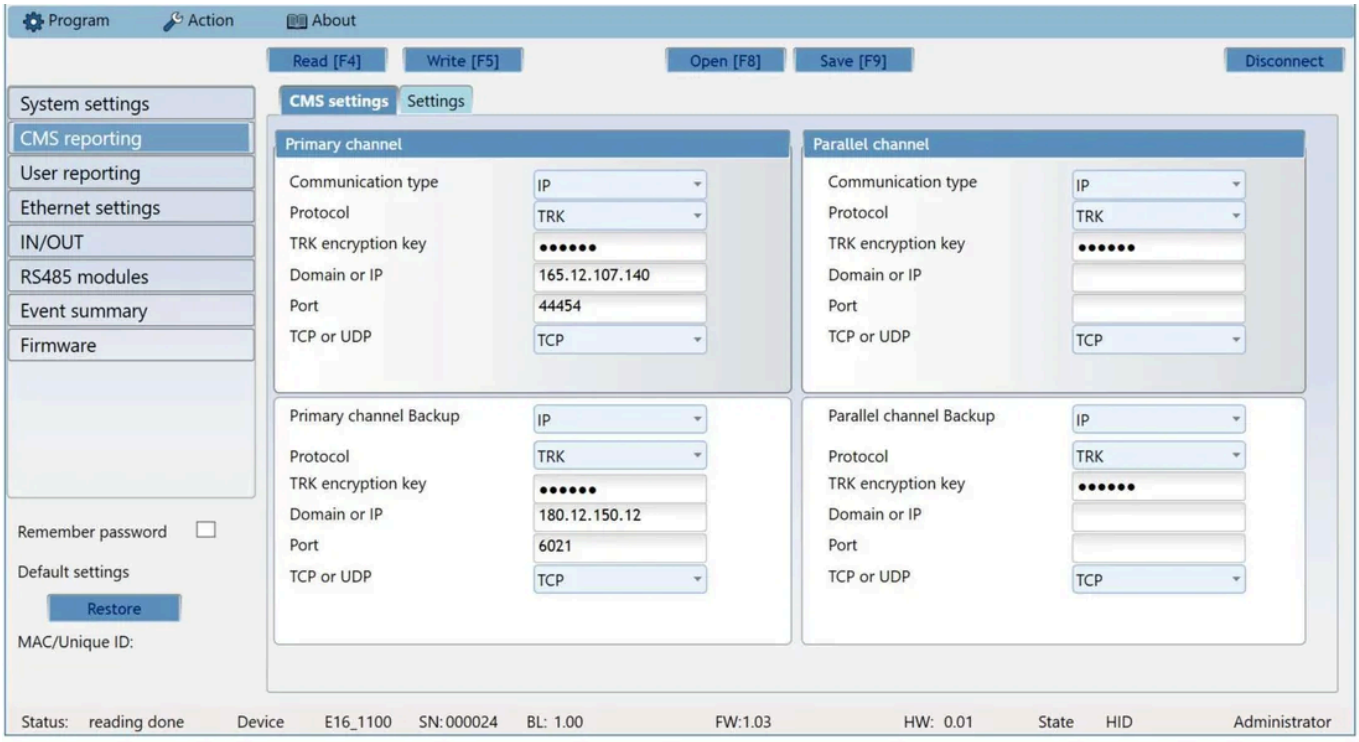


Figura 29. TrikdisConfig – CMS reporting, pestaña CMS settings: canal principal y paralelo (arriba), sus canales de respaldo (abajo).

Primary channel – canal principal

- **Communication type** – **IP**; con el valor **Disable** se puede desactivar el canal (por ejemplo, si el equipo solo funciona con Protegus 2, sin CRA).
- **Protocol** – TRK (receptores Trikdis), DC-09_2007 o DC-09_2012 (receptores universales), TL150 (SUR-GARD).
- **TRK encryption key** – clave de cifrado de 6 dígitos; debe ser la misma en el comunicador y en el receptor.
- **Domain or IP**, **Port** – la dirección y el puerto del receptor.
- **TCP or UDP** – el protocolo de transmisión.

