Controlador de puertas GV17 GATOR – manual de instalación y programación

Manual de instalación y programación del controlador de puertas Trikdis GV17 GATOR: conexionado, tarjeta SIM y configuración en TrikdisConfig, usuarios y permisos, control por llamada, por SMS y desde la aplicación Protegus 2.



Edición: 2026-11-18
Versión web siempre actualizada: https://trikdis.es/manual-gv17

Índice

1. Descripción general

1.1 Para qué sirve y cómo funciona
1.2 Versiones
1.3 Características técnicas
1.4 Partes del equipo y bornes
1.5 Indicaciones LED
1.6 Contenido del paquete y herramientas necesarias

2. Puesta en marcha rápida

2.1 Puesta en servicio en tres pasos
2.2 Que solo abran los autorizados
2.3 Configuración de la aplicación y de la CRA

3. Instalación y conexionado

3.1 Fijación y colocación de la tarjeta SIM
3.2 Alimentación
3.3 Entradas
3.4 Conexión de un relé a la salida universal
3.5 Conexión del automatismo de la puerta
3.6 Conexión del lector RFID (Wiegand 26/34)
3.7 Módulo WiFi W485
3.8 Módulo Ethernet E485
3.9 Expansores RF-LORA e iO-LORA con lector RFID
3.10 Expansores iO8 e iO8-LORA

4. Control a distancia

4.1 Control con una llamada telefónica
4.2 Control con el teclado del teléfono (DTMF)
4.3 Control desde la aplicación Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.4 Widget en la pantalla de inicio del teléfono
4.5 Gestión de usuarios en la aplicación
4.6 Control con un mensaje SMS
4.7 Programación por SMS

5. Configuración con el software TrikdisConfig

5.1 La barra de estado
5.2 Página «System Options»
5.3 Página «IN/OUT»
5.3.1 Pestaña IN/OUT – entradas y salidas
5.3.2 Pestaña Scheduler – horarios de las salidas
5.3.3 Pestaña Holidays – días festivos
5.4 Página «Modules»
5.4.1 Pestaña Modules
5.4.2 Pestaña Parameters – módulo WiFi W485
5.4.3 Pestaña Parameters – módulo Ethernet E485
5.5 Página «IP Reporting»
5.6 Página «User list»

5.6.1 Pestaña Users – los usuarios
5.6.2 Registro de una tarjeta RFID (llavero)
5.6.3 Pestaña Scheduler – horarios de los usuarios
5.6.4 Pestaña Black list – lista negra
5.7 Página «System events»
5.8 Página «Events Log»
5.9 Restablecimiento de la configuración de fábrica
5.10 Indicación del estado de la puerta
6. Programación a distancia
7. Comprobación del funcionamiento
8. Actualización del firmware
9. Solución de problemas y preguntas frecuentes
10. Instrucciones de seguridad
Ver también

1. Descripción general

El **GV17 GATOR** es el controlador de puertas por red móvil de Trikdis: está diseñado para el control a distancia de puertas eléctricas, barreras, puertas de garaje y otros equipos. El usuario lo controla con una **llamada telefónica**, con un **mensaje SMS** o desde la aplicación **Protegus 2**; el equipo gestiona los números de teléfono (tarjetas RFID, direcciones de correo electrónico) de hasta **7 administradores** y **1000 usuarios**, y para cada usuario se puede fijar una limitación horaria propia (horario, periodo de validez) y un contador. El GATOR avisa de los cambios de estado de las entradas y salidas (activación y restablecimiento) por SMS y en la aplicación – el texto de los SMS lo defines tú –, y también transmite los eventos a la CRA en formato Contact ID. Con un módulo WiFi **W485** o Ethernet **E485**, el control y la transmisión funcionan también por internet, sin datos móviles; con un transceptor **RF-LORA** se le pueden conectar hasta 8 expansores inalámbricos **iO-LORA** y un expansor **iO8-LORA**, de modo que con un solo equipo se pueden controlar hasta 8 puertas o barreras alejadas entre sí, cada una con su propio lector RFID (los lectores RFID conectados a los expansores iO-LORA pueden conmutar hasta 8 salidas – un lector siempre solo una salida de su propio expansor –; para ello el GATOR necesita el firmware 2.13 o posterior). La configuración se hace con el software **TrikdisConfig**, por cable USB o a distancia.



Figura 1. El controlador de puertas GV17 GATOR: delante los indicadores NETWORK, DATA, POWER y TROUBLE, arriba el conector de antena, abajo la regleta de bornes extraíble.

1.1 Para qué sirve y cómo funciona

Para qué sirve sobre todo

- **Apertura a distancia de puertas, barreras y puertas de garaje** para la familia, una comunidad de vecinos, los empleados de una empresa o los usuarios de un aparcamiento: el usuario llama al número de la tarjeta SIM del GATOR y la puerta se abre – el equipo rechaza la llamada, por lo que la llamada es gratuita. Lo mismo se puede hacer desde la aplicación con un botón, con un widget colocado en la pantalla de inicio del teléfono o por SMS.
- **Control de acceso con tarjeta RFID y código**: con uno o dos lectores Wiegand 26/34 (entrada y salida), salida con pulsador, con horario por usuario (quién puede entrar y cuándo), periodo de validez y contador de accesos; a partir de las entradas y salidas también se puede llevar un **registro de jornada** en Protegus 2 – hay un artículo aparte sobre ello: GV17 como sistema de control de acceso y/o registro de jornada.
- **Cualquier otro equipo**: encendido y apagado a distancia, en modo de impulso o biestable, también según un horario: iluminación, riego, bomba, calefacción.
- **Varias puertas en un sistema**: de forma inalámbrica con los módulos RF-LORA e iO-LORA, hasta 8 ubicaciones, cada una con su propio relé, entrada y lector RFID – Control de acceso inalámbrico y flexible con el sistema GATOR RF-LoRa.

Cómo funciona

- **Control**: con una llamada telefónica (de fábrica cualquiera que llame; con una lista de usuarios, solo los autorizados), durante la llamada con el teclado del teléfono (DTMF), con un comando SMS, desde la aplicación móvil y web Protegus 2, con un widget de Android, con tarjeta RFID y código.
- **Notificación al usuario**: por SMS a los administradores (sobre los eventos de las entradas y salidas, prueba, nuevo usuario), por notificación push en la aplicación Protegus 2.
- **Transmisión a la CRA**: con códigos de evento Contact ID a los receptores IP de software y de hardware de Trikdis, que funcionan con cualquier software de CRA; receptor principal y de reserva (si se interrumpe la conexión con el receptor principal, los mensajes van automáticamente al receptor de reserva), SMS de reserva; los eventos pueden ir a la vez a la CRA y a Protegus 2.
- **Entradas y salidas**: 2 entradas (NO, NC o EOL 10 kΩ), 2 bornes universales (entrada o salida de colector abierto, 50 mA), 1 salida de relé (1 A / 30 V DC, 0,5 A / 125 V AC). Cada expansor iO-LORA amplía el sistema con 1 entrada y 1 salida de relé (hasta 8 expansores, es decir, en total 8 entradas y 8 salidas adicionales), el expansor iO8 o iO8-LORA con más entradas y salidas (se puede conectar uno al GATOR).
- **Instalación y configuración**: de fábrica listo para funcionar; los usuarios se añaden y se eliminan desde la aplicación Protegus 2 (como administrador), por SMS o con el software TrikdisConfig; la configuración se hace con un cable USB Mini-B o a distancia; el firmware también se puede actualizar a distancia; dos niveles de acceso (instalador y administrador).

1.2 Versiones

El GATOR existe en dos versiones de red móvil; las dos se conectan, se configuran y se controlan igual, solo cambia el módem. En la barra de estado de TrikdisConfig ves el tipo exacto con la forma **GV17_xxxx** (apartado 5.1).

Versión	Módem	Bandas
GV17-4G	4G (LTE)	En Europa LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 (para Latinoamérica se fabrica una versión con otras bandas)
GV17-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis GV17 - GATOR controlador de acceso 4G GSM / IP

Trikdis GV17 - GATOR controlador de acceso 2G GSM / IP

Debido al apagado progresivo de las redes 2G, para instalaciones nuevas recomendamos la versión 4G. En los equipos con código de tipo **GV17_2E70** y **GV17_2S70** no funciona el control con el teclado durante la llamada (DTMF) (apartado 4.2); el control por llamada, por SMS y desde la aplicación funciona igual en ellos.

1.3 Características técnicas

Característica	Valor
Bandas del módem 2G (GSM)	850 / 900 / 1800 / 1900 MHz
Bandas del módem 4G (LTE)	Europa: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28; Latinoamérica: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Tensión de alimentación	9–32 V DC o 12–24 V AC
Consumo	100 mA
Entradas	2, tipo seleccionable: NC, NO, EOL = 10 kΩ
Entradas/salidas universales	2; como entrada NC, NO, EOL = 10 kΩ, como salida de colector abierto (OC), hasta 50 mA
Salida	1 relé, 1 A / 30 V DC, 0,5 A / 125 V AC
Memoria de eventos no enviados	hasta 60 eventos
Registro de eventos	hasta 5000 eventos
Usuarios que reciben mensajes y pueden controlar (administradores)	7
Usuarios que pueden controlar	1000
Entorno de funcionamiento	–20 … +50 °C, humedad relativa hasta el 80 % a +20 °C
Dimensiones	92 × 62 × 26 mm
Peso	80 g

1.4 Partes del equipo y bornes

Los números de la figura indican las partes del equipo; el significado de los bornes figura en la tabla.

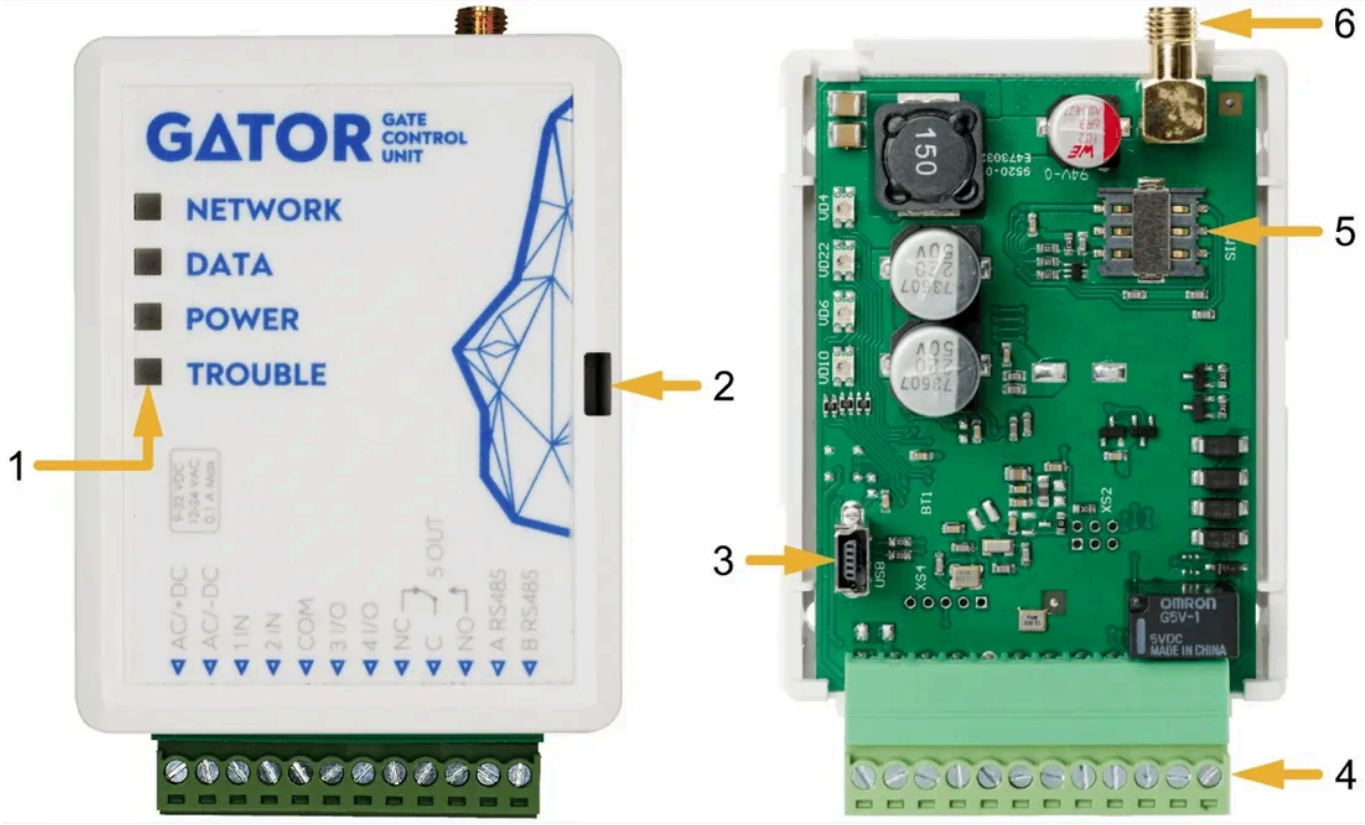


Figura 2. Partes del GATOR.

- 1 indicadores LED
- 2 ranura para retirar la tapa frontal
- 3 conector USB Mini-B para la programación
- 4 regleta de bornes extraíble
- 5 ranura de la tarjeta nano-SIM
- 6 conector SMA de la antena de red móvil

Borne	Función
AC/+DC	alimentación: polo positivo de 9–32 V DC o 12–24 V AC
AC/−DC	alimentación: polo negativo de 9–32 V DC o 12–24 V AC
1 IN	entrada 1, tipo NO, NC o EOL (de fábrica: entrada NO)
2 IN	entrada 2, tipo NO, NC o EOL (de fábrica: desactivada)
COM	común de las entradas
3 I/O	entrada o salida (de fábrica: desactivada)
4 I/O	entrada o salida (de fábrica: desactivada)
NC	contacto normalmente cerrado del relé
C	contacto común del relé
NO	contacto normalmente abierto del relé
A RS485	hilo A del bus RS485
B RS485	hilo B del bus RS485

El programa y los comandos SMS llaman a la salida de relé **5 OUT** (OUTPUT5) y a los dos bornes universales, usados como salida, **3 OUT** y **4 OUT**. La regleta de bornes de 12 polos se puede extraer del equipo y también se vende por separado:

1.5 Indicaciones LED

Indicador	Luz	Significado
NETWORK	verde, fija	conectado a la red móvil
	parpadeo amarillo	intensidad de la señal móvil con 0–5 destellos; 3 ya es suficiente
DATA	verde, fija	envío de mensaje en curso
	amarillo, fija	hay eventos en la memoria pendientes de envío
POWER	parpadeo verde	la tensión de alimentación es correcta
	parpadeo amarillo	la tensión de alimentación no es correcta
	parpadeo rojo y amarillo	modo de configuración
TROUBLE	apagado	no hay fallo de funcionamiento
	1 destello	no hay tarjeta SIM
	2 destellos	el código PIN de la tarjeta SIM es incorrecto
	3 destellos	no se puede conectar a la red móvil
	4 destellos	no se puede conectar a la nube de Protegus ni al receptor IP principal
	5 destellos	no se puede conectar al receptor IP de reserva
	6 destellos	el reloj interno no está ajustado
	7 destellos	la tensión de alimentación no es correcta

Si no se enciende ningún LED, comprueba la tensión de alimentación y el conexionado.

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

1.6 Contenido del paquete y herramientas necesarias

En la caja: 1 controlador de puertas GV17 GATOR, 1 antena de red móvil, 3 resistencias de 10 kΩ, 1 cinta adhesiva de doble cara (5 cm) y 2 tornillos.

Qué vas a necesitar

Antes de empezar la instalación, comprueba que tienes todo a mano: cable USB Mini-B para la configuración · cable de al menos 4 hilos para el conexionado · destornillador plano de 2,5 mm · tarjeta nano-SIM activada (desactiva la petición del PIN) con servicio de datos móviles, si también usas la aplicación o la CRA · antena externa, si la cobertura en el lugar es débil · el manual del instalador del equipo controlado (motor de la puerta, barrera), con el conexionado de la entrada de control y de la salida de estado de la puerta. Los accesorios indicados se compran por separado: pídelos a tu distribuidor.

Con cobertura débil, en una caja metálica o detrás de una pared gruesa, en lugar de la antena incluida usa una antena con cable de 2,5 m que se pueda colocar fuera:

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

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

2. Puesta en marcha rápida

El GATOR viene listo para funcionar de fábrica

Si alguien llama al número de teléfono de la tarjeta SIM colocada en el equipo, el GATOR rechaza la llamada y activa la salida de relé **5 OUT** durante **3 segundos**. Si este funcionamiento te sirve, el equipo se puede poner en servicio sin ninguna otra configuración.

2.1 Puesta en servicio en tres pasos

1. **Coloca la tarjeta nano-SIM** en la ranura del GATOR (apartado 3.1). Antes, desactiva la petición del PIN de la tarjeta en un teléfono; de lo contrario, el equipo no se registra en la red (o tienes que introducir el PIN en TrikdisConfig, apartado 5.2).
2. **Conecta la alimentación y el automatismo de la puerta** según los esquemas del capítulo 3: la alimentación a los bornes **AC/+DC** y **AC/−DC**, la entrada de control del automatismo a los contactos **C** y **NO** del relé.
3. **Conecta la alimentación.** Si funciona correctamente, el LED **POWER** parpadea en verde, el LED **NETWORK** se enciende en verde y entretanto parpadea en amarillo según la intensidad de la señal. Llama al número de la tarjeta SIM: el equipo rechaza la llamada y el relé se activa durante 3 segundos.

2.2 Que solo abran los autorizados

De fábrica **cualquiera** que llame a su número puede controlar el GATOR. Si quieres permitirlo solo a personas concretas, envía un SMS con el número de teléfono de los usuarios (envía el comando desde tu propio teléfono, porque quien llama o envía un SMS al equipo por primera vez se convierte en su administrador, apartado 4.1):

```
SETU 123456 +CC123456789#Pedro#pedro@example.com
```

Después de añadir el primer número, el GATOR solo reacciona a las llamadas de los números que están en la lista y no hace caso a las demás. Puedes añadir más usuarios de la misma manera, uno por uno; el conjunto completo de comandos SMS se describe en el apartado 4.7, y la lista también se puede gestionar en TrikdisConfig y en la aplicación Protegus 2 (apartados 5.6 y 4.5).

Cambia la contraseña de administrador

Con la contraseña de fábrica `123456`, cualquiera que conozca el número del equipo puede reprogramar el GATOR. En la primera puesta en marcha cámbiala por SMS (`PSW 123456 nuevacontraseña`, 6 caracteres) o en TrikdisConfig (**System Options** → **Administrator Code**).

2.3 Configuración de la aplicación y de la CRA

- **Aplicación Protegus 2:** en TrikdisConfig, en la página **IP Reporting**, activa el servicio en la nube (**Enable cloud service**, apartado 5.5) y cambia el código de fábrica `123456` del **Cloud Access Code**; lo mismo por SMS: `CONNECT 123456 PROTEGUS=ON`. Después, el sistema se puede añadir a la aplicación

según el apartado 4.3. Para ello la tarjeta SIM necesita servicio de datos móviles (o un módulo W485 / E485).

- **CRA:** en la página **IP Reporting** introduce la dirección, el puerto y la clave de cifrado del receptor, y en la página **System Options** el número de abonado (apartados 5.2 y 5.5).
- **Orden recomendado de la configuración en TrikdisConfig:** contraseña de administrador y datos de la SIM (APN) → función de las entradas y salidas, tiempo de impulso → usuarios, tarjetas RFID, horarios → nube y CRA → comprobación según el capítulo 7.

Si quieres modificar la configuración de fábrica o activar otras funciones del equipo, el capítulo 5 describe la configuración del software TrikdisConfig.

3. Instalación y conexionado

Figyelem!

Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

Este capítulo describe la fijación del GATOR, la alimentación, la conexión de las entradas, del relé y del automatismo de la puerta y, después, la conexión de los lectores RFID y de los módulos de expansión (W485, E485, RF-LORA + iO-LORA, iO8 / iO8-LORA). En los esquemas, los nombres de los bornes del GATOR coinciden con las serigrafías del equipo (apartado 1.4).

3.1 Fijación y colocación de la tarjeta SIM

1. Retira la tapa frontal (introduce el destornillador en la ranura lateral y suéltala haciendo palanca) y, a continuación, extrae la regleta de bornes.
2. Saca la placa de circuito impreso de la caja: presiona la pestaña de fijación y levántala.
3. Fija la parte trasera de la caja en el lugar deseado con tornillos (o con la cinta adhesiva de doble cara incluida).
4. Vuelve a colocar la placa de circuito impreso y la regleta de bornes.
5. Enrosca la antena de red móvil en el conector SMA.
6. Coloca la tarjeta nano-SIM en la ranura.
7. Vuelve a colocar la tapa frontal.

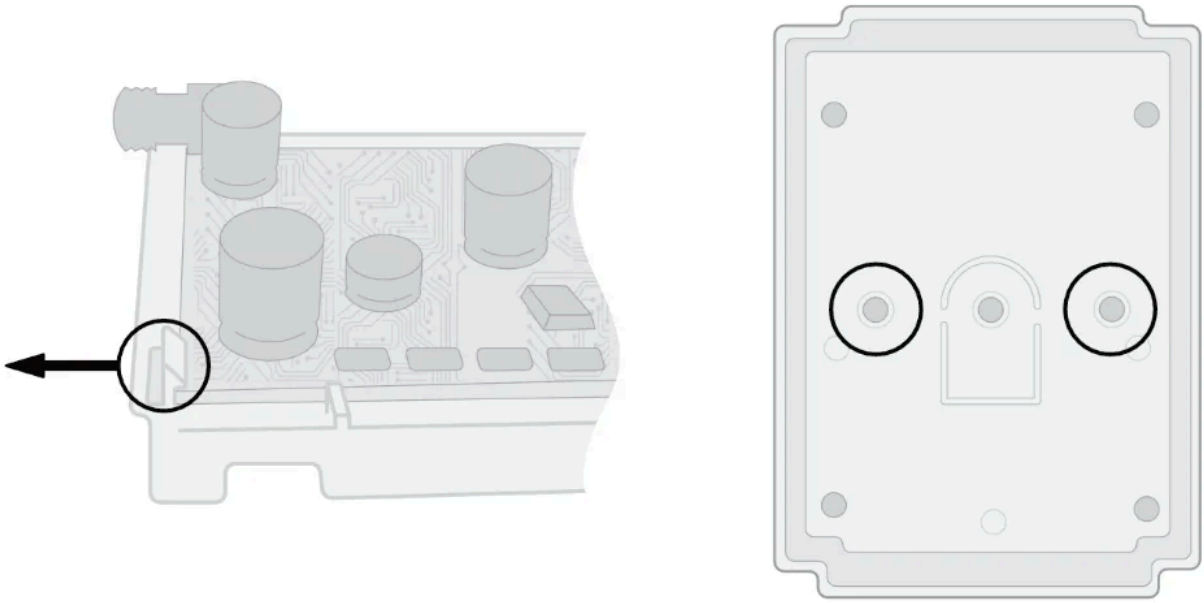


Figura 3. A la izquierda, la pestaña de fijación de la placa de circuito impreso (presionándola en el sentido de la flecha se libera la placa); a la derecha, los dos orificios para tornillos de la parte trasera.

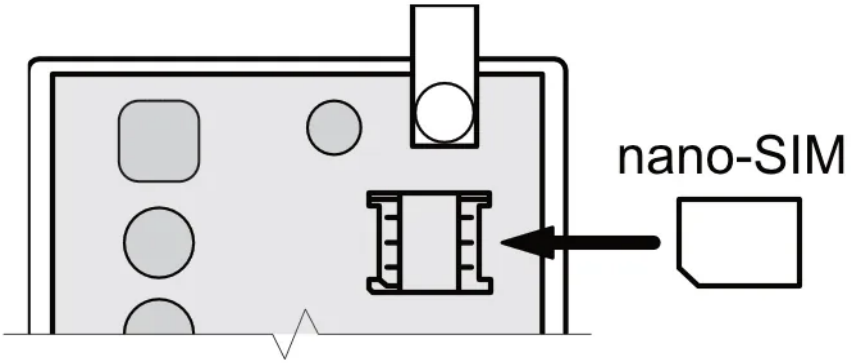


Figura 4. Colocación de la tarjeta nano-SIM en el sentido de la flecha, en la ranura de la placa de circuito impreso.

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

3.2 Alimentación

El GATOR funciona con **9–32 V DC** o **12–24 V AC**; los dos bornes de alimentación (**AC/+DC**, **AC/−DC**) admiten ambos tipos de alimentación. En la mayoría de los casos basta la salida de alimentación para accesorios de la unidad de control del motor de la puerta (normalmente 24 V AC o DC), por lo que no hace falta una fuente de alimentación aparte. Si usas una alimentación propia, sirve un transformador de ~230 V / 16 V de al menos 10 VA (con un fusible de 125 mA en el lado de 230 V) o una fuente de alimentación de corriente continua de 9–32 V y al menos 0,2 A. El equipo no tiene batería de reserva: si la puerta tiene que abrirse también durante un corte de corriente, aliméntalo desde un SAI. Conecta los cables según el esquema siguiente.

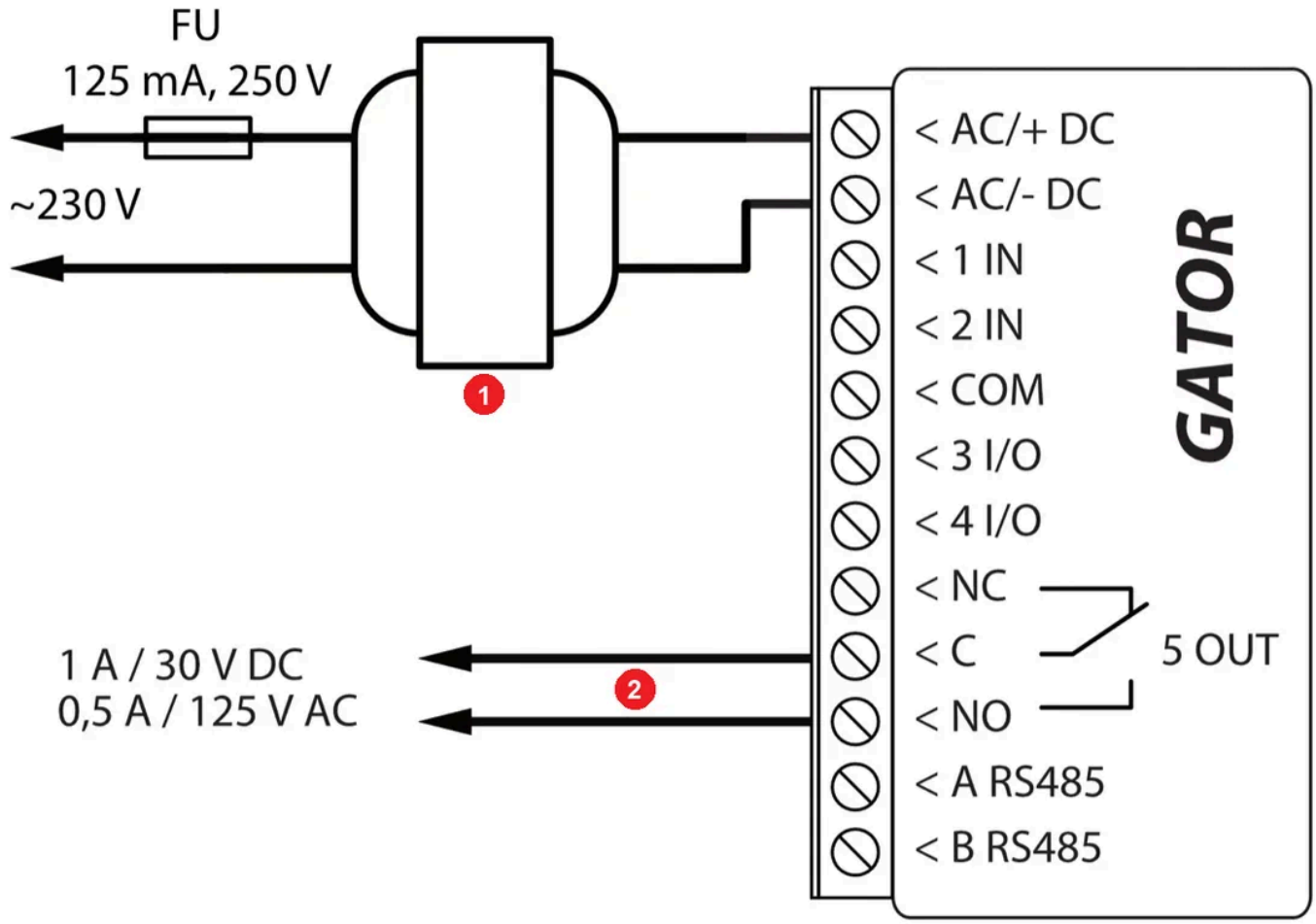


Figura 5. Conexión de la alimentación y del automatismo de la puerta: alimentación de red desde un transformador de ~230 V / 16 V, 10 VA, 50 Hz (fusible de 125 mA, 250 V) o desde una fuente de alimentación de corriente continua de 9–32 V, 0,2 A, a los bornes AC/+DC y AC/−DC; la entrada de control del automatismo a los contactos C y NO del relé; capacidad de carga del relé: 1 A / 30 V DC o 0,5 A / 125 V AC.

- 1 transformador, ~230 V / 16 V, 10 VA, 50 Hz („Transformer"), o fuente de alimentación de corriente continua, 9–32 V, 0,2 A („or DC power supply source")
- 2 control de la puerta („Gate control") – la entrada de control del automatismo de la puerta

En los esquemas, la alimentación de los lectores RFID, de los relés y de los módulos de expansión se toma del borne **AC/+DC**: esto solo es posible con alimentación de **corriente continua** (en los esquemas 9–16 V DC, 0,5 A; en los módulos W485 / E485 e iO8, 10–28 V DC). Con alimentación de corriente alterna, el lector y el módulo necesitan una fuente de alimentación DC aparte.

3.3 Entradas

El GATOR tiene **cuatro entradas**: **1 IN** y **2 IN** son siempre entradas; **3 I/O** y **4 I/O** son bornes universales que se pueden configurar como entrada o como salida. Todas funcionan respecto al borne **COM** y pueden ser de tipo **NO**, **NC** o **EOL** (con resistencia de fin de línea de 10 kΩ); el paquete incluye tres resistencias de fin de línea. A la entrada puedes conectar el final de carrera o la salida de estado de la puerta (indicación del estado de la puerta, apartados 3.5 y 5.10), un pulsador de salida (apartado 3.6) o cualquier detector o contacto de cuyo cambio quieras recibir un SMS o una notificación push, o con el que quieras conmutar una salida (**CTRL by IN**, apartado 5.3). El tipo y el tiempo de reacción se ajustan en la página **IN/OUT** de TrikdisConfig; de fábrica solo está activa la 1 IN (NO). Conecta las entradas según el tipo configurado (NC, NO, EOL), conforme al esquema siguiente.

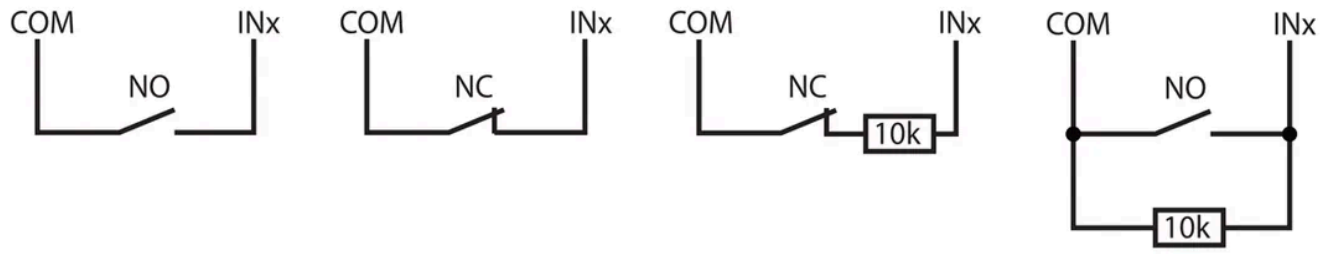


Figura 6. Las cuatro formas de conectar las entradas entre el borne COM y el borne IN. De izquierda a derecha: **NO** – contacto normalmente abierto – cierre = alarma, apertura = restablecimiento; **NC** – contacto normalmente cerrado – apertura = alarma, cierre = restablecimiento; **NC + EOL** – contacto normalmente cerrado con resistencia de 10 kΩ en serie – cortocircuito y corte = alarma, 10 kΩ = reposo; **NO + EOL** – contacto normalmente abierto con resistencia de 10 kΩ en paralelo – cortocircuito y corte = alarma, 10 kΩ = reposo.

3.4 Conexión de un relé a la salida universal

Como salida, los bornes **3 I/O** y **4 I/O** son de colector abierto, con una capacidad de carga de hasta **50 mA**: directamente solo pueden conmutar la bobina de un relé pequeño. Con los contactos del relé se puede encender y apagar a distancia cualquier equipo. El esquema corresponde a una alimentación de corriente continua: un extremo de la bobina va al borne **AC/+DC** y el otro a la salida; en TrikdisConfig la función del borne debe ajustarse a **Output** (apartado 5.3).

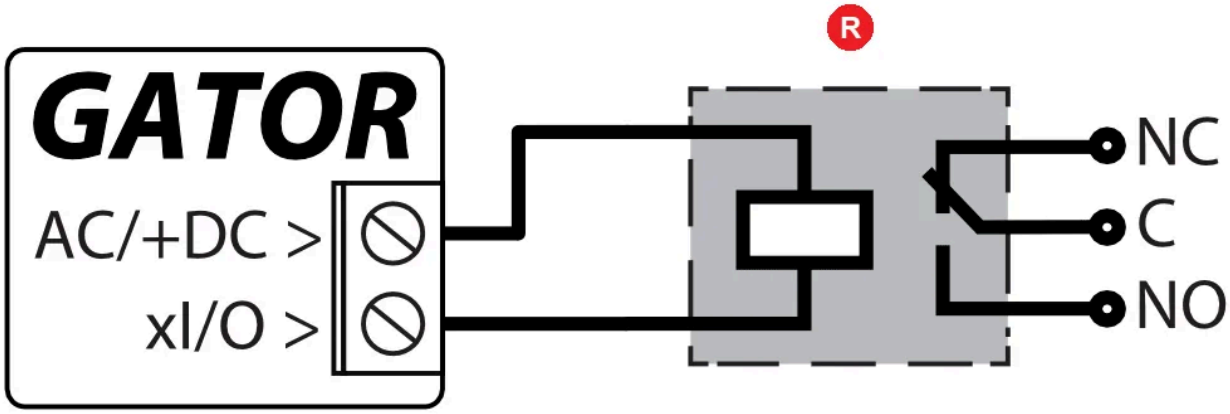


Figura 7. Relé externo en la salida universal: la bobina entre el borne AC/+DC y el borne 3 I/O o 4 I/O configurado como salida; los contactos NC, C y NO del relé conmutan el equipo.

- R relé („Relay")

3.5 Conexión del automatismo de la puerta

Haz siempre el conexionado sin tensión. Los bornes de la unidad de control del automatismo y su tensión nominal se describen en la documentación del motor de la puerta: el esquema solo muestra la disposición típica.

La puerta se abre mediante los bornes **IN** y **COM** (de control) del automatismo: aquí van los contactos **C** y **NO** del relé del GATOR, y el impulso del relé hace lo mismo que el botón del mando a distancia. La mayoría de los automatismos tienen una **salida de estado de la puerta** (OUT), que indica si la puerta está abierta o cerrada; puede ser una salida de tensión o una salida de relé. En el esquema, el relé auxiliar K1 está conectado a un automatismo con salida de tensión: con la puerta abierta se miden ~230 V entre los bornes OUT y N del automatismo, el relé K1 se activa y activa la entrada **1 IN** del GATOR. Así, el estado de la 1 IN sigue

exactamente la posición de la puerta, que también muestran Protegus 2 y el icono del widget; el ajuste correspondiente está en el apartado 5.10. Con un automatismo con salida de relé, el K1 no hace falta: el contacto de estado se puede conectar directamente entre 1 IN y COM.

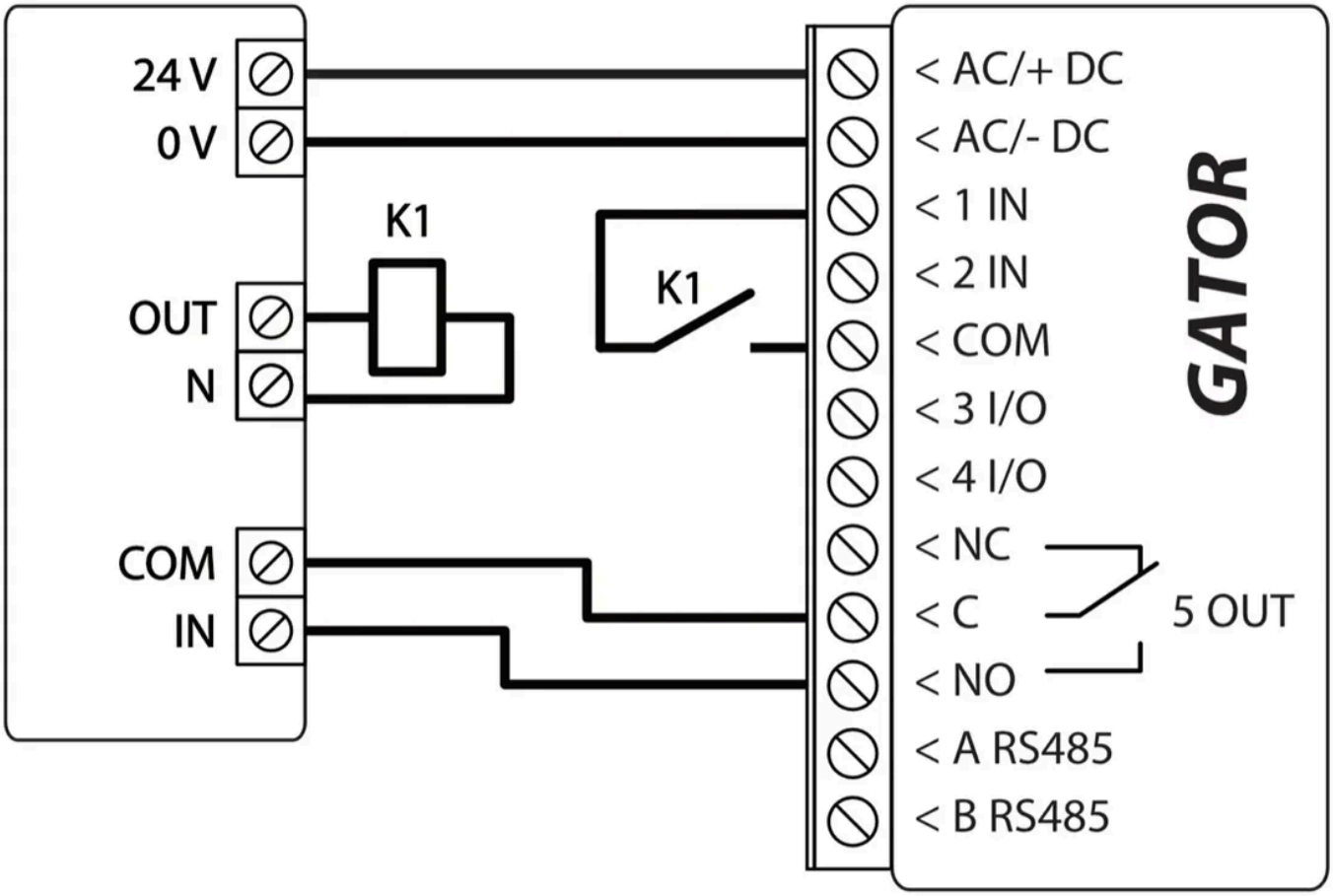


Figura 8. Conexión de la unidad de control del automatismo („Gate control unit") con el GATOR mediante el relé auxiliar K1. Alimentación („Power"): la salida de alimentación de 24 V del automatismo al borne AC/+DC del GATOR, los 0 V al borne AC/−DC; estado de la puerta („Gate status"): los bornes OUT y N del automatismo a la bobina del relé K1, el contacto del K1 entre los bornes 1 IN y COM del GATOR; control de la puerta („Gate control"): el borne COM del automatismo al contacto C de la 5 OUT del GATOR, el borne IN al contacto NO de la 5 OUT.

3.6 Conexión del lector RFID (Wiegand 26/34)

El GATOR admite uno o dos lectores RFID con protocolo **Wiegand 26/34** (lectores de tarjetas y también lectores con teclado de código). Con las tarjetas y los códigos dados de alta en la lista de usuarios, el lector conmuta la salida **5 OUT** (el permiso, el horario y el contador de cada usuario también se aplican al lector). El lector se configura en la página **IN/OUT** de TrikdisConfig (apartado 5.3) y las tarjetas se dan de alta en la página **User list** (apartado 5.6); el código de colores de los cables sigue el estándar Wiegand: rojo +U, negro GND, verde D0, blanco D1.

Un lector: D0 va al borne **1 IN**, D1 al borne **2 IN**, y el pulsador de salida entre **COM** y **3 I/O**. En el programa, el **Wiegand reader mode** debe ser **Single Reader** y, si hay botón de salida, marca la casilla **IO3 as exit button (5 OUT)**: al pulsar el botón, la 5 OUT se activa durante el tiempo de impulso configurado. Si no hay botón, deja la casilla sin marcar.