Primary channel Backup – canal de respaldo. Toma el relevo de la comunicación si el canal principal no funciona; su configuración es la misma que la anterior. Como el E16 se comunica por una única vía de red (la red local), el canal de respaldo es una segunda dirección de receptor por la misma vía: cubre un fallo del lado del receptor, no la caída de la conexión a internet.

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.

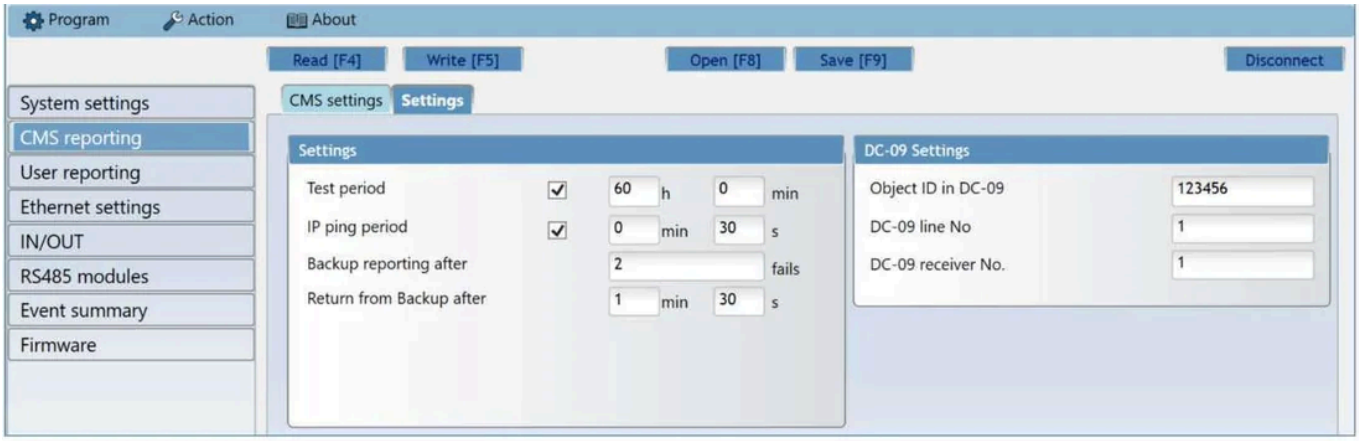


Figura 30. TrikdisConfig – CMS reporting, pestaña Settings: informe de prueba, PING, temporizaciones del canal de respaldo y datos DC-09.

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

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

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

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

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

El grupo **DC-09 settings** solo es visible si en algún canal está configurado el protocolo DC-09. Los servidores de nombres (DNS), en el E16, no se indican aquí, sino en la página **Ethernet settings** (apartado 6.5).

6.4 User reporting

En la pestaña **PROTEGUS Cloud** habilitas el servicio Protegus, con el que el usuario puede vigilar y controlar el comunicador a distancia; más información sobre el servicio: www.protegus.app. El E16 no tiene notificaciones ni control por SMS, por eso en esta página solo hay esta pestaña.



Figura 31. TrikdisConfig – User reporting, pestaña PROTEGUS Cloud.

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

6.5 Ethernet settings

Aquí configuras cómo se conecta el E16 a la red local. De fábrica viene marcado **Use DHCP**: el equipo obtiene automáticamente del router la dirección, la puerta de enlace y los servidores de nombres, y en la mayoría de los casos no hay que hacer nada.



Figura 32. TrikdisConfig – página Ethernet settings: configuración de red por DHCP o manual, servidores de nombres.

- **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.

6.6 IN/OUT

Aquí indicas la función de los tres bornes I/O de doble función del comunicador: **Disabled** (no usado), **IN** (entrada) u **OUT** (salida). Para una entrada también hay que indicar el tipo (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Configuración por defecto: I/O 1 e I/O 2 entrada (NO), I/O 3 salida.

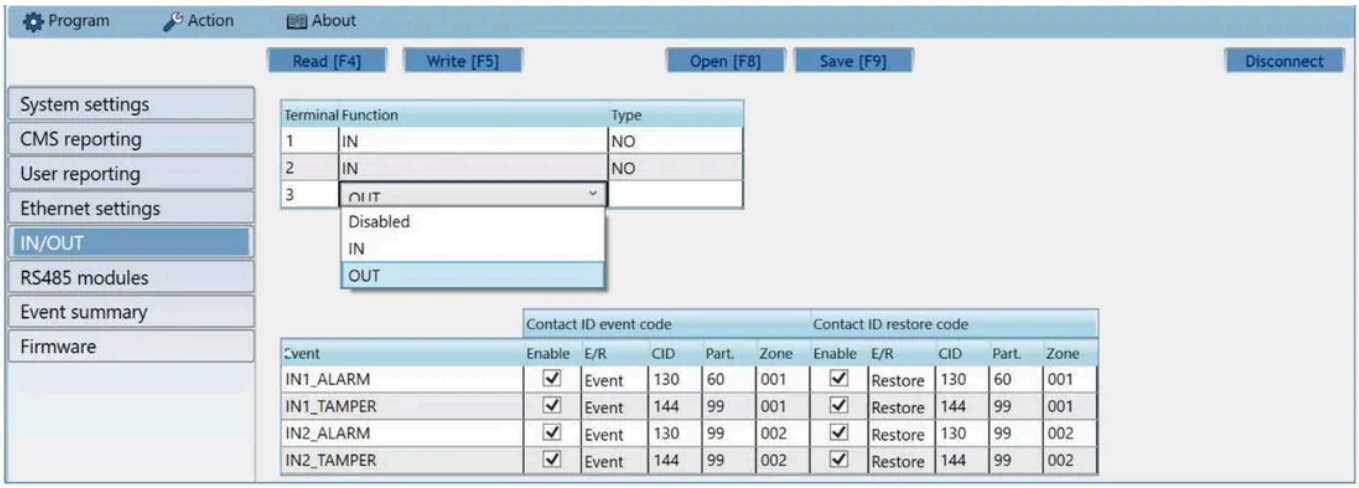


Figura 33. TrikdisConfig – página IN/OUT: función de los bornes I/O y eventos de las entradas.

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 (restablecimiento).
- **CID** – el código Contact ID; puedes indicarlo o dejar el valor por defecto. El evento va con este código a Protegus 2 y a la CRA.
- **Part.** – el número de partición en el mensaje.
- **Zone** – el número de zona en el mensaje.

6.7 RS485 modules

Los expansores iO-8 conectados al bus RS485 hay que darlos de alta en la pestaña **Modules list**.