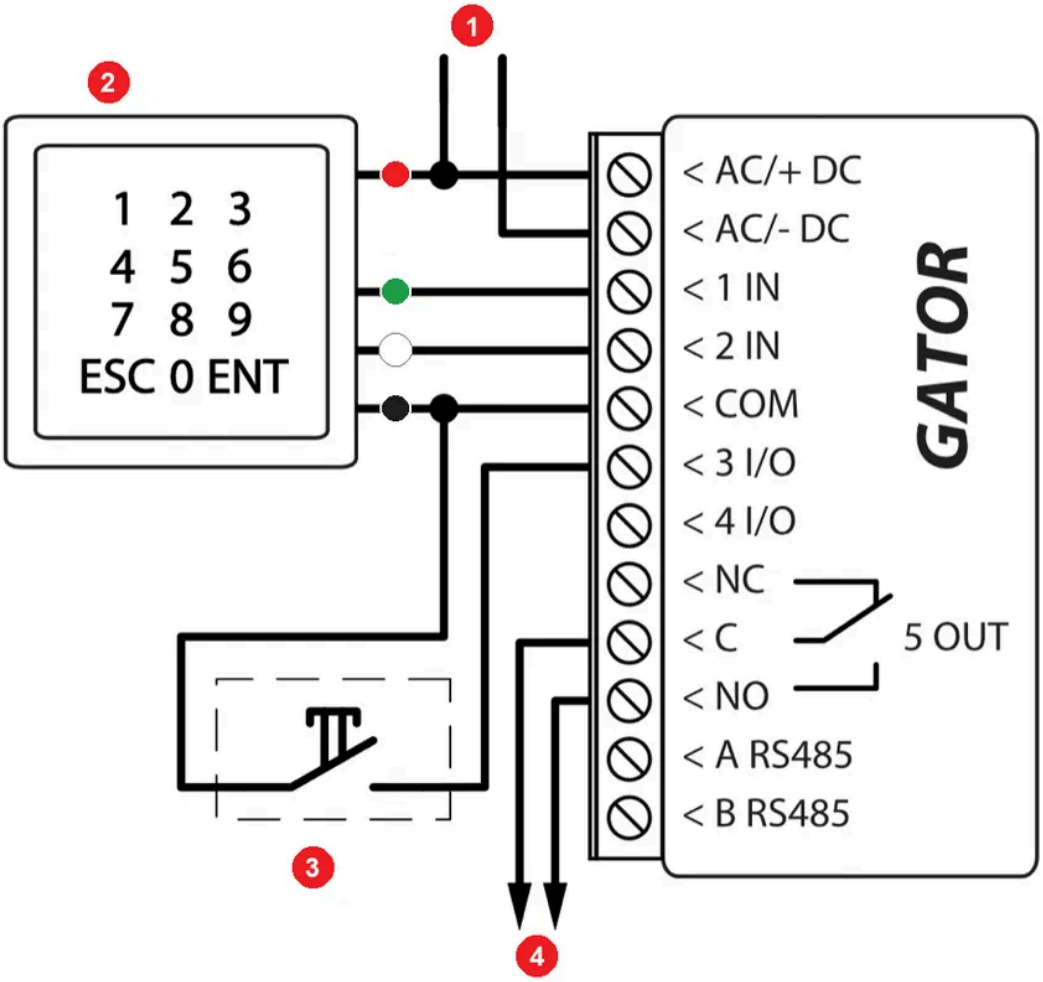


Figura 9. Conexión de un lector Wiegand 26/34 y del botón de salida: alimentación de corriente continua, 9–16 V, 0,5 A, a los bornes AC/+DC y AC/−DC; el cable rojo (+U) del lector de entrada al borne AC/+DC, el verde (D0) a 1 IN, el blanco (D1) a 2 IN, el negro (GND) a COM; el pulsador de salida entre los bornes COM y 3 I/O; el automatismo de la puerta en los contactos C y NO del relé (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 fuente de alimentación de corriente continua („DC power supply"), 9–16 V, 0,5 A
- 2 lector de entrada („Entry reader") – lector RFID con teclado, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)")
- 3 pulsador de salida („»Exit« button")
- 4 control de la puerta („Gate control") – la entrada de control del automatismo; capacidad de carga del relé: 1 A / 30 V DC, 0,5 A / 125 V AC
- cable rojo, +U („R - red (+U)")
- cable negro, GND („B - black (GND)")
- cable blanco, D1 („W - white (D1)")
- cable verde, D0 („G - green (D0)")

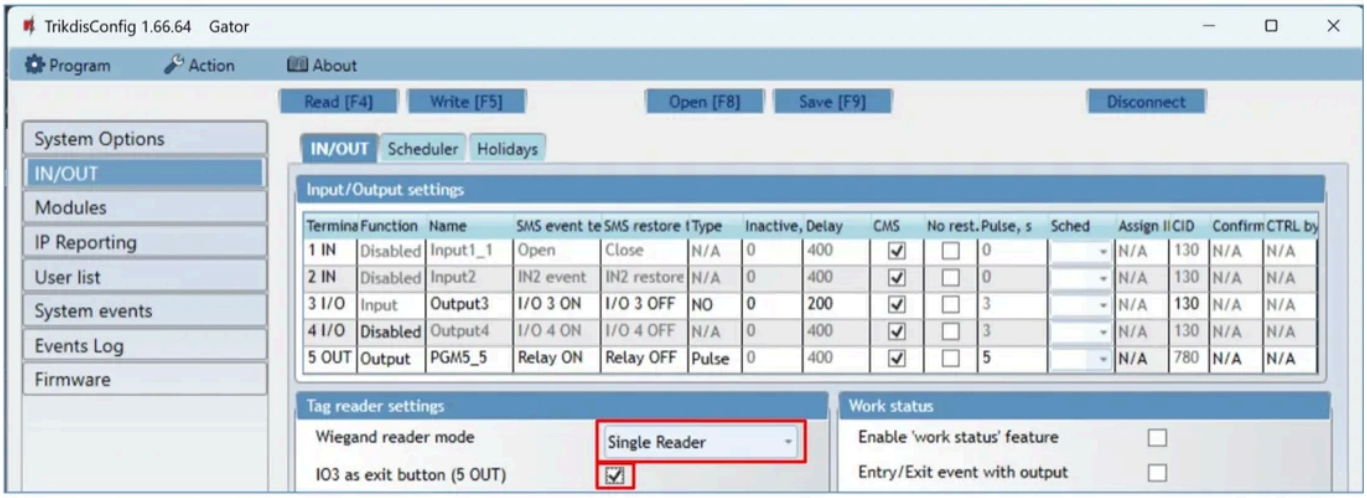


Figura 10. TrikdisConfig – IN/OUT, **Tag reader settings**: con un lector, **Wiegand reader mode = Single Reader**; con botón de salida, **IO3 as exit button (5 OUT)** marcado.

Dos lectores (entrada y salida): los cables D0 / D1 del primer lector van a los bornes **1 IN** / **2 IN** y los del segundo a los bornes **3 I/O** / **4 I/O**; en el programa, **Wiegand reader mode = Dual Reader**. Con dos lectores, la 3 I/O está ocupada y no se le puede conectar un botón de salida.

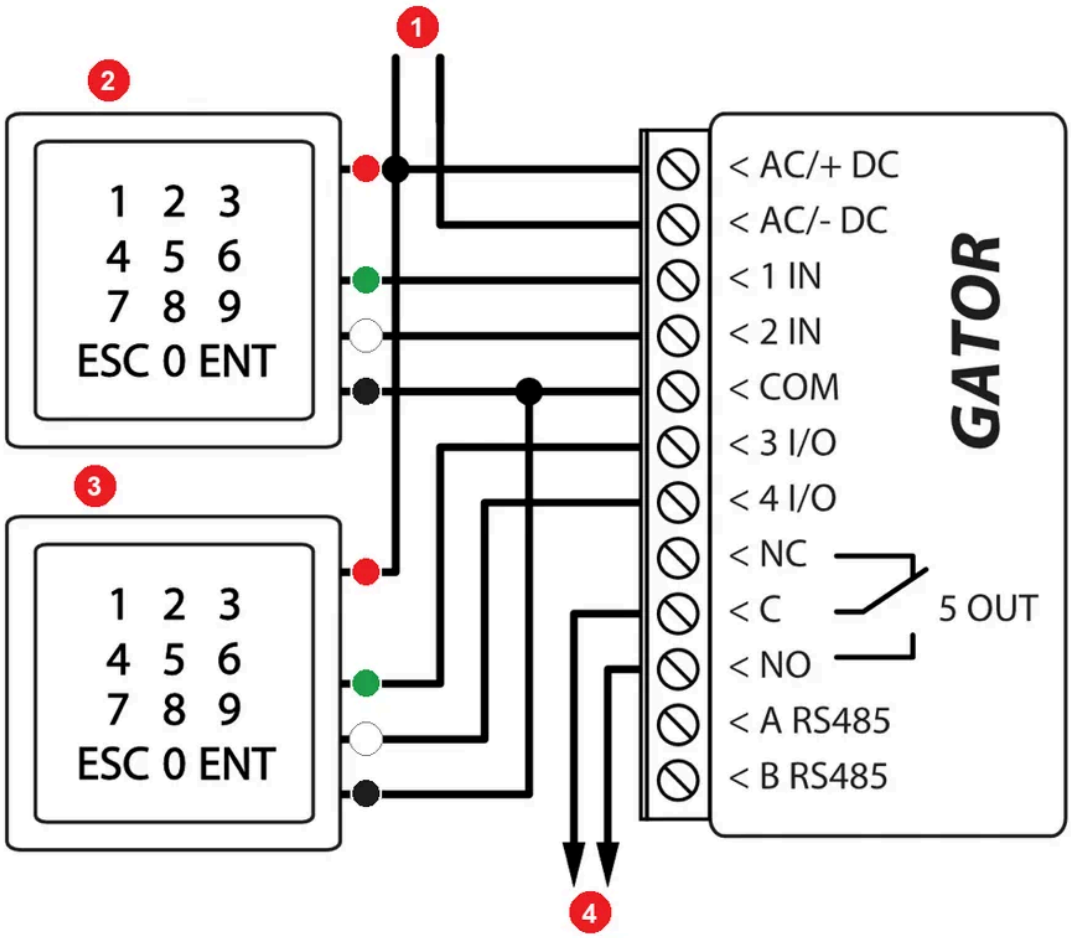


Figura 11. Conexión de dos lectores Wiegand 26/34, ambos lectores RFID con teclado („RFID reader with keypad (Wiegand 26/34)"): alimentación de corriente continua, 9–16 V, 0,5 A; el cable verde (D0) del lector de entrada al borne 1 IN, el blanco (D1) a 2 IN; el cable verde (D0) del lector de salida al borne 3 I/O, el blanco (D1) a 4 I/O; el cable rojo (+U) de ambos lectores al borne AC/+DC, el negro (GND) a COM; el automatismo de la puerta en los contactos C y NO del relé (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 fuente de alimentación de corriente continua („DC power supply"), 9–16 V, 0,5 A
- 2 lector de entrada („Entry reader")
- 3 lector de salida („Exit reader")
- 4 control de la puerta („Gate control") – la entrada de control del automatismo; capacidad de carga del relé: 1 A / 30 V DC, 0,5 A / 125 V AC
- cable rojo, +U („R - red (+U)")
- cable negro, GND („B - black (GND)")
- cable blanco, D1 („W - white (D1)")
- cable verde, D0 („G - green (D0)")

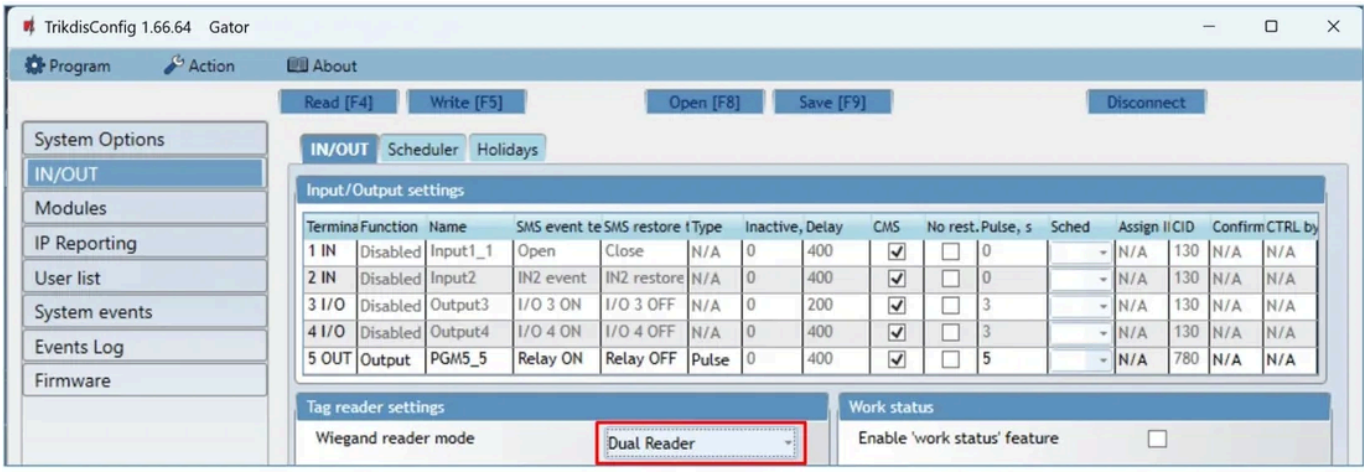


Figura 12. TrikdisConfig – IN/OUT, **Tag reader settings**: con dos lectores, **Wiegand reader mode = Dual Reader**.

Si el lector tiene salida de 5 V (baja tensión), marca la casilla **Low voltage reader**; si el lector da impulsos muy cortos y no reconoce la tarjeta, desactiva el filtro interno con la casilla **Disable reader filter** (apartado 5.3).

3.7 Módulo WiFi W485

El módulo **W485** envía los mensajes del GATOR a la CRA y a la aplicación Protegus 2 a través de la red WiFi local y del router de internet, de modo que no se consumen datos móviles. Si se interrumpe la WiFi, el equipo pasa por sí solo a la red móvil y, cuando vuelve la WiFi, regresa al W485. La función está disponible desde el firmware **1.06** del GATOR. El módulo se conecta al bus **RS485** (A–A, B–B), con cable de alarma, a **hasta 100 m**, y funciona con la misma alimentación de 10–28 V DC que el GATOR. **Con el W485, el GATOR también se puede usar sin tarjeta SIM**: en ese caso solo se puede controlar desde la aplicación, sin llamadas ni SMS. La configuración del módulo está en el apartado 5.4.

Trikdis W485 módulo WiFi (RS485)

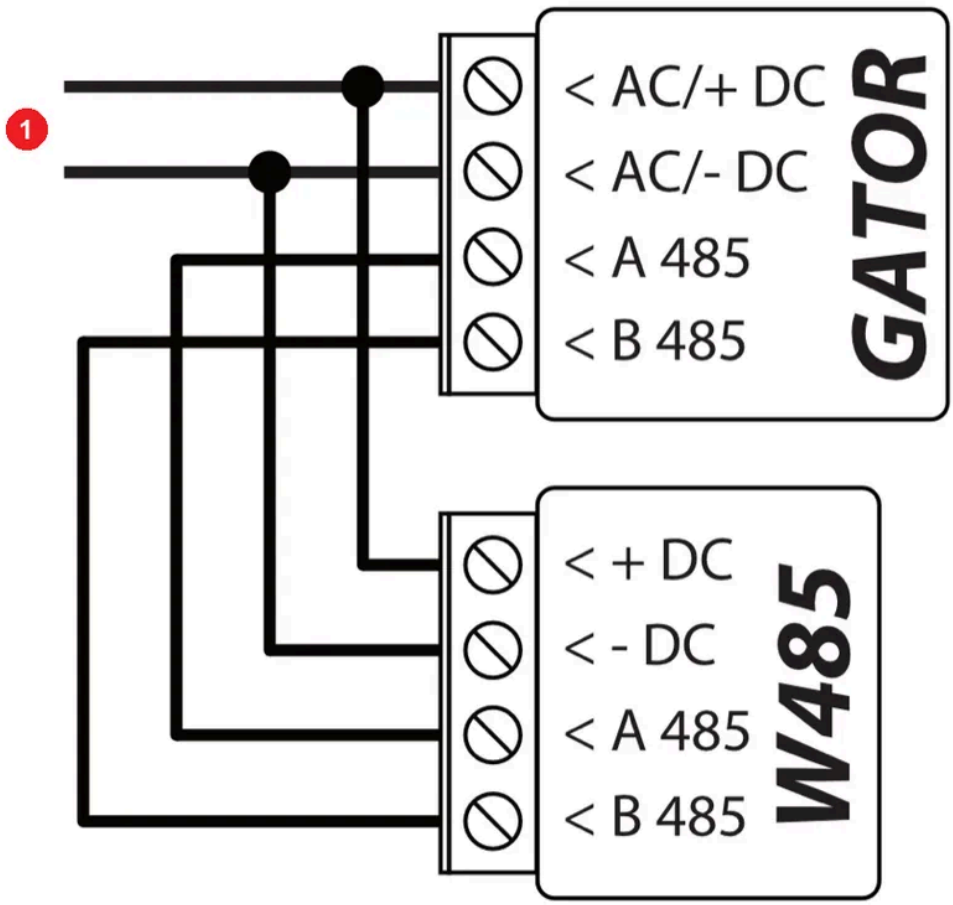


Figura 13. Conexión del módulo W485: el polo positivo de la fuente de alimentación de 10–28 V DC, 0,5 A al borne AC/+DC del GATOR y al +DC del W485, el negativo a AC/−DC y a −DC; conexión RS485 („RS485 connection"), hasta 100 m („up to 100m"): A 485 – A 485, B 485 – B 485.

- 1 fuente de alimentación („Power supply"), 10–28 V DC, 0,5 A

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.

3.8 Módulo Ethernet E485

El módulo **E485** hace lo mismo con internet por cable: los mensajes del GATOR van a la CRA y a la aplicación Protegus 2 por el cable Ethernet conectado al router; el equipo no usa internet móvil y la red móvil solo es de reserva: si se interrumpe internet por cable, envía los mensajes por internet móvil y, cuando vuelve la conexión por cable, otra vez por el E485. Desde el firmware **1.06**; bus RS485 de hasta 100 m; alimentación común de 10–28 V DC; también se puede usar sin tarjeta SIM. La configuración está en el apartado 5.4.

Trikdis E485 módulo Ethernet (RS485)

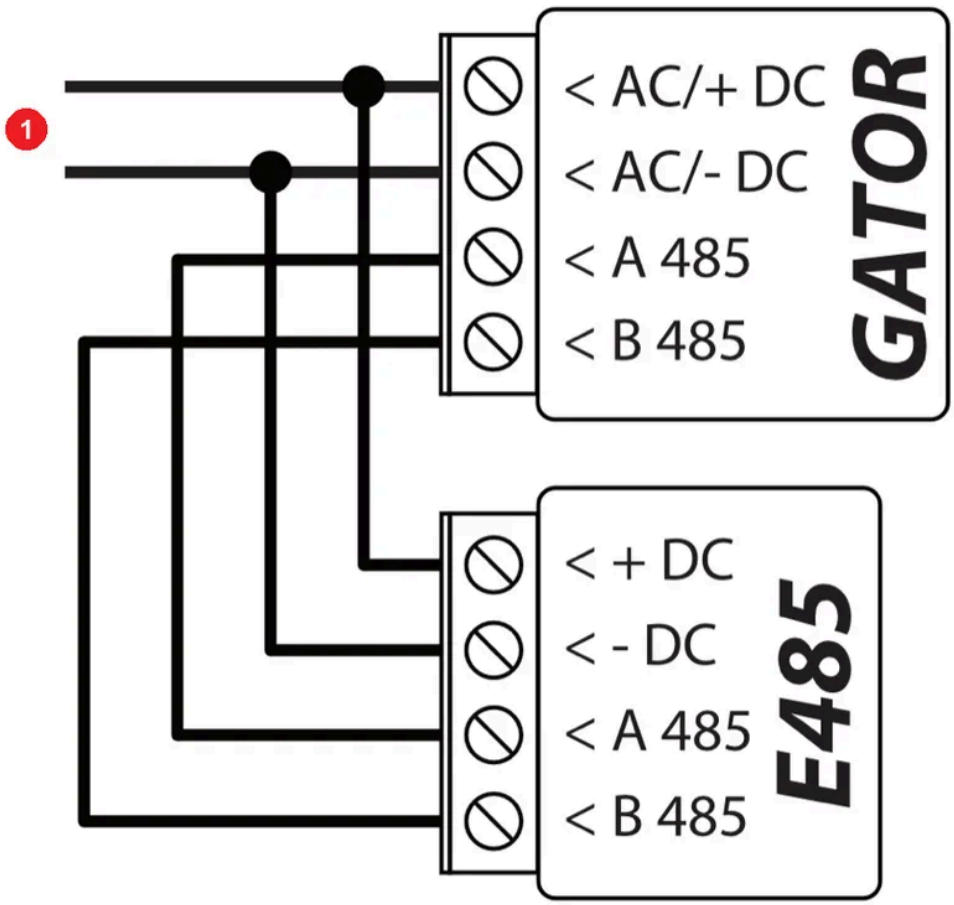


Figura 14. Conexión del módulo E485: el polo positivo de la fuente de alimentación de 10–28 V DC, 0,5 A al borne AC/+DC del GATOR y al +DC del E485, el negativo a AC/−DC y a −DC; conexión RS485 („RS485 connection"), hasta 100 m („up to 100m"): A 485 – A 485, B 485 – B 485.