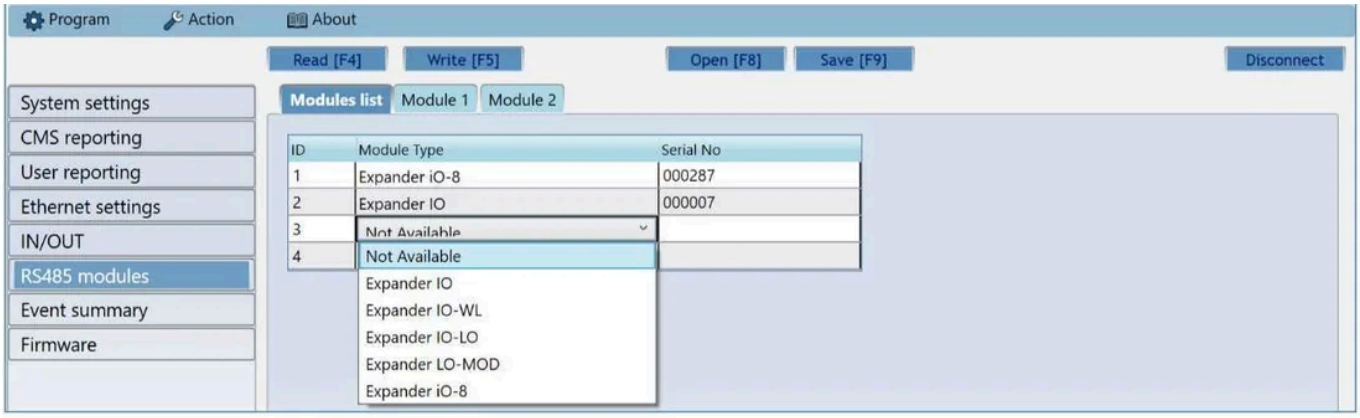


Figura 34. TrikdisConfig – RS485 modules, pestaña Modules list: tipo de módulo (Expander iO-8) y número de serie.

- **Module Type** – el tipo de módulo conectado, de la lista (**Expander iO-8**).
- **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 mientras el comunicador registra el módulo. Después vuelve a conectar el cable, lee el equipo (**Read [F4]**) y en la página RS485 modules aparece la pestaña propia y numerada del módulo.

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

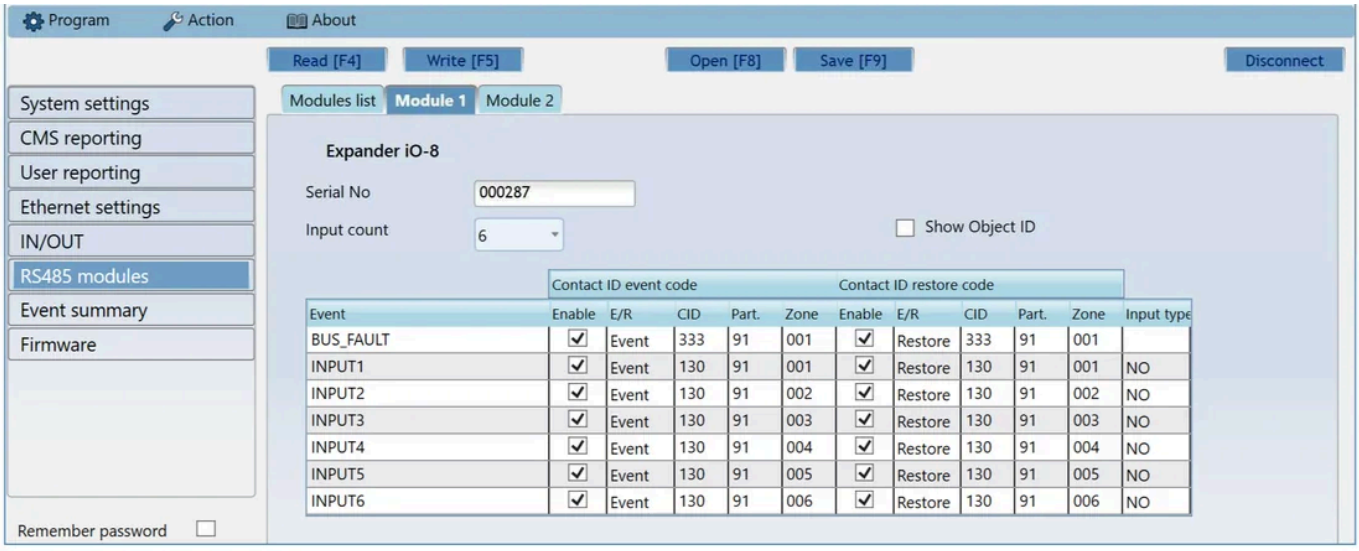


Figura 35. TrikdisConfig – RS485 modules, pestaña del módulo iO-8 (arriba) y tabla de eventos del expansor (abajo).

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

Mensaje	Contact ID	Cuándo se genera
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**.

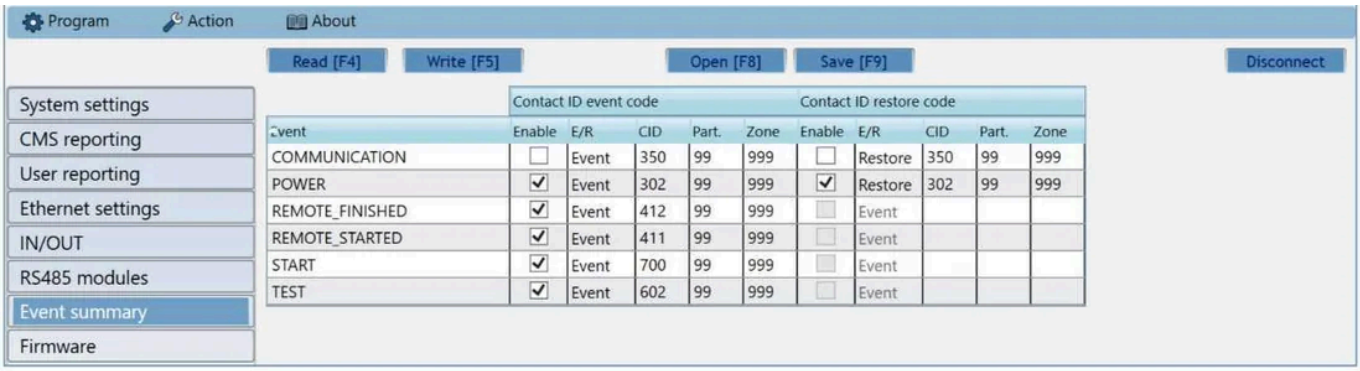


Figura 36. TrikdisConfig – página Event summary: los mensajes internos del equipo (COMMUNICATION, POWER, REMOTE_FINISHED, REMOTE_STARTED, START, TEST) y sus códigos Contact ID.

6.9 Restablecer la configuración de fábrica

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

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

7. Programación a distancia

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

Para el acceso remoto se necesita:

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

Pasos:

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

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

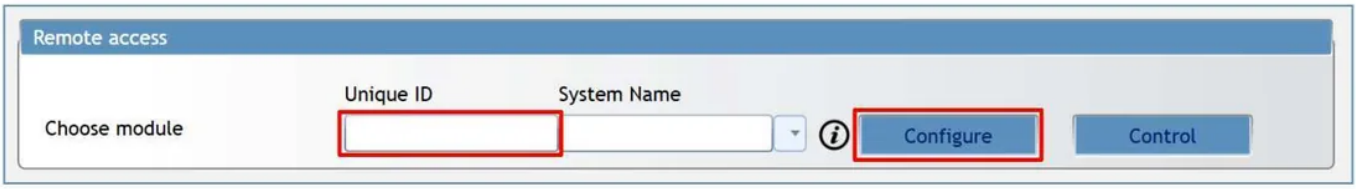


Figura 37. TrikdisConfig – Remote access: identificador del equipo (Unique ID; en el E16, la dirección MAC), nombre del sistema y botón Configure.

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.

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

Comprueba también el comportamiento ante una caída de la red: desconecta el cable Ethernet y mira si el LED TROUBLE señala la falta con 1 destello; después, al volver a conectarlo, si el LED NETWORK vuelve a estar verde fijo y si los eventos almacenados llegan a la CRA y a la aplicación.

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.