- 1 fuente de alimentación („Power supply"), 10–28 V DC, 0,5 A

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.

3.9 Expansores RF-LORA e iO-LORA con lector RFID

Desde el firmware **2.13** del GATOR, el sistema se puede ampliar de forma inalámbrica: el transceptor **RF-LORA** se conecta al bus RS485 y mantiene por radio la conexión con hasta **8 expansores iO-LORA** (en campo abierto, hasta 5000 m). Cada expansor iO-LORA amplía el GATOR con una entrada y una salida de relé, y se le puede conectar su propio lector RFID Wiegand 26/34: el lector conmuta **solo** la salida de relé **de su propio expansor**, no una salida remota. Así, con un solo GATOR se pueden controlar hasta 8 puertas o barreras alejadas entre sí, cada una con su propio lector de tarjetas y su botón de salida – detalles de la solución: Control de acceso inalámbrico y flexible con el sistema GATOR RF-LoRa.

Trikdis RF-LORA módulo expansor inalámbrico

Trikdis IO-LORA módulo expansor inalámbrico

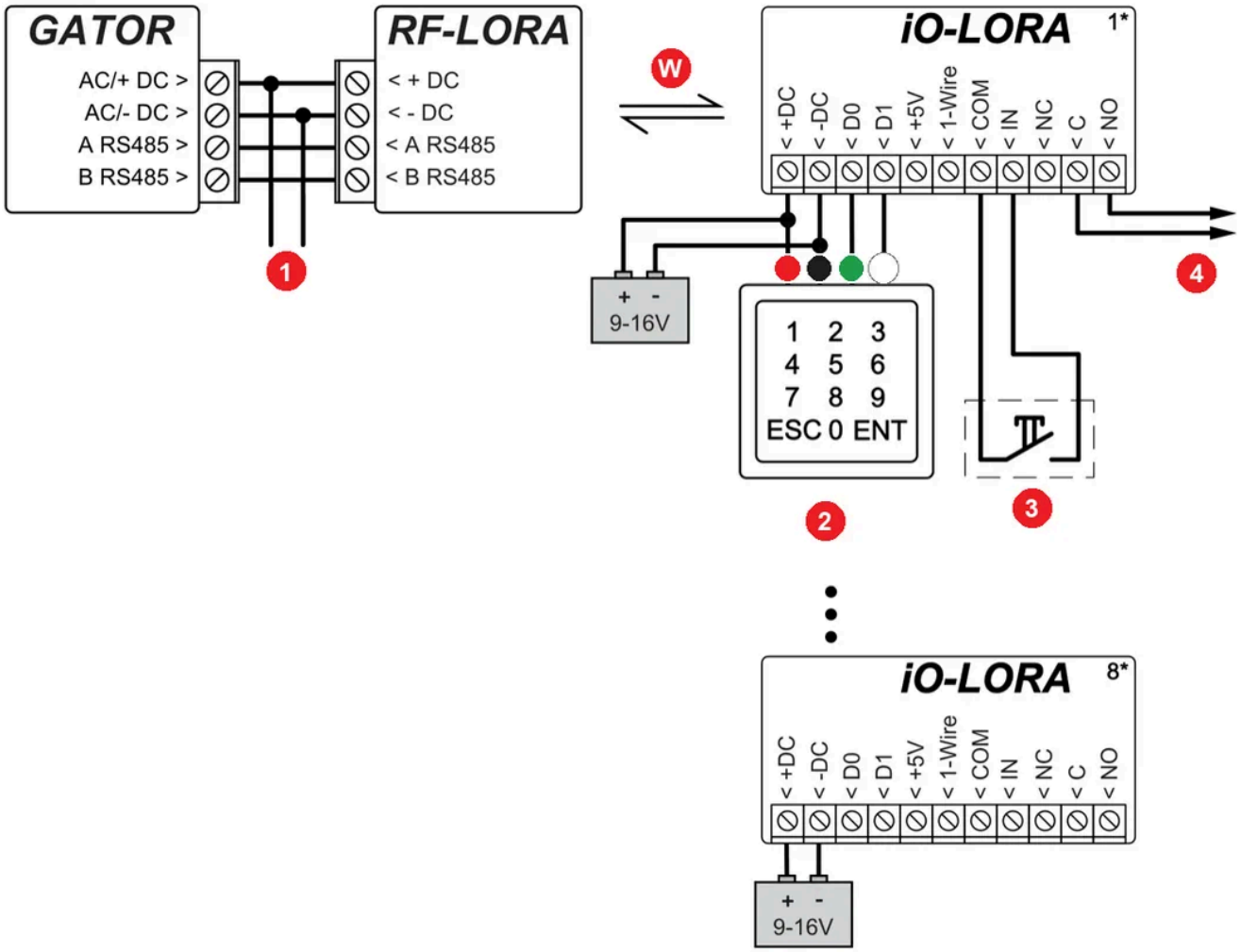


Figura 15. Transceptor RF-LORA en el GATOR y expansores iO-LORA con lector RFID: alimentación común de 9–16 V DC, 0,5 A para el GATOR y el RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A–A, B–B; conexión por radio entre el RF-LORA y los expansores iO-LORA 1…8, hasta 5000 m; cada iO-LORA tiene su propia alimentación de 9–16 V; el lector en el iO-LORA: rojo (+U) al borne +DC, negro (GND) a −DC, verde a D0, blanco a D1; pulsador de salida entre los bornes COM e IN del iO-LORA; el automatismo de la puerta en los contactos C y NO del relé del iO-LORA (2 A / 230 V AC).

- 1 fuente de alimentación de corriente continua („DC power supply"), 9–16 V, 0,5 A
- W conexión inalámbrica („Wireless connection"), hasta 5000 m („up to 5000 m")
- 2 lector RFID con teclado, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)")
- 3 pulsador de salida („»Exit« button")
- 4 control de la puerta („Gate control") – la entrada de control del automatismo; capacidad de carga del relé del iO-LORA: 2 A / 230 V AC
- cable rojo, +U („R - red (+U)")
- cable negro, GND („B - black (GND)")
- cable verde, D0 („G - green (D0)")
- cable blanco, D1 („W - white (D1)")

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.

Configuración en TrikdisConfig (la descripción de las ventanas está en el capítulo 5):

1. Inicia TrikdisConfig, conecta el GATOR al ordenador con un cable USB Mini-B o entra a distancia, y lee la configuración (**Read [F4]** – el programa muestra la configuración actual del equipo). Si el programa lo pide, introduce el código de administrador o de instalador de 6 dígitos en la ventana emergente. En la

página **Modules**, selecciona en la lista el elemento **iO-LORA controller** y escribe en el campo **Serial No.** el número de serie de seis dígitos del expansor (en la etiqueta del expansor). El RF-LORA no hace falta darlo de alta aparte.



Figura 16. TrikdisConfig – Modules: el expansor iO-LORA seleccionado; en el campo **Serial No.** va el número de serie.

2. Para cada expansor iO-LORA dado de alta aparecen en la lista de la página **IN/OUT** una entrada (por ejemplo **6 IN iO-LORA 1**) y una salida (**7 OUT iO-LORA 1**). La función de la entrada debe ser **Exit button** (aquí conectan los bornes IN y COM del expansor el botón de salida): al pulsarlo, el relé del expansor (en el ejemplo **7 OUT**) se activa durante el tiempo de impulso configurado. El tipo de salida es **Pulse** y el tiempo de impulso es el adecuado para el automatismo de la puerta (en el ejemplo 3 s).

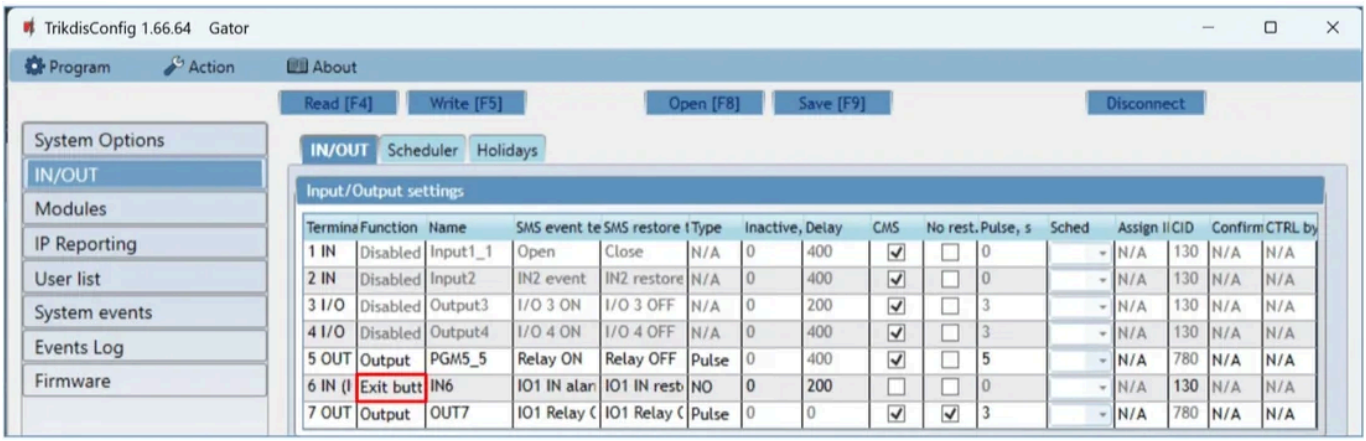


Figura 17. TrikdisConfig – IN/OUT: la función de la **6 IN** es **Exit button**; la salida **7 OUT** es de tipo **Pulse**, con un impulso de 3 s.

3. En la página **User list**, introduce el nombre del usuario, el número de la tarjeta RFID (**Phone/RFID**) y, con un lector de código, el código; marca la casilla **En** e indica qué salida puede controlar (en el ejemplo, la 7). Escribe la configuración (**Write [F5]**), espera a que termine la actualización y luego pulsa **Disconnect** y desconecta el cable USB.

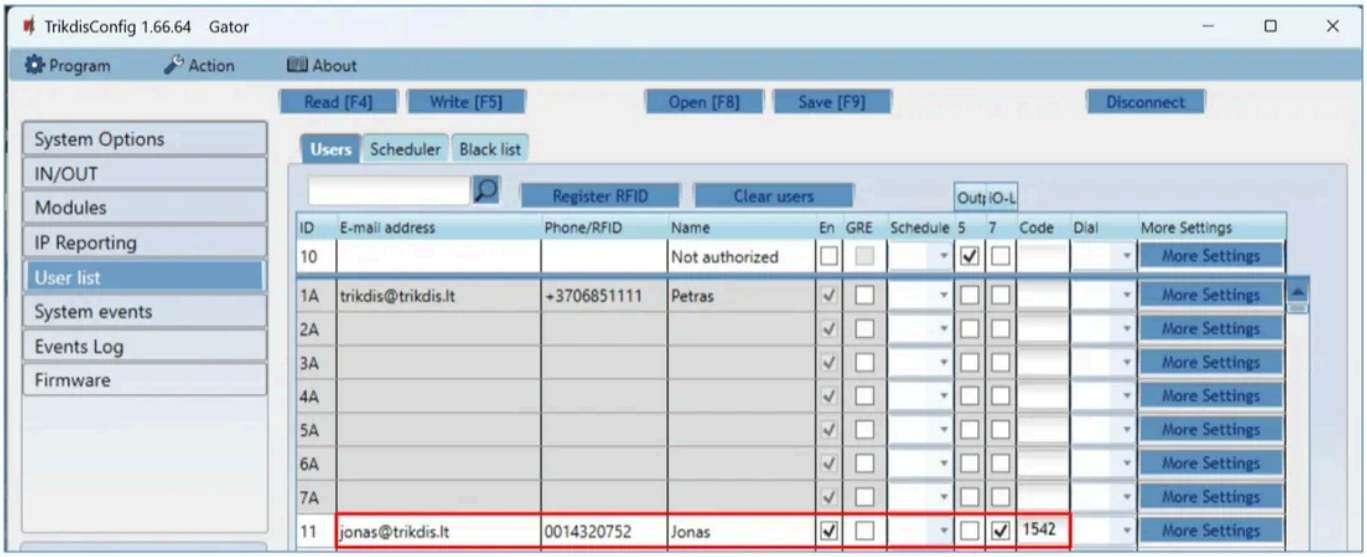


Figura 18. TrikdisConfig – User list: en el usuario están rellenados el número RFID, el nombre y el código, **En** marcado y la salida 7 seleccionada.

4. **Comprobación:** activa la salida con la tarjeta o con el código y, después, pulsa el botón de salida: las dos veces el relé debe activarse durante el tiempo de impulso configurado.

3.10 Expansores iO8 e iO8-LORA

Si necesitas más entradas o salidas en un mismo lugar, al GATOR se le puede conectar **un** expansor **iO8** (por cable, RS485) o **iO8-LORA** (inalámbrico, a través del RF-LORA). Las entradas y salidas del expansor aparecen en la lista de la página **IN/OUT** y se gestionan igual que las propias del GATOR; el módulo debe darse de alta en la página **Modules** con su número de serie (apartado 5.4).

Trikdis iO8 módulo expansor cableado | **Trikdis IO8-LORA módulo expansor inalámbrico**

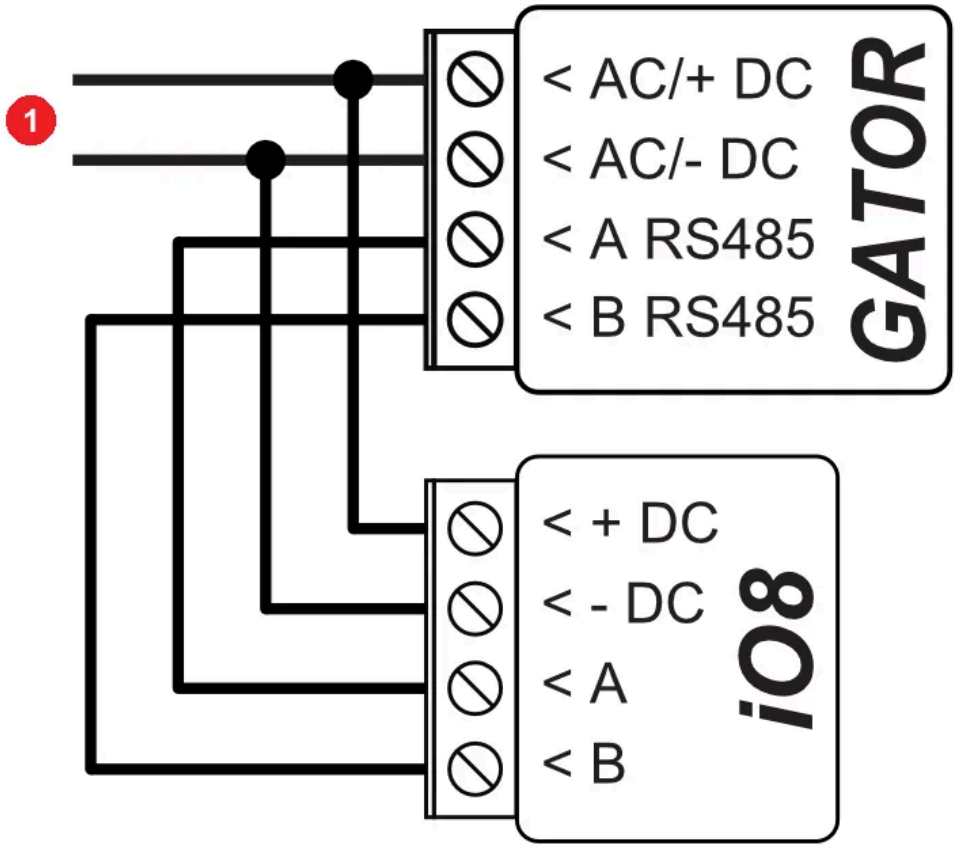


Figura 19. Conexión del expansor iO8: el polo positivo de la fuente de alimentación de 10–28 V DC, 0,5 A al borne AC/+DC del GATOR y al +DC del iO8, el negativo a AC/−DC y a −DC; conexión RS485 („RS485 connection"), hasta 100 m („up to 100m"): el borne A RS485 del GATOR al borne A del iO8, el B RS485 al borne B.

- 1 fuente de alimentación („Power supply"), 10–28 V DC, 0,5 A

El iO8 funciona con 10–26 V DC: si la fuente de alimentación da más de 26 V, el iO8 recibe una fuente de alimentación aparte, uniendo el polo negativo de las dos fuentes.

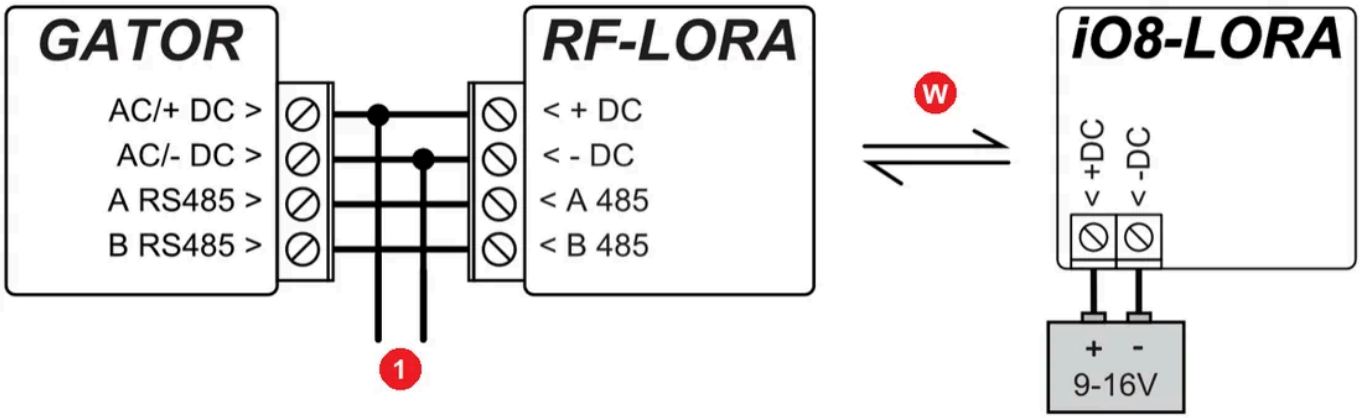


Figura 20. El expansor iO8-LORA a través del transceptor RF-LORA: alimentación de 9–16 V DC, 0,5 A para el GATOR y el RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A RS485 – A 485, B RS485 – B 485; conexión por radio entre el RF-LORA y el iO8-LORA, hasta 5000 m; el iO8-LORA tiene su propia alimentación de 9–16 V.

- 1 fuente de alimentación de corriente continua („DC power supply"), 9–16 V, 0,5 A
- W conexión inalámbrica („Wireless connection"), hasta 5000 m („up to 5000 m")

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

puesta en marcha.

4. Control a distancia

El GATOR se puede controlar de cuatro maneras: con una **llamada telefónica** (gratuita, porque el equipo no contesta la llamada), durante la llamada con el **teclado del teléfono** (DTMF), desde la aplicación **Protegus 2** o con un **widget** colocado en la pantalla de inicio del teléfono, y con un **comando SMS**. En los cuatro modos, la lista de usuarios (apartado 5.6) decide quién puede hacer qué; con los comandos SMS, el administrador también puede modificar la configuración.

4.1 Control con una llamada telefónica

Llama al número de la tarjeta SIM colocada en el GATOR. El equipo **rechaza automáticamente** la llamada y activa la salida de relé **5 OUT** durante **3 segundos**: la llamada no cuesta nada. De fábrica, cualquiera que conozca su número puede controlar así el equipo.