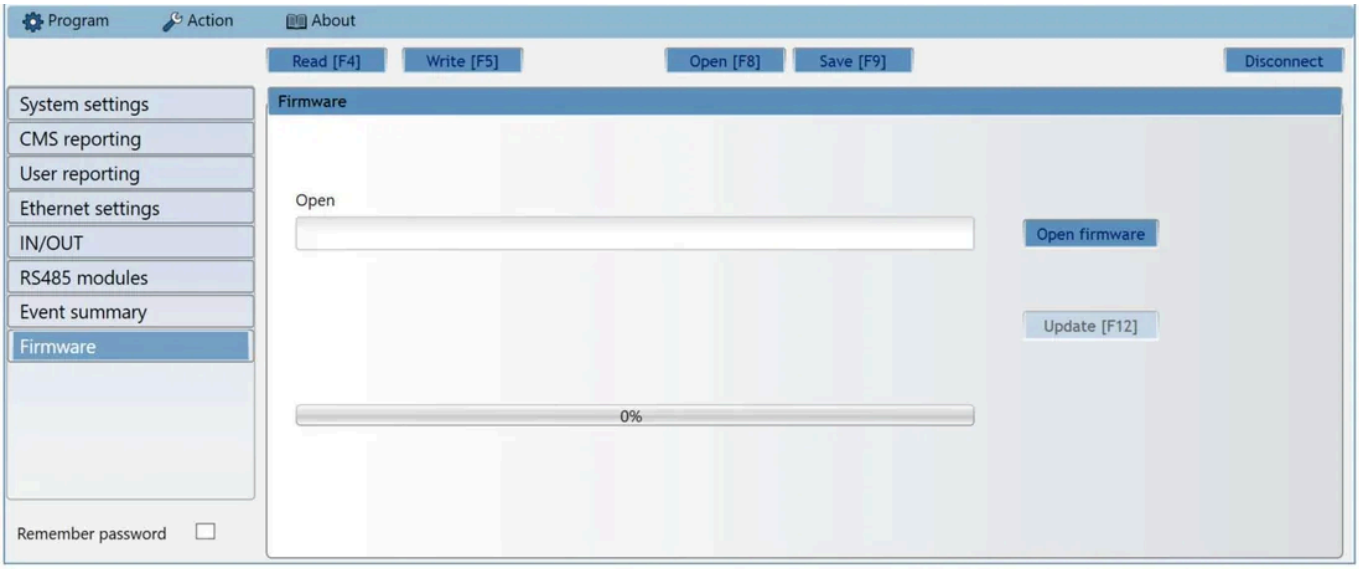


Figura 38. TrikdisConfig – página Firmware: Open firmware y Update [F12] (arriba), indicador de progreso de la actualización (abajo).

Para la actualización hace falta conexión a internet. El antivirus, el cortafuegos o una configuración de red estricta pueden impedir la descarga automática del firmware; en ese caso, cambia la configuración del antivirus o descarga el archivo manualmente y ábrelo en la página Firmware.

10. Solución de problemas y preguntas frecuentes

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

El LED NETWORK no se enciende: no hay red

1. Mira los destellos del LED **TROUBLE**: 1 = no hay conexión física (cable, puerto), 2 = no ha obtenido dirección IP (DHCP), 3 = no puede resolver el nombre del receptor o de la nube Protegus (DNS).
2. **1 destello:** comprueba el cable Ethernet en ambos extremos y que el puerto del router o del switch esté activo (el LED del puerto encendido); prueba con otro puerto u otro cable.
3. **2 destellos:** el DHCP del router debe estar activado, o asigna al equipo una dirección IP fija en la página **Ethernet settings** (apartado 6.5). En una red de empresa, el administrador de red puede autorizar el equipo por su dirección MAC.
4. **3 destellos:** el servidor de nombres no está accesible. Por defecto está configurado el DNS público de Google; si la red bloquea los DNS externos, introduce el servidor de nombres local en la página **Ethernet settings**.

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. En una red filtrada por cortafuegos hay que permitir el tráfico TCP/UDP saliente hacia el puerto del receptor; no hace falta abrir puertos (de entrada) en el router.

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

1. Comprueba el cableado según el esquema del apartado 3.3: el error más frecuente es tener invertidos los hilos **CLK** y **DATA**, o la línea de datos conectada a un borne equivocado de la central.
2. En el campo **System settings** → **Security panel model** de TrikdisConfig debe estar seleccionado el tipo exacto de la central conectada.
3. En las centrales Texecom, Caddx, Honeywell e InnerRange también hay que configurar la central (capítulo 4); sin ello, la central no da datos en el bus.
4. En una central Paradox, puede que el puerto serie venga bloqueado de fábrica: así puedes desbloquearlo.
5. Después del cableado, desconecta la alimentación de la central Pyronix y reiníciala para que acepte el comunicador.
6. Con una central DSC PowerSeries **NEO**, el E16 no funciona (el bus de la NEO no admite dispositivos externos): aquí hace falta un comunicador de línea telefónica (E16T).

Los eventos llegan, pero no puedo armar desde la aplicación

Con control directo:

1. En la página **System settings** debe estar marcado **Remote Arm/Disarm**.
2. En centrales Paradox y Texecom, **Security panel PC download password** debe coincidir con la contraseña PC o UDL de la central (apartados 4.2 y 4.3).
3. En una central Paradox, el firmware de la central debe ser como mínimo **V.4**; el código del usuario no debe ser el código maestro; después de cambiar un código, reinicia el comunicador.
4. En una central Honeywell Vista debe estar habilitada la 2.ª dirección AUI (apartado 4.6).
5. En Protegus 2, **no** debe haber ninguna salida asignada a la partición (Control with Protegus2 desactivado).

Con zona de interruptor de llave:

1. **Remote Arm/Disarm** debe estar sin marcar, y el borne I/O debe estar como **OUT** en la página **IN/OUT**.
2. La zona de la central debe ser de tipo interruptor de llave y, en Protegus 2, la partición debe tener asignada la salida correcta, en el modo por impulso o biestable que corresponda a la zona (apartado 5.3).

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. Introduce la **dirección MAC (Unique ID)** con exactitud, copiándola de la caja o de la base.

4. El equipo debe estar en línea: LED NETWORK verde, TROUBLE sin parpadear, y el LED DATA se apaga después de un evento. En una red con cortafuegos hay que permitir la conexión saliente hacia la nube Protegus.

No puedo acceder a distancia con TrikdisConfig

1. El equipo debe estar en línea (LED NETWORK verde) y la conexión con Protegus debe estar habilitada.
2. **CMS reporting** → **Settings** → **IP ping period** no debe ser 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.

¿Hay que abrir o redirigir puertos en el router?

No. El E16 solo establece conexiones **salientes** hacia el receptor y la nube Protegus, por lo que no hacen falta ni redirección de puertos ni IP pública; la programación a distancia también se hace a través de esta conexión saliente. Solo asegúrate de que el cortafuegos no bloquee el tráfico saliente hacia el puerto del receptor ni hacia la nube Protegus.

¿Funciona por wifi o por red móvil?

No: el E16 solo tiene conector Ethernet por cable. Si el router no tiene una alimentación fiable, alimenta los equipos de red con un SAI.

¿Qué pasa durante un corte de corriente?

El E16 se alimenta de la central de alarma, así que sigue funcionando con la batería de la central, pero el router y el módem normalmente se apagan y, con ello, se pierde internet. Mientras no hay conexión, el LED TROUBLE lo señala con 1 o 6 destellos; el equipo guarda los eventos (hasta 60 mensajes) y, cuando vuelve internet, los envía por orden. Si la caída de internet no es admisible para el sistema, alimenta también los equipos de red con un SAI.

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 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

- Buscador de compatibilidad: qué comunicador corresponde a cada central de alarma.
- G16: control directo para centrales de alarma DSC PowerSeries: armado con el código de teclado, estado de las zonas, anulación de zonas; vale igual para el E16.
- DSC Power Series NEO y comunicadores Trikdis: compatibilidad y soluciones: por qué el E16 no se puede conectar a la NEO y cuál es la solución.
- Desbloqueo del puerto serie bloqueado en las centrales de alarma Paradox: desbloqueo del puerto serie de las centrales Paradox más recientes.
- 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 E16 Ethernet comunicador - módulo IP

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

CRP2B cable de conexión puerto serie para paneles de alarma Paradox

Trikdis CRP4 cable serie para paneles de control Texecom

Trikdis iO8 módulo expansor cableado

Derechos de autor

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

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

Versión siempre actualizada de este manual: https://trikdis.es/manual-e16