- **Solo los autorizados**: si añades a la lista de usuarios aunque sea un solo número (por SMS: `SETU …`, apartado 4.7; en TrikdisConfig o en la aplicación), el GATOR solo reacciona a las llamadas de los números que están en la lista. En TrikdisConfig lo mismo se conmuta con la casilla **En** de la entrada número 10, llamada **Not authorized**, de la **User list** (apartado 5.6): marcada, puede llamar cualquiera; sin marcar, solo los miembros de la lista.
- **Qué salida abre**: si un usuario puede controlar varias salidas, con la llamada conmutan las salidas marcadas en la columna **Dial**; después el equipo cuelga.
- **Duración de la llamada**: con el valor **System Options** → **Hang-up after** en 0, el equipo rechaza la llamada al instante; con un valor mayor, la contesta y cuelga pasado el tiempo indicado; esto es necesario para el control con el teclado (apartado 4.2).

Quien llame **por primera vez** al GATOR con la configuración de fábrica, o le envíe el primer SMS, se convierte en el **administrador** del equipo: a partir de entonces solo él puede gestionarlo con comandos SMS. Por eso, haz la primera llamada desde el teléfono del propietario o del instalador.

4.2 Control con el teclado del teléfono (DTMF)

Si el GATOR contesta la llamada (**Hang-up after** mayor que 0), el usuario puede conmutar varias salidas con el teclado del teléfono:

1. Llama al número de la tarjeta SIM del GATOR: el equipo contesta la llamada.
2. Marca el comando de control en el teclado del teléfono según la tabla.

Código DTMF	Función	Descripción
`SALIDA*ESTADO#`	control de la salida	**SALIDA** – el número de la salida. **ESTADO** – 0: apagar; 1: encender; 2: apagar durante el tiempo de impulso; 3: encender durante el tiempo de impulso (el tiempo de impulso se ajusta en la tabla **IN/OUT** de TrikdisConfig). **#** – fin del comando. Ejemplo – encender la salida 5: `5*1#`; encender la salida 4 durante el tiempo de impulso: `4*3#`
`#`	fin del comando	si te has equivocado al marcar el comando, pulsa la tecla **#** y vuelve a marcarlo

El control con el teclado (DTMF) no funciona en los equipos con código de tipo **GV17_2E70** y **GV17_2S70**. El tipo exacto lo ves en la barra de estado de TrikdisConfig (apartado 5.1).

4.3 Control desde la aplicación Protegus 2

En Protegus 2, el usuario abre la puerta desde cualquier lugar, ve el estado del sistema y el estado de la puerta (si el estado de la puerta está conectado, apartados 3.5 y 5.10), recibe todos los eventos del sistema como notificación push y, como administrador, también gestiona los usuarios. La aplicación es gratuita; en el teléfono se descarga de las tiendas de aplicaciones y en el navegador se abre en https://web.protegus.app.

Antes de añadir el sistema

En TrikdisConfig, en la página **IP Reporting**, debe estar marcado **Enable cloud service** (apartado 5.5; por SMS: `CONNECT 123456 PROTEGUS=ON`), la alimentación debe ser correcta (el LED **POWER** parpadea en verde) y el equipo debe estar en la red (el LED **NETWORK** se enciende en verde y parpadea en amarillo). La tarjeta SIM debe tener servicio de datos móviles o debe haber un módulo W485 / E485.

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

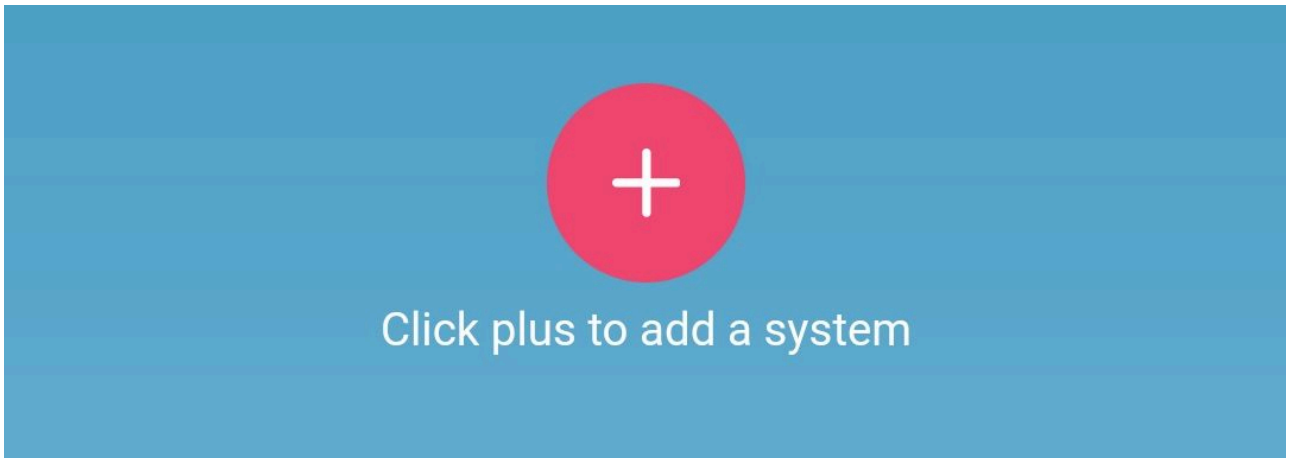
A rendszer létrehozása a Protegus 2 alkalmazásban

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



2. Regisztrálj egy fiókot, ha még nincs.

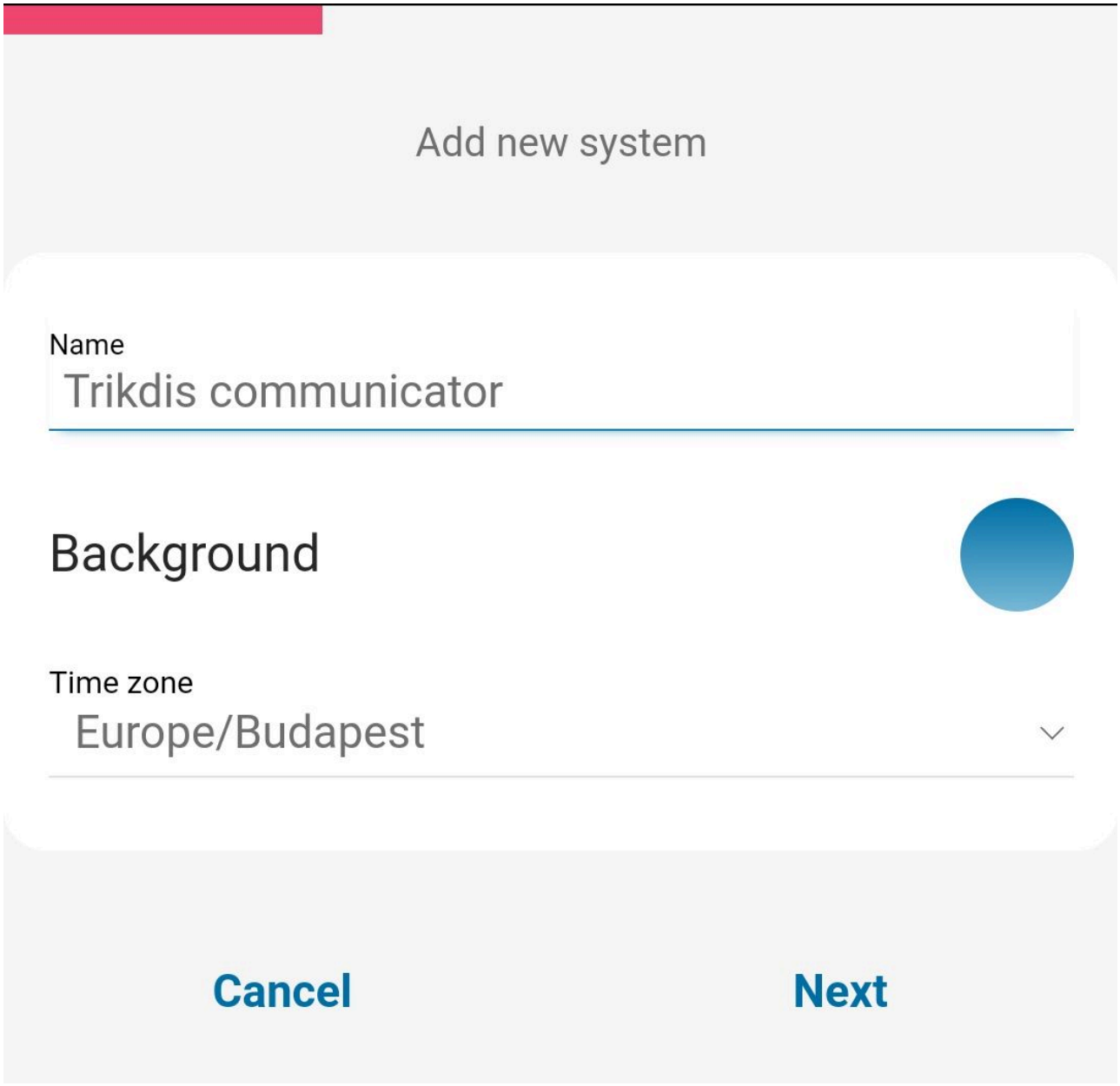
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



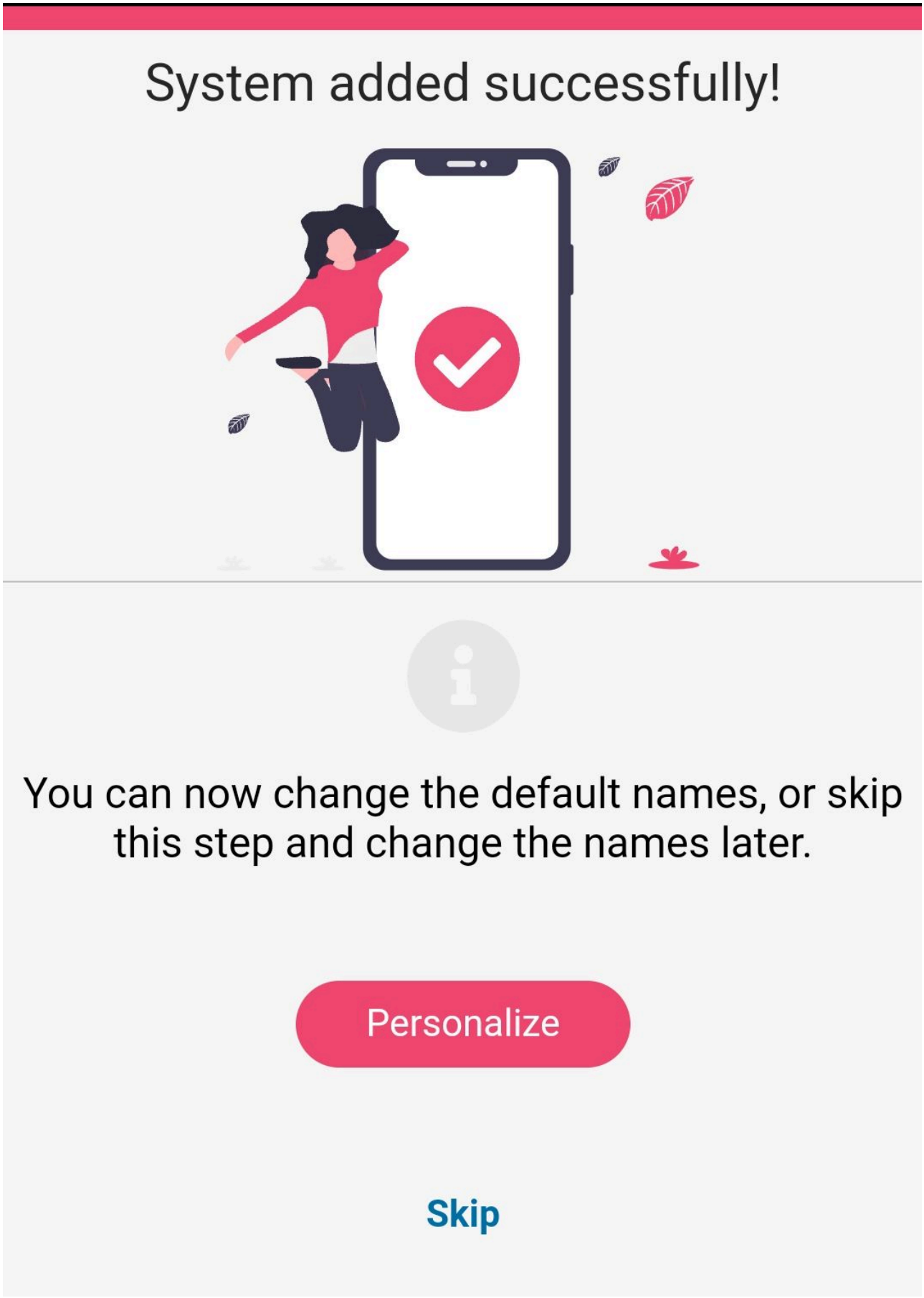
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



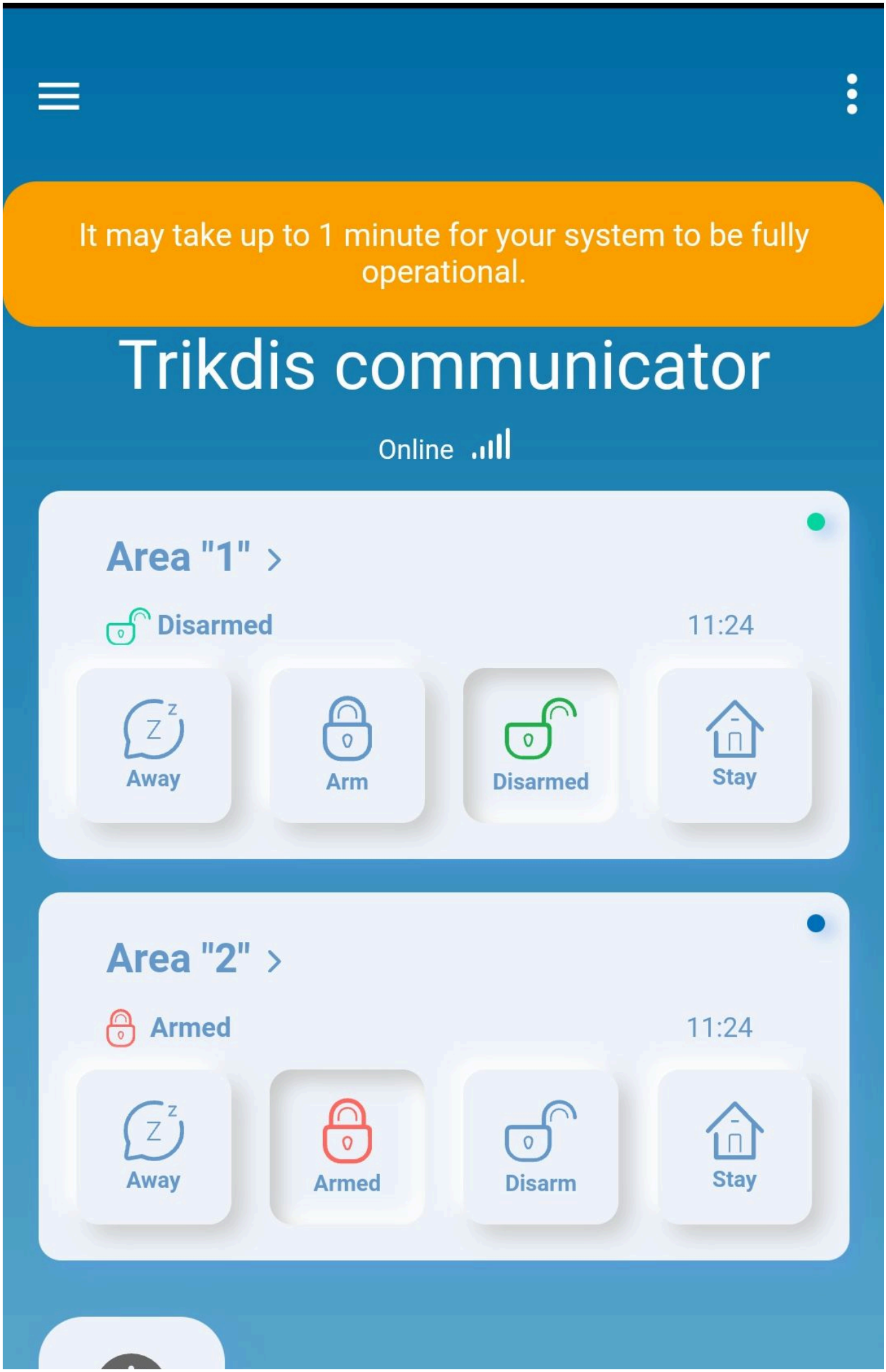
6. Add meg a rendszer nevét és válassz idozónát



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



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


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



Al añadir el GATOR, ten en cuenta lo siguiente:

1. El identificador único es el número **IMEI** del GATOR: está en la etiqueta de la parte inferior del equipo y de la caja, y también lo ves en la barra de estado de TrikdisConfig; el código QR de la etiqueta también se puede leer con la cámara del teléfono. Si el instalador ha cambiado el valor de fábrica `123456` del **Cloud Access Code**, la aplicación también lo pide.
2. Después de introducir el nombre del sistema, puedes saltarte el paso **Personalize** con el botón **Skip**: los nombres de las salidas y entradas se pueden cambiar también más tarde.
3. Espera a que desaparezca el aviso con fondo amarillo: el sistema queda operativo en 1 minuto como máximo.

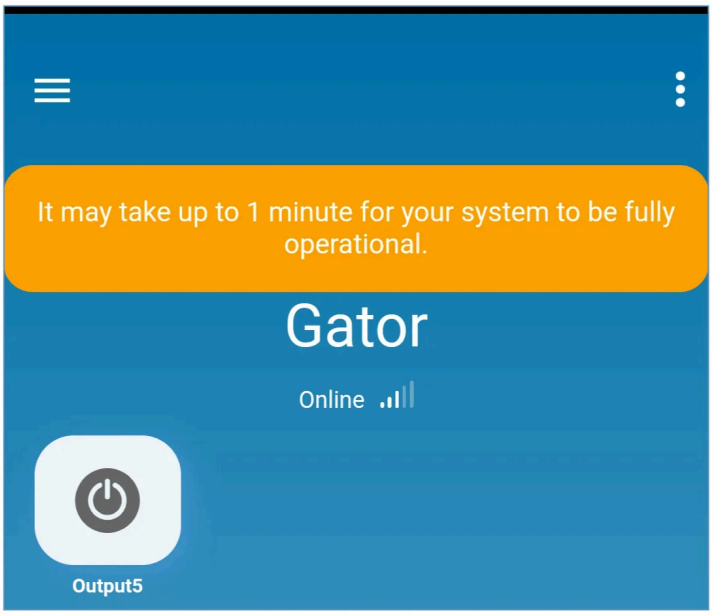


Figura 21. El GATOR en Protegus 2 después de añadirlo: el sistema está **Online**; la franja amarilla indica que hay que esperar como máximo 1 minuto hasta el funcionamiento completo.

4. La puerta se abre con el botón **Output5**. **Consejo:** mantén pulsado el botón, elige editar y, tocando el icono, elige uno adecuado para el uso (puerta, barrera, garaje) y guárdalo. Si el estado de la puerta está conectado, el icono también muestra si la puerta está abierta o cerrada.

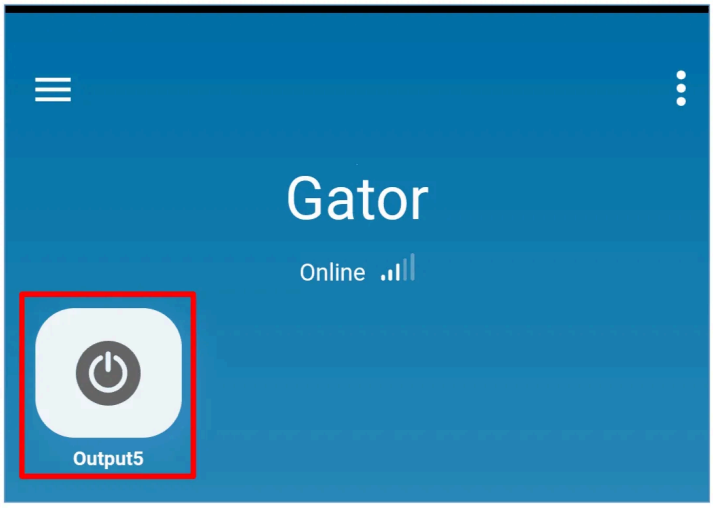


Figura 22. La pantalla de inicio del sistema con el botón **Output5**: este conmuta el relé del GATOR.

Ver también

El equipo de automatización de puertas GV17 se puede usar con Protegus 2 · Protegus: aplicación para Android / iPhone y web · Notificaciones push en el navegador en la aplicación Protegus 2

4.4 Widget en la pantalla de inicio del teléfono

El botón de apertura de la puerta también se puede poner en la pantalla de inicio del teléfono, de modo que abres con un toque, sin abrir la aplicación. **Solo funciona en Android**; la forma de colocar el widget puede variar un poco según el teléfono. El GATOR debe estar añadido a Protegus 2 y debes haber iniciado sesión en la aplicación; después, cierra la ventana de la aplicación.

1. Mantén pulsada una zona vacía de la pantalla de inicio y, en la barra que aparece, elige **Widgets**.
2. Busca **Protegus 2** en la lista y elige el widget **Switch Protegus 2**.
3. Selecciona la salida que quieres controlar (por ejemplo **Gator Output5**) y pulsa el botón **ADD WIDGET**.
4. El botón aparece en la pantalla de inicio. Pruébalo: vuelve a la pantalla de inicio y pulsa el botón; después de pulsarlo, un indicador circular muestra que la salida se ha activado; con el estado de la puerta conectado, el color del botón muestra si la puerta está abierta o cerrada.



Figura 23. Paso 1 – el elemento de menú **Widgets** tras mantener pulsada la pantalla de inicio.

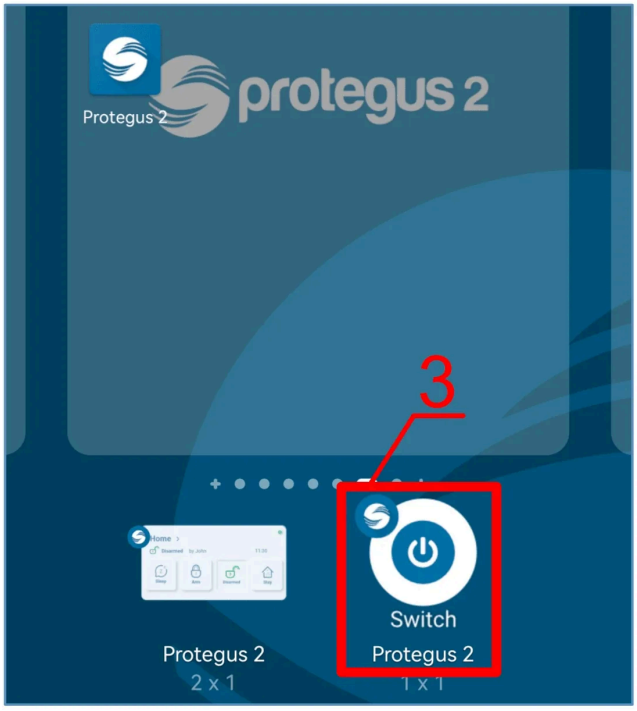


Figura 24. Paso 2 – entre los widgets de Protegus 2, **Switch Protegus 2**.



Figura 25. Paso 3 – selección de la salida **Gator Output5** y el botón **ADD WIDGET**.



Figura 26. Paso 4 – el widget **Output5** en la pantalla de inicio; el botón verde indica la salida activada (puerta abierta).

4.5 Gestión de usuarios en la aplicación

Como administrador, también puedes añadir y eliminar usuarios en Protegus 2; el usuario añadido ve y abre la puerta desde su propia cuenta, y también puede recibir notificaciones por SMS (si el mensaje de bienvenida **HELLO** está activado, recibe un SMS cuando se le añade).

1. Inicia la aplicación Protegus 2 en tu teléfono e inicia sesión con tu nombre de usuario y tu contraseña. En la pantalla del sistema, abre el menú **Settings** (ajustes) y después el apartado **System configuration**.
2. Elige la lista **Users** (usuarios) y pulsa el botón **+** (**Add new user** – nuevo usuario).
3. Introduce la **dirección de correo electrónico**, el **nombre** y el **número de teléfono** del usuario (o el número de la tarjeta RFID, apartado 5.6), con un lector de código su **código** de 4 dígitos, e indica qué salida puede controlar (**Output5**).
4. Pulsa el botón **Add user** (añadir usuario): el nuevo usuario aparece en la lista. Con el botón **Back** vuelves a la ventana principal.

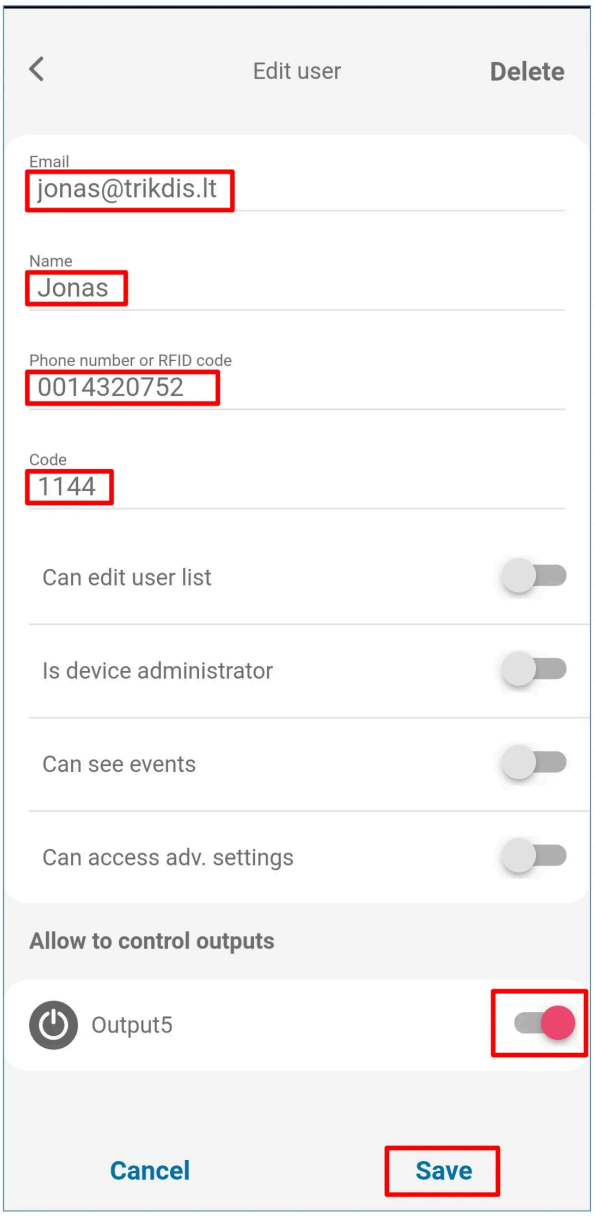


Figura 27. Edición de un usuario en Protegus 2: dirección de correo electrónico, nombre, número de teléfono o número de tarjeta RFID, código y autorización para controlar la **Output5**.

4.6 Control con un mensaje SMS

La salida de relé (**OUTPUT5**) se conmuta con estos comandos SMS; `xxxxxx` es la contraseña de administrador de 6 dígitos (de fábrica `123456`). También puedes conmutar otras salidas por SMS, pero antes hay que configurarlas como salida en TrikdisConfig (apartado 5.3).

Comando	Parámetro	Descripción
`OUTPUTx xxxxxx ON`	ON	encender la salida; **x** es el número de la salida. Ejemplo: `OUTPUT5 123456 ON`
`OUTPUTx xxxxxx OFF`	OFF	apagar la salida. Ejemplo: `OUTPUT5 123456 OFF`
`OUTPUTx xxxxxx PULSE=ttt`	PULSE=ttt	encender la salida durante **ttt** segundos (1–999, con tres cifras). Ejemplo: `OUTPUT5 123456 PULSE=002`

4.7 Programación por SMS

El equipo solo acepta los comandos SMS de los números de **administrador** (1A–7A); cada comando contiene la contraseña de administrador de 6 dígitos. El equipo envía un SMS de respuesta sobre la ejecución si en el administrador está activado **ACK for SMS message** (apartado 5.6).

Cambio de la contraseña de administrador – por seguridad, que sea lo primero que hagas:

```
PSW 123456 xxxxxx
```

`123456` – la contraseña de fábrica; `xxxxxx` – la nueva contraseña de 6 caracteres.

Que solo controlen los autorizados – envía los datos de los usuarios desde el teléfono del administrador:

```
SETU xxxxxx +PHONENO#NAME#EMAIL
```

`PHONENO` – el número de teléfono del usuario en formato internacional (+CC..., donde CC es el prefijo del país); `NAME` – su nombre; `EMAIL` – su dirección de correo electrónico (para Protegus 2). Después de añadir el primer número, el GATOR solo reacciona a las llamadas de los números de la lista.

Derechos de administrador para otra persona – los demás administradores reciben los mensajes del sistema y pueden añadir usuarios:

```
SETA xxxxxx Nox=+PHONENO#NAME#EMAIL
```

`Nox` – el número de orden del administrador en la lista (1–7); si escribes **1**, cedes tu propio derecho de administrador.

Lista de comandos SMS (en todos, la contraseña va después de la palabra de comando; en los ejemplos, la de fábrica `123456`):

Comando	Parámetro	Descripción
`INFO`	–	datos del equipo: tipo, IMEI, intensidad de la señal, tensión de alimentación, versión de firmware, número de serie, fecha y hora. Ejemplo: `INFO 123456`
`ASKI`	–	estado de las entradas. Ejemplo: `ASKI 123456`
`ASKO`	–	estado de las salidas. Ejemplo: `ASKO 123456`
`SETA`	`NoX=número de teléfono#nombre#correo`	añadir un administrador en la posición X (1A–7A); el número debe empezar con + y el prefijo del país, los campos se separan con #. Ejemplo: `SETA 123456 No3=+CC123456789#Juan#juan@example.com`
`SETA`	`NoX=DEL`	eliminar el administrador X. Ejemplo: `SETA 123456 No2=DEL`
`SETU`	`número de teléfono#nombre#correo`	añadir un usuario nuevo (posiciones 11–1010); aquí también el número debe empezar con + y el prefijo del país, los campos se separan con #. Ejemplo: `SETU 123456 +CC123456789#Pedro#pedro@example.com`
`DELU`	`número de teléfono` o `nombre`	eliminar un usuario por número de teléfono o por nombre. Ejemplo: `DELU 123456 +CC123456789`, `DELU 123456 Pedro`
`SETB`	`correo` o `número de teléfono`	añadir a la lista negra (dirección de correo electrónico o número de teléfono). Ejemplo: `SETB 123456 juan@example.com`, `SETB 123456 +CC123456789`
`DELB`	`ALL`	borrar toda la lista negra. Ejemplo: `DELB 123456 ALL`

Comando	Parámetro	Descripción
`DELB`	`correo` o `número de teléfono`	borrar una entrada de la lista negra (en la dirección de correo electrónico importan las mayúsculas y minúsculas). Ejemplo: `DELB 123456 juan@example.com`, `DELB 123456 +CC123456789`
`RESET`	–	reiniciar el equipo. Ejemplo: `RESET 123456`
`PSW`	`nueva contraseña`	cambiar la contraseña de administrador. Ejemplo: `PSW 123456 654123`
`TXTA`	`nombre del objeto`	ajustar el nombre del objeto. Ejemplo: `TXTA 123456 Casa`
`TXTE`	`N1=texto` … `N5=texto`	texto del SMS enviado al activarse la entrada o la salida; N1…N5 es el número del borne. Ejemplo: `TXTE 123456 N1=Puerta abierta`
`TXTR`	`N1=texto` … `N5=texto`	texto del SMS enviado en el restablecimiento. Ejemplo: `TXTR 123456 N5=Rele apagado`
`SETD`	`IDx=yy`	tiempo de inactividad de la entrada x en minutos (0–2880): tras la activación, el equipo avisa y durante ese tiempo no reacciona a los nuevos cambios de la entrada; 0 = desactivado. Ejemplo: `SETD 123456 ID1=30`
`RESD`	`IDx`	anular el tiempo de inactividad ya en curso de la entrada x. Ejemplo: `RESD 123456 ID1`
`TIME`	`AAAA/MM/DD,hh:mm:ss`	ajustar la fecha y la hora. Ejemplo: `TIME 123456 2026/10/30,12:23:00`
`RDR`	`número de teléfono#texto`	reenviar un SMS al número indicado (por ejemplo, una recarga de saldo al operador). Ejemplo: `RDR 123456 +CC123456789#Recarga 10 EUR`
`HELLO`	`ON` / `OFF`	activar / desactivar el aviso por SMS al nuevo usuario sobre su alta (para usuarios añadidos desde la aplicación o por SMS). Ejemplo: `HELLO 123456 ON`
`NATH`	`ON` / `OFF`	activar y desactivar el modo **Not authorized** (puede llamar cualquiera) sin cambiar los demás ajustes; con varias salidas, enumerando las salidas que conmutan con la llamada (activa el modo **Not authorized** y las salidas enumeradas, y desactiva las demás salidas). Ejemplo: `NATH 123456 ON`, `NATH 123456 ON=5,7,22`, `NATH 123456 OFF`
`UUSD`	`*código#`	enviar un código USSD al operador móvil (consulta del saldo, recarga). Ejemplo: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON` / `Protegus=OFF`	conectarse a la nube de Protegus o desconectarse. Ejemplo: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`APN=nombre`, `USER=nombre`, `PSW=contraseña`	nombre APN, nombre de usuario y contraseña de la conexión de datos móviles. Ejemplo: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`Code=contraseña`	cambiar el código de acceso a la nube de Protegus (**Cloud Access Code**). Ejemplo: `CONNECT 123456 Code=123456`

Sustituye el prefijo del país (CC) y la dirección de correo electrónico de los ejemplos por tus propios datos. En el SMS, evita las letras con tilde y los caracteres especiales (á, é, ñ…) si el ajuste **System Options → Text language** no está en el juego de caracteres adecuado (apartado 5.2). La lista de APN: Configuración del APN – lista de operadores móviles europeos.

5. Configuración con el software TrikdisConfig

Toda la configuración del GATOR está disponible en el programa **TrikdisConfig**, que funciona en Windows, por cable USB o a distancia (capítulo 6). Con la configuración de fábrica, el equipo abre con una llamada (capítulo 2); el programa hace falta cuando configuras usuarios, tarjetas RFID, horarios, textos de SMS, módulos, la nube de Protegus o la CRA.

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!

1. Retira la tapa frontal del GATOR con un destornillador plano, como muestra la figura.
2. Conecta el GATOR al ordenador con un cable **USB Mini-B**.
3. Inicia TrikdisConfig. El programa reconoce el equipo y abre la ventana de programación del GATOR.
4. Haz clic en el botón **Read [F4]**: el programa lee la configuración actual del equipo. Si lo pide, introduce el código de 6 dígitos de **administrador** o de **instalador** en la ventana emergente (el código de administrador de fábrica es `123456`).



Figura 28. Cómo retirar la tapa frontal: introduciendo el destornillador en la ranura lateral y moviéndolo hacia abajo, la tapa se suelta; debajo está el conector USB Mini-B.

Advertencia

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

El botón **Restore**, en la parte inferior izquierda de la ventana de programación, devuelve la configuración de fábrica (apartado 5.9).

5.1 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 29. La barra de estado del GATOR: en el campo de la izquierda el **IMEI/Unique ID**, abajo **Status: reading done**, **Device: GV17_2200** (el código de tipo), el número de serie, las versiones **BL** y **FW** y el modo de conexión (USB). En el GATOR, el campo **Device** debe tener la forma **GV17_xxxx**.

5.2 Página «System Options»

Ajustes generales del equipo: identificador, hora, código de administrador, contestación de llamadas, prueba, tarjeta SIM y zona horaria.

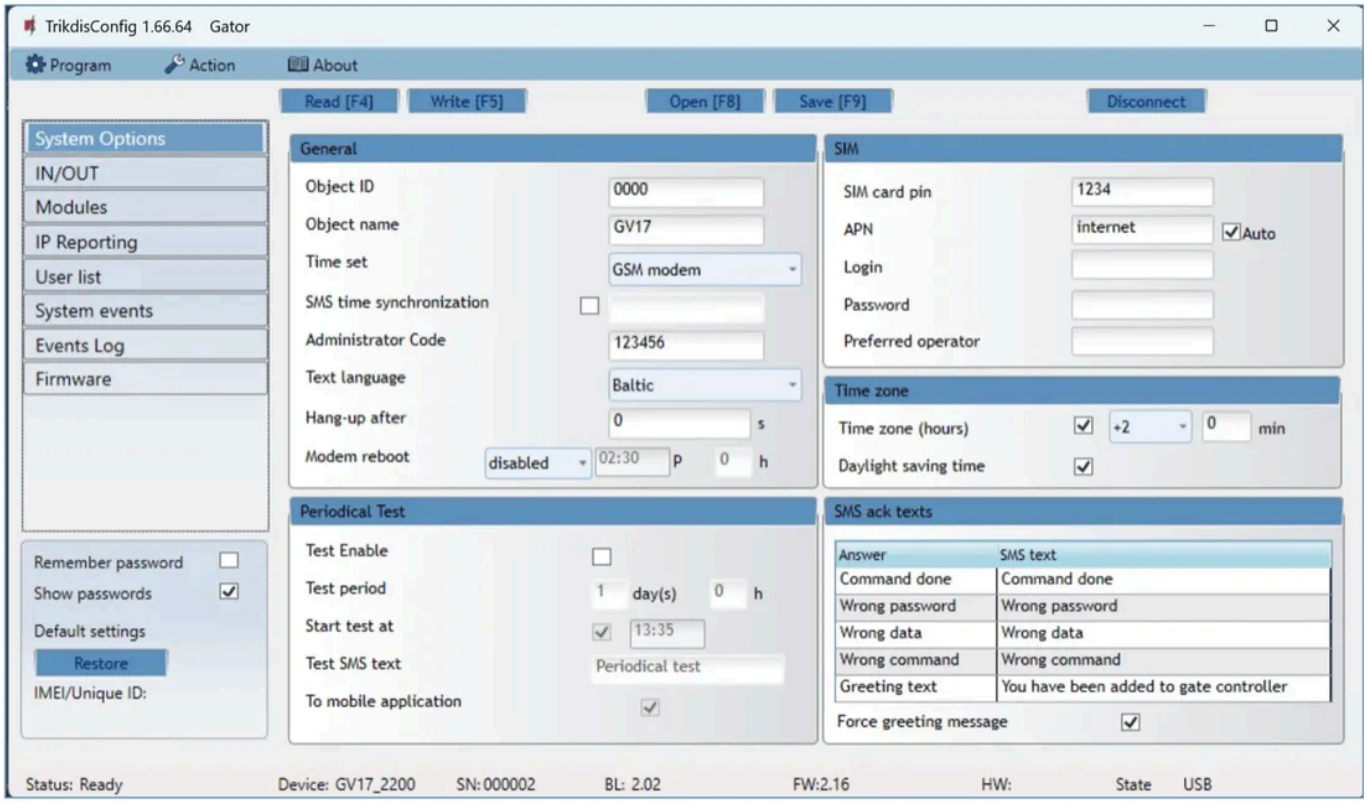


Figura 30. TrikdisConfig – **System Options**: los grupos **General**, **Periodical test**, **SIM**, **Time zone** y **SMS ack texts**.

Grupo General

- **Object ID** – el número de abonado recibido de la CRA (número hexadecimal de 4 dígitos, 0–9, A–F). No uses los valores FFFE y FFFF.
- **Object name** – el equipo envía todos los eventos con este nombre.
- **Time set** – la fuente de sincronización de la hora (por ejemplo, la red móvil).
- **SMS time synchronization** – márcalo e introduce el número de la tarjeta SIM del GATOR en formato internacional (+CC…), si la hora se sincroniza por SMS.
- **Administrator Code** – el código de administrador: con él se pueden modificar todos los parámetros del GATOR (de fábrica `123456`; cámbialo).
- **Text language** – el juego de caracteres de los mensajes SMS.
- **Hang-up after** – con 0, el equipo rechaza la llamada (abre con la llamada); con otro valor, la contesta y cuelga pasados los segundos indicados; para el control con el teclado (DTMF) (apartado 4.2).
- **Modem reboot** – reinicio diario del módem a una hora determinada.

Grupo Periodical test

- **Test Enable** – marcado, el equipo envía un informe de prueba periódico.
- **Test period** – el tiempo entre los informes de prueba.
- **Start test at** – la hora de la primera prueba.
- **Test SMS text** – el texto del SMS de prueba.
- **To mobile application** – marcado, el informe de prueba también se envía a la aplicación Protegus 2.

Grupo SIM

- **SIM card PIN** – el código PIN de la tarjeta SIM, si no has desactivado la petición.

- **APN** – el punto de acceso de la conexión de datos móviles. Con la casilla **Auto**, el equipo elige un APN de la lista incorporada (datos de varios operadores internacionales y nacionales) y solo usa el valor escrito en el campo si no encuentra el operador. Si no se establece la conexión de datos, escribe el APN del operador: Configuración del APN – lista de operadores móviles europeos.
- **Login**, **Password** – el nombre de usuario y la contraseña del APN, si el operador los pide.
- **Preferred operator** – si indicas un código de operador (MCC + MNC), el GATOR solo se conecta a esa red; es importante con las tarjetas SIM internacionales (roaming).

Grupo Time zone – aquí se ajusta la hora exacta del país: indica la zona horaria y marca si en el país hay horario de verano.

- **Time zone (hours)** – márcalo e indica la zona horaria del país (por ejemplo, hora de Europa Central: +1).
- **Daylight saving time** – márcalo si en el país hay horario de verano.

Grupo SMS ack texts – el texto de los SMS de respuesta que recibe el usuario después de los comandos SMS.

- **Force greeting message** – marcado, el equipo envía un SMS de bienvenida al nuevo usuario añadido por SMS o desde Protegus 2 (por SMS: `HELLO 123456 OFF` lo desactiva).

5.3 Página «IN/OUT»

Los ajustes de las entradas y salidas, de los lectores RFID y del registro de jornada, en tres pestañas: **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 Pestaña IN/OUT – entradas y salidas

En la tabla hay un borne por fila; aquí decides cuál es entrada y cuál salida, y cómo deben avisar.

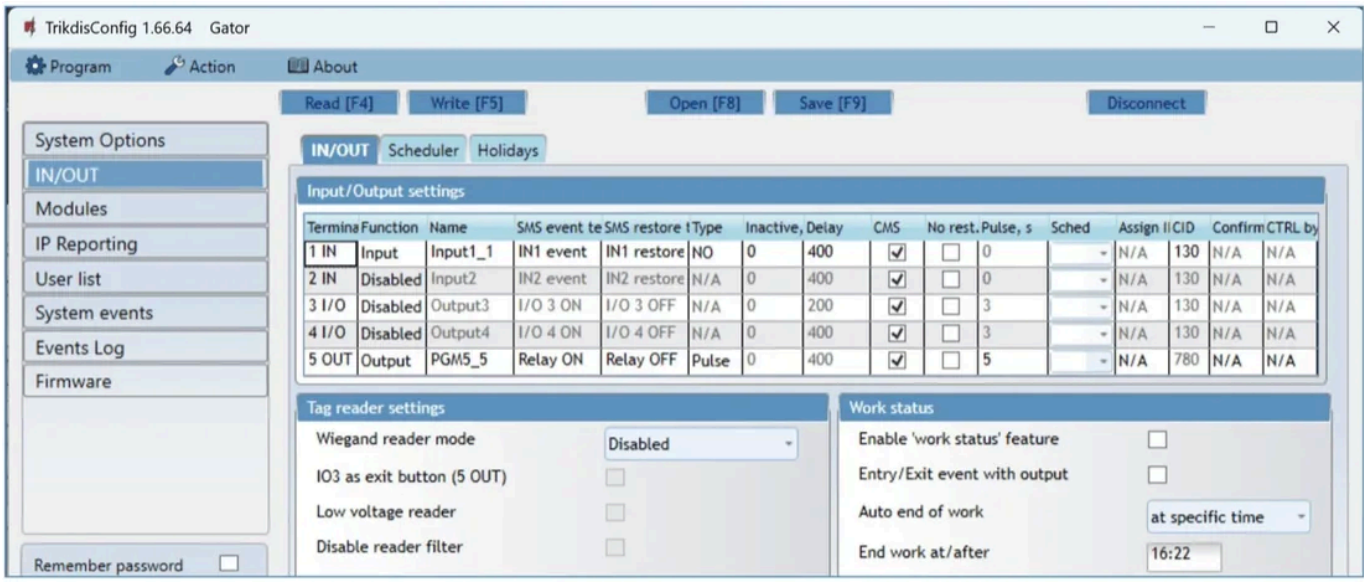


Figura 31. TrikdisConfig – **IN/OUT**: la tabla **Input/Output settings** (de fábrica la 1 IN como entrada, la 2 IN, la 3 I/O y la 4 I/O desactivadas, la 5 OUT como salida de tipo **Pulse**); debajo, los grupos **Tag reader settings** y **Work status**.

Grupo Input/Output settings

- **Terminal** – el número de los bornes del GATOR (1 IN … 5 OUT; los bornes de los expansores al final de la lista).

- **Function** – la función del borne: **Input** (entrada), **Output** (salida) o **Disabled** (desactivado).
- **Name** – el nombre de la entrada o salida (así aparece en la aplicación y en los SMS).
- **SMS event text** – el texto del SMS enviado en la activación.
- **SMS restore text** – el texto del SMS enviado en el restablecimiento.
- **Type** – en la entrada, el tipo de circuito (**NC**, **NO**, **EOL = 10 kΩ**); en la salida, el funcionamiento: **Pulse** (impulso) o **Level** (biestable).
- **Inactive** – tras la primera activación, la entrada no vuelve a avisar durante este tiempo; 0 = desactivado.
- **Delay** – el tiempo de reacción de la entrada en milisegundos (de fábrica 400 ms).
- **CMS** – marcado, el evento se envía a la CRA y también a Protegus 2.
- **No rest.** – no enviar el evento de restablecimiento.
- **Pulse** – la duración del impulso en segundos, si la salida es de tipo **Pulse** (de fábrica 3 s en la 5 OUT; para el automatismo de la puerta suelen bastar 1–3 s).
- **Sched** – el número del horario que controla la salida (de la pestaña **Scheduler**).
- **Assign IN** – la entrada asignada a la salida: en lugar del estado de la salida, la aplicación muestra el estado real de la entrada (de la puerta) (apartado 5.10).
- **CID** – el código Contact ID del evento.
- **Confirm** – el número de la entrada cuyo estado activo es condición para conmutar la salida.
- **CTRL by IN** – la activación de la entrada seleccionada conmuta la salida (automatismo local, funciona también sin red).

Grupo Tag reader settings – los ajustes de los lectores RFID (conexionado en el apartado 3.6)

- **Wiegand reader mode** – el número de lectores Wiegand conectados: **Single Reader** o **Dual Reader**.
- **IO3 as exit button (5 OUT)** – márcalo si el pulsador de salida está conectado al borne 3 I/O: al pulsarlo, la 5 OUT se activa durante el tiempo de impulso configurado.
- **Low voltage reader** – para un lector de baja tensión (nivel de señal de 5 V).
- **Disable reader filter** – desactiva el filtro interno de impulsos cortos, si el equipo no reconoce las señales del lector.

Grupo Work status – registro de jornada en Protegus 2 (detalles: GV17 – sistema de control de acceso y/o registro de jornada)

- **Enable "work status" feature** – activa la indicación del estado de trabajo en la aplicación.
- **Entry/Exit event with output** – marcado, también se genera un evento de entrada / salida al conmutar la salida a distancia.
- **Auto end of work** – el modo de cierre automático de la jornada.
- **End work at/after** – la hora del cierre o el tiempo que transcurre hasta el cierre, según el ajuste anterior.

5.3.2 Pestaña Scheduler – horarios de las salidas

Las salidas también pueden conmutar por sí solas según un horario (por ejemplo, la puerta abierta en horario laboral y cerrada por la noche). El horario se asigna en la columna **Sched** de la salida.

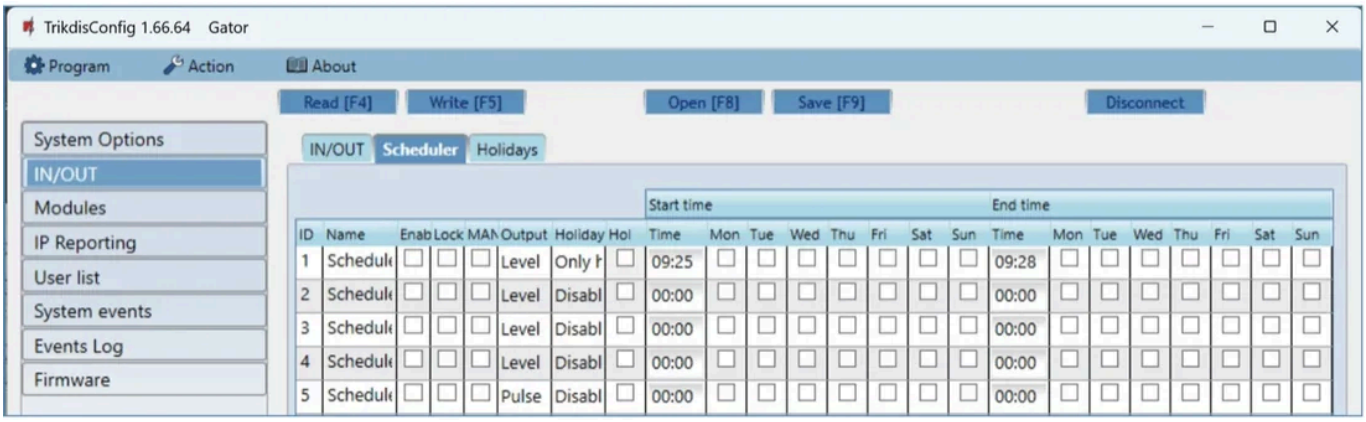


Figura 32. TrikdisConfig – IN/OUT, pestaña **Scheduler**: para cada horario, activación, bloqueo, modo de salida, modo de festivos, hora de inicio y de fin con los días de la semana.

- **Name** – el nombre del horario.
- **Enable** – activación del horario.
- **Lock** – marcado, mientras el horario está activo la salida no se puede conmutar de otra manera (por llamada, desde la aplicación).
- **MANUAL** – marcado, al empezar el horario la salida no conmuta sola; el horario empieza cuando el usuario activa la salida.
- **Output mode** – el funcionamiento de la salida durante el horario: **Level** – la salida está activada durante todo el periodo indicado; **Pulse** – la salida se activa al principio y al final del horario durante el tiempo de impulso configurado.
- **Holiday mode** – cómo funciona el horario en los días festivos; **Hol** – márcalo si en los festivos se usan las horas de festivo.
- **Start time** – los días de la semana y la hora a partir de la cual se activa la salida.
- **End time** – los días de la semana y la hora hasta la cual la salida permanece activada.

Si el modo de la salida es **Level** y solo se indica la **End time**, la salida se desactiva a la hora indicada si hasta entonces estaba activada.

5.3.3 Pestaña Holidays – días festivos

Aquí indicas los días del calendario en los que el horario funciona con las horas de festivo.

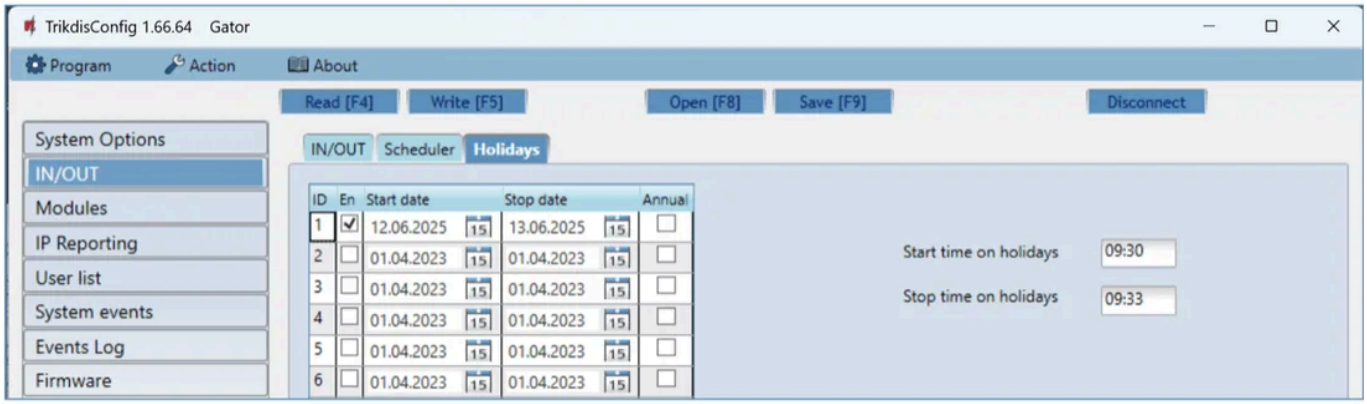


Figura 33. TrikdisConfig – IN/OUT, pestaña **Holidays**: periodos festivos con fecha de inicio y de fin, y la hora de inicio y de fin en los festivos.

- **En.** – activación del periodo festivo.
- **Start date**, **Stop date** – el primer y el último día del periodo.
- **Annual** – festivo que se repite cada año: el equipo solo tiene en cuenta el mes y el día.

- **Start time on holidays**, **Stop time on holidays** – la hora de inicio y de fin en los festivos.

5.4 Página «Modules»

5.4.1 Pestaña Modules

Al GATOR se pueden conectar, por el bus RS485 o por radio, estos módulos: módulo WiFi **W485**, módulo Ethernet **E485**, expansor inalámbrico **iO-LORA** (a través del transceptor RF-LORA, hasta 8; los lectores RFID conectados a los expansores iO-LORA pueden conmutar así hasta 8 salidas adicionales, un lector siempre solo una salida de su propio expansor – desde el firmware 2.13 del GATOR, apartado 3.9), expansor por cable **iO8** e inalámbrico **iO8-LORA** (a través del RF-LORA; de los dos, uno en total). El transceptor RF-LORA no hace falta añadirlo a la lista. Si en el lugar hay WiFi o internet por cable, con el módulo W485 o E485 el GATOR envía los mensajes por internet a la nube de Protegus y a la CRA: no se consumen datos móviles (el tráfico de datos de la tarjeta SIM incluso se puede bloquear), e incluso el GATOR se puede usar sin tarjeta SIM, controlándolo solo desde la aplicación.

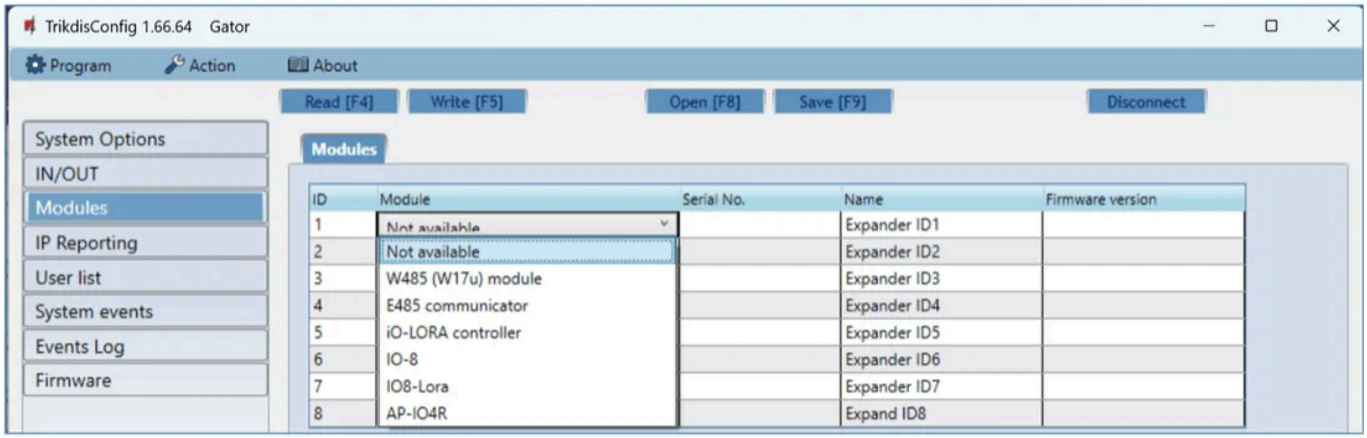


Figura 34. TrikdisConfig – **Modules**: en la lista desplegable **Module**, los módulos W485, E485, iO-LORA, iO8, iO8-LORA y **AP-IO4R** (iO4R); al lado, las columnas **Serial No.**, **Name** y **Firmware version**.

- **Module** – elige en la lista el módulo conectado.
- **Serial No.** – el número de serie de 6 dígitos del módulo (en la etiqueta de la carcasa y de la caja del módulo).

Después de seleccionar el módulo y escribir el número de serie aparece la pestaña **Parameters** con los ajustes propios del módulo.

Expansor de relés iO4R

El **AP-IO4R** de la lista es el expansor de relés **iO4R**: sirve para supervisar y puentear a distancia los sensores de seguridad del automatismo de la puerta, y para contar los ciclos de la puerta. Se configura en la aplicación Protegus 2, en el modo **Advanced Gator Monitoring**, que se puede elegir al añadir el controlador de puertas; consulta el manual del iO4R.

5.4.2 Pestaña Parameters – módulo WiFi W485

Después de seleccionar el W485, aquí introduces los datos de la red WiFi y el modo de uso de la tarjeta SIM.

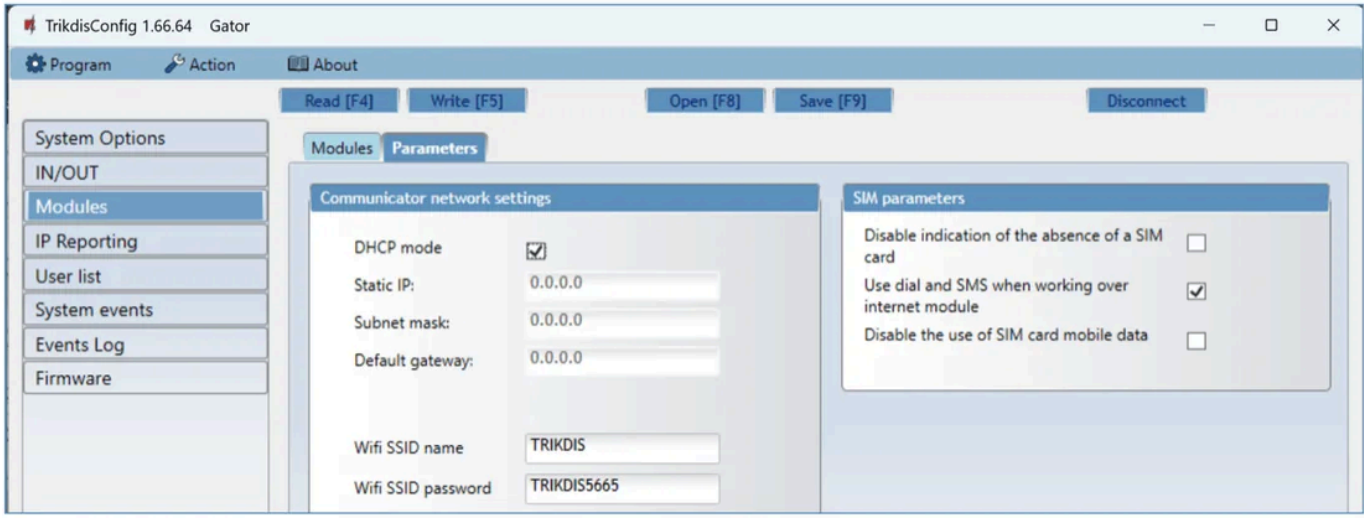


Figura 35. TrikdisConfig – Modules, pestaña **Parameters** del W485: **Communicator network settings** (DHCP, dirección IP, nombre y contraseña de la red WiFi) y **SIM parameters**.

Grupo Communicator network settings

- **DHCP mode** – marcado, el módulo recibe automáticamente del router los ajustes de red (dirección IP, máscara de subred, puerta de enlace); sin marcar, los introduces a mano.
- **Static IP**, **Subnet mask**, **Default gateway** – la dirección IP fija, la máscara de subred y la dirección de la puerta de enlace en la configuración manual.
- **Wifi SSID name** – el nombre de la red WiFi a la que se conecta el W485 (red de 2,4 GHz).
- **Wifi SSID password** – la contraseña de la red WiFi.

Grupo SIM parameters

- **Disable indication of the absence of a SIM card** – marcado, el equipo no indica como fallo la falta de tarjeta SIM (para el uso sin SIM, solo por internet).
- **Use dial and SMS when working over internet module** – marcado, el control por llamada y por SMS también funciona junto con el módulo. Sin marcar, mientras la conexión a internet funcione, el equipo no usa llamadas ni SMS; si se interrumpe internet, la llamada y el SMS vuelven a funcionar y el equipo envía un SMS a los usuarios.
- **Disable the use of SIM card mobile data** – marcado, el equipo no usa los datos móviles de la tarjeta SIM y los datos solo van por el W485. Si se interrumpe la WiFi, el equipo guarda los eventos y los envía cuando vuelve la conexión.

5.4.3 Pestaña Parameters – módulo Ethernet E485

Después de seleccionar el E485, aquí introduces los datos de la red por cable y el modo de uso de la tarjeta SIM.

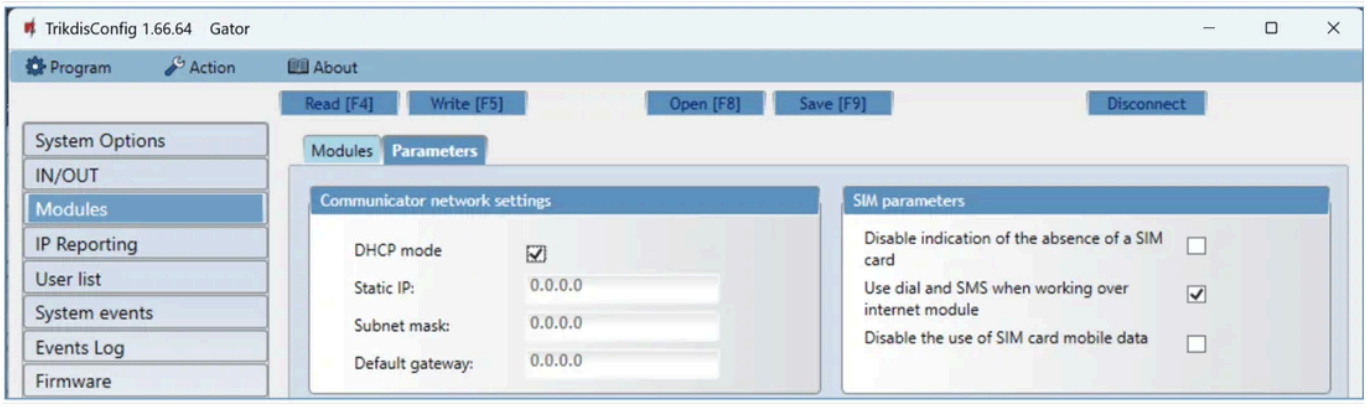


Figura 36. TrikdisConfig – Modules, pestaña **Parameters** del E485: ajustes de red (DHCP o dirección IP fija) y **SIM parameters**.

- **DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway** – lo mismo que en el W485: configuración de red automática o manual.
- **SIM parameters** – las tres casillas significan lo mismo que lo descrito para el W485; con los datos móviles bloqueados, los datos solo van por el E485, y mientras falla internet el equipo guarda los eventos.

5.5 Página «IP Reporting»

El GATOR envía los eventos al receptor IP de la CRA y a la nube de Protegus; la nube se activa en esta página.

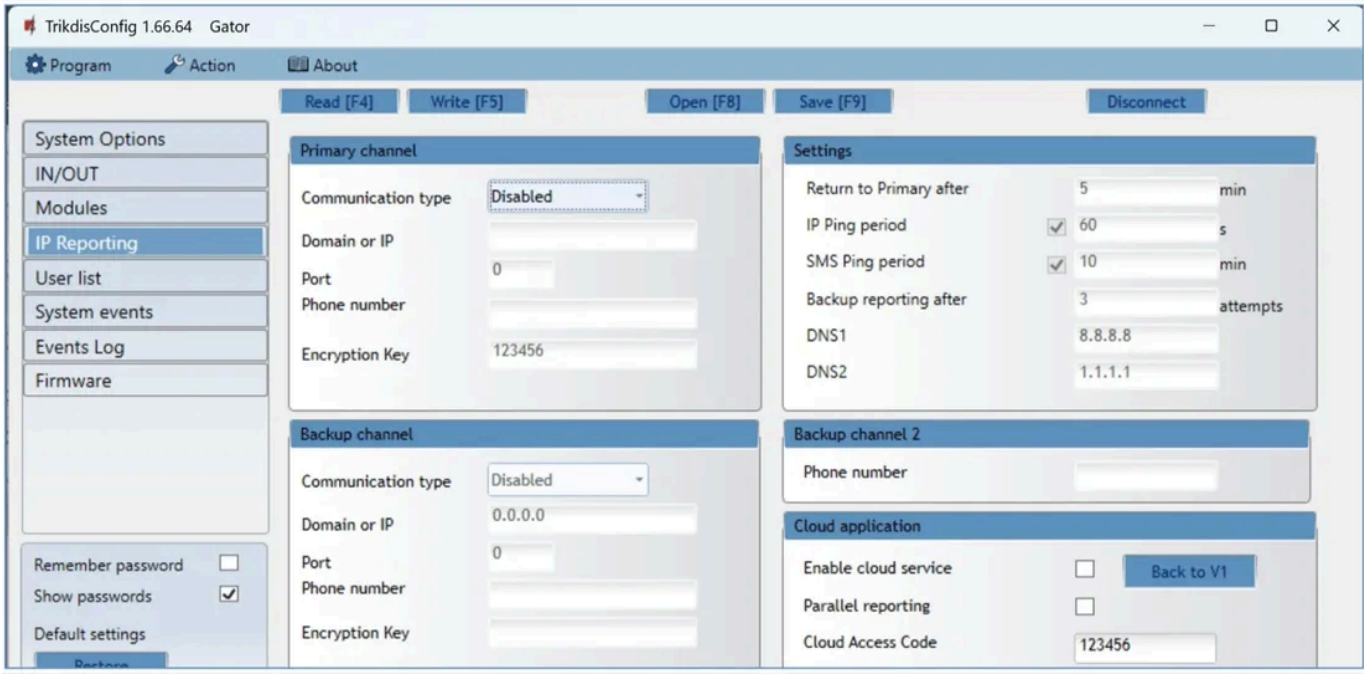


Figura 37. TrikdisConfig – **IP Reporting**: **Primary channel** y **Backup channel** (de fábrica desactivados), **Settings**, el canal SMS de reserva y el grupo **Cloud application** con la casilla **Enable cloud service** y el **Cloud Access Code**.

Grupo Primary channel

- **Communication type** – el tipo de conexión con el receptor de la CRA: **IP** o **SMS**; **Disabled** = sin transmisión.
- **Domain or IP** – el nombre de dominio o la dirección IP del receptor.
- **Port** – el puerto de red del receptor.
- **Phone number** – el número de teléfono del receptor SMS de la CRA (+CC…), si el tipo es SMS.
- **Encryption Key** – clave de cifrado de 6 dígitos, que debe coincidir con la configurada en el receptor.

Grupo Backup channel – el receptor de reserva, con los mismos ajustes que el principal.

Grupo Settings

- **Return to primary after** – pasado este tiempo, el equipo intenta volver del canal de reserva al principal.
- **IP Ping period** – activación e intervalo de las señales PING que mantienen la conexión.
- **SMS Ping period** – lo mismo en el canal SMS.
- **Backup reporting after** – tras este número de intentos fallidos, el equipo pasa al canal de reserva.
- **DNS1**, **DNS2** – la dirección IP de los servidores de nombres.

Grupo Backup channel 2

- **Phone number** – el número del receptor SMS de la CRA. El equipo envía aquí un SMS si no consigue enviar el mensaje ni por el canal IP principal ni por el de reserva; también funciona si en la red del operador móvil falla la conexión IP. Solo está activo si los dos canales IP son de red móvil; el receptor SMS recibe un mensaje en el primer encendido del equipo y cuando se pierde la conexión TCP/IP o UDP/IP.

Grupo Cloud application

- **Enable cloud service** – activación de la nube de Protegus: el GATOR se comunica con la aplicación y también se puede programar a distancia con TrikdisConfig (capítulo 6).
- **Parallel reporting** – marcado, los eventos van a la vez a la CRA, a Protegus 2 y a los usuarios; sin marcar, la aplicación y los usuarios solo los reciben después de la confirmación de la CRA.
- **Cloud Access Code** – código de 6 dígitos para conectarse a Protegus 2 (de fábrica `123456`); la aplicación lo pide al añadir el sistema si no es el de fábrica.

5.6 Página «User list»

La lista de administradores y usuarios, el registro de tarjetas RFID, los horarios de usuario y la lista negra, en cuatro pestañas.

5.6.1 Pestaña Users – los usuarios

En la tabla hay un administrador o un usuario por fila, con sus permisos.

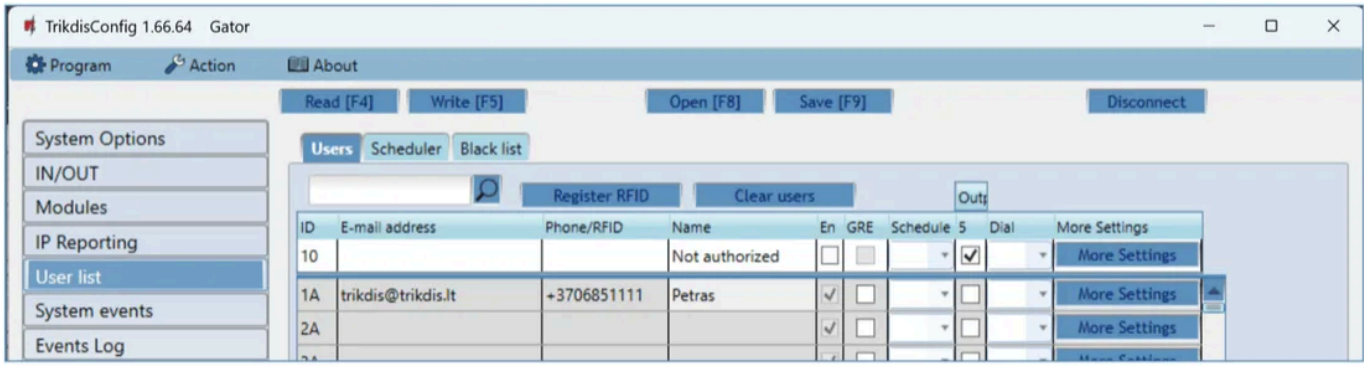


Figura 38. TrikdisConfig – **User list**, pestaña **Users**: arriba los botones **Register RFID** y **Clear users**; en la tabla, las columnas **ID**, **E-mail address**, **Phone/RFID**, **Name**, **En**, **GRE**, **Schedule**, **Dial** y el botón **More settings**; la fila 10 es la entrada **Not authorized**.

- **ID** – el número de orden del usuario. Las filas con la letra **A** (**1A–7A**) son los administradores: pueden configurar el equipo, conmutar las salidas y reciben los mensajes. Las filas con número **11–1010** son los usuarios: solo pueden conmutar las salidas.
- **E-mail address** – la dirección de correo electrónico del usuario (para Protegus 2).
- **Phone/RFID** – el número de teléfono en formato internacional (+CC…) o el número de identificación de la tarjeta RFID.
- **Name** – el nombre del usuario.
- **En** – habilitación del usuario: marcado, el usuario puede conmutar las salidas.
- **GRE** – envío de un SMS de bienvenida al usuario.
- **Schedule** – el número del horario según el cual el usuario puede controlar (apartado 5.6.3).
- **Output** – la salida o las salidas que puede controlar el usuario.
- **Code** – con un lector Wiegand con código (teclado), el código del usuario.
- **Dial** – la salida o las salidas que conmutan con la llamada, si el usuario tiene varias salidas; después de conmutar, el equipo cuelga.
- **More settings** – la ventana de más ajustes (abajo).

La fila 10, «Not authorized»

Si en el usuario número 10, llamado **Not authorized**, la casilla **En está marcada**, el GATOR se puede controlar con una llamada **desde cualquier número de teléfono**. Si no está marcada, solo pueden llamar los que están en la lista; cada usuario conmuta la salida marcada en su propia columna **Dial**. Lo mismo se ajusta por SMS con el comando `NATH` (apartado 4.7).

Tras el apagado de la red 2G, es posible que algunos operadores móviles no permitan las llamadas de voz por la red 4G (VoLTE) al módem Quectel EG915U-EU que utilizamos. En ese caso, la apertura de la puerta mediante llamada y la notificación por llamada telefónica no funcionan. El envío de SMS y la conexión de datos (aplicación Protegus 2) no se ven afectados por esta limitación y siguen funcionando.

Más ajustes – administrador (1A–7A)

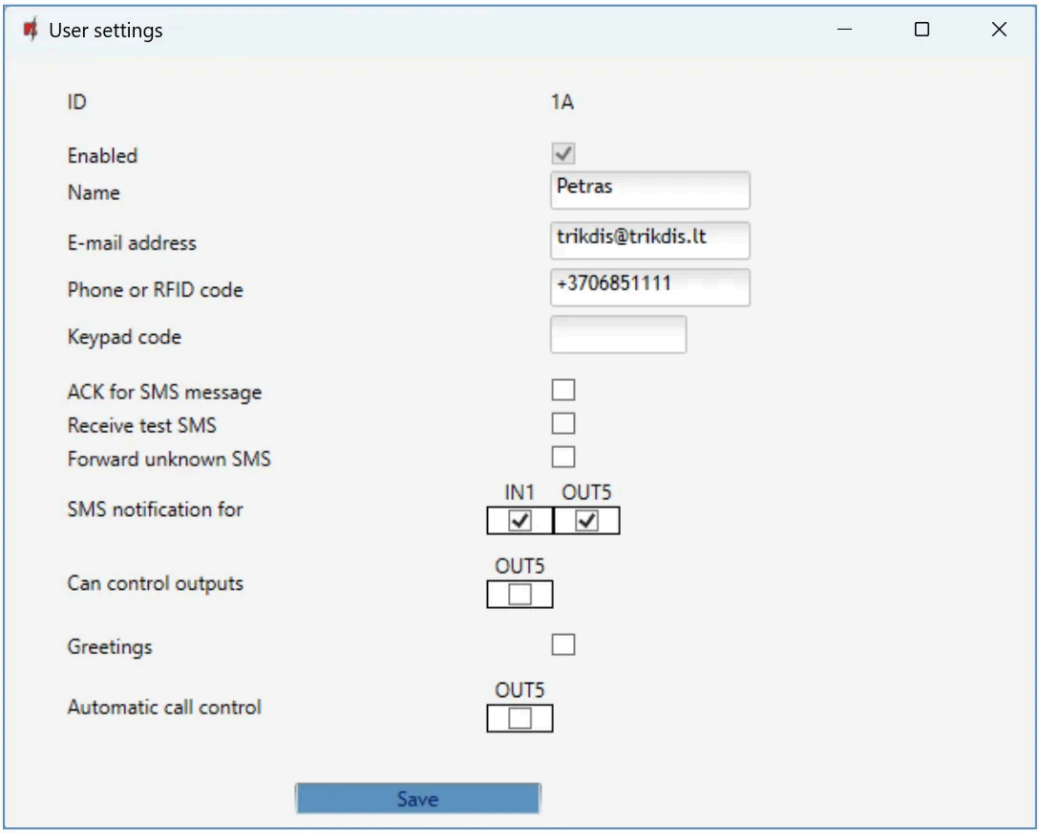


Figura 39. TrikdisConfig – **User settings** de un administrador: **Enabled**, los datos, **ACK for SMS message**, **Receive test SMS**, **Forward unknown SMS**, **SMS notification for** (IN1, IN2, OUT3, OUT4, OUT5), **Can control output**, **Greetings** y **Automatic call control**.

- **ID**, **Enabled**, **Name**, **E-mail address**, **Phone or RFID code**, **Keypad code** – los datos correspondientes a las columnas de la lista.
- **ACK for SMS message** – el administrador recibe un SMS de respuesta sobre la ejecución de los comandos SMS.
- **Receive test SMS** – recibe el SMS de prueba periódico.
- **Forward unknown SMS** – el equipo le reenvía los SMS que llegan de un número desconocido (por ejemplo, el aviso de saldo del operador).
- **SMS notification for** – de los cambios de qué eventos (IN1, IN2, OUT3, OUT4, OUT5) recibe un SMS.
- **Can control output** – las salidas que puede controlar.
- **Greetings** – envío de un SMS de bienvenida.
- **Automatic call control** – las salidas que conmutan con su llamada; después, el equipo cuelga.

Más ajustes – usuario (11–1010)

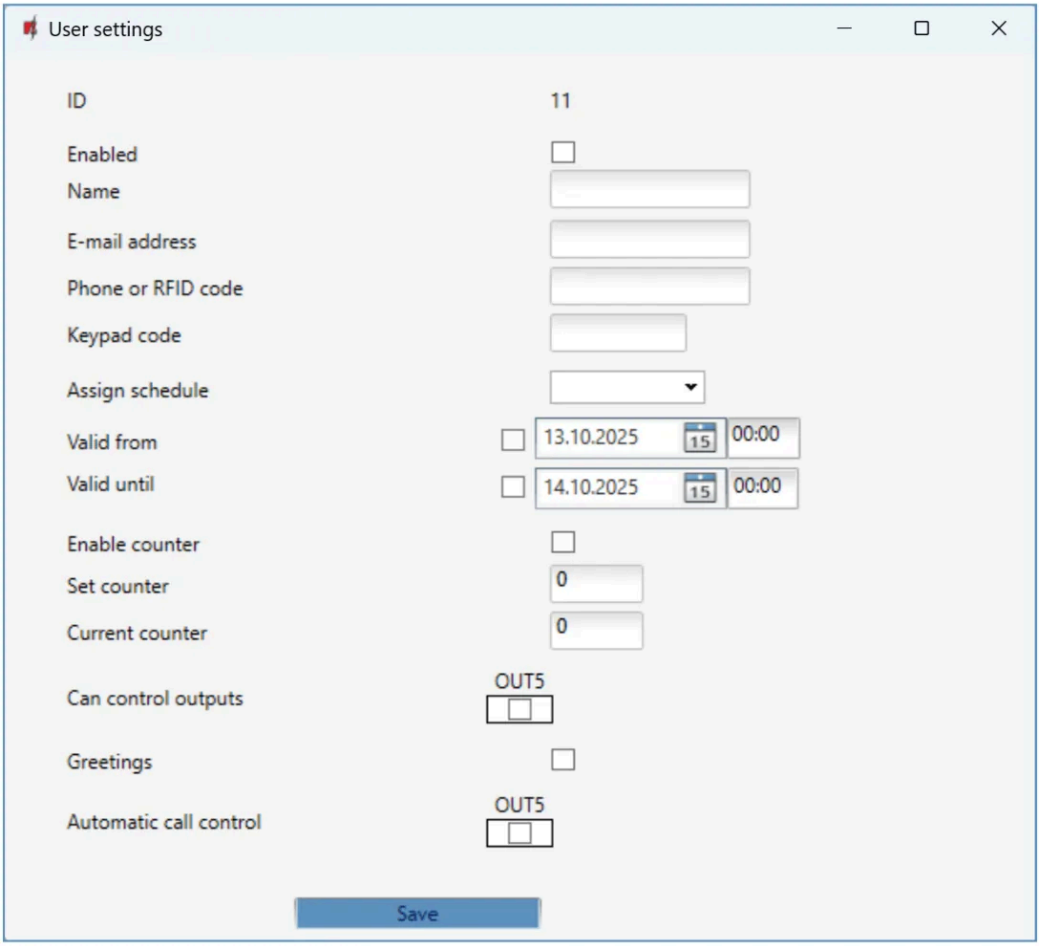


Figura 40. TrikdisConfig – **User settings** de un usuario: **Assign schedule**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs**, **Greetings**, **Automatic call control**.

- **Assign schedule** – el horario o los horarios durante los cuales el usuario puede controlar.
- **Valid from**, **Valid until** – el inicio y el fin del permiso (fecha y hora); por ejemplo, para un inquilino o un invitado.
- **Enable counter** – activación del contador; **Set counter** – cuántas veces puede controlar el usuario dentro del tiempo indicado; **Current counter** – el número de conmutaciones hasta ahora.
- **Can control outputs**, **Greetings**, **Automatic call control** – como en el administrador.

5.6.2 Registro de una tarjeta RFID (llavero)

1. Conecta el lector RFID (apartado 3.6), conecta la alimentación del GATOR, inicia TrikdisConfig y conéctate por cable USB o a distancia. En la página **IN/OUT**, ajusta el número de lectores (**Wiegand reader mode**).
2. En la página **User list**, haz clic en el botón **Register RFID**.

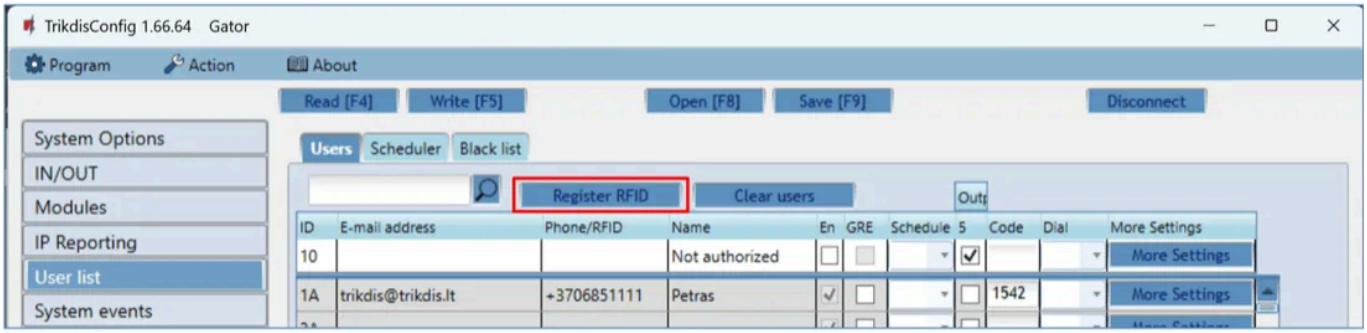


Figura 41. TrikdisConfig – User list: el botón **Register RFID** encima de la tabla de usuarios.

3. Se abre la ventana de registro (**Add RFID tag/card to reader**).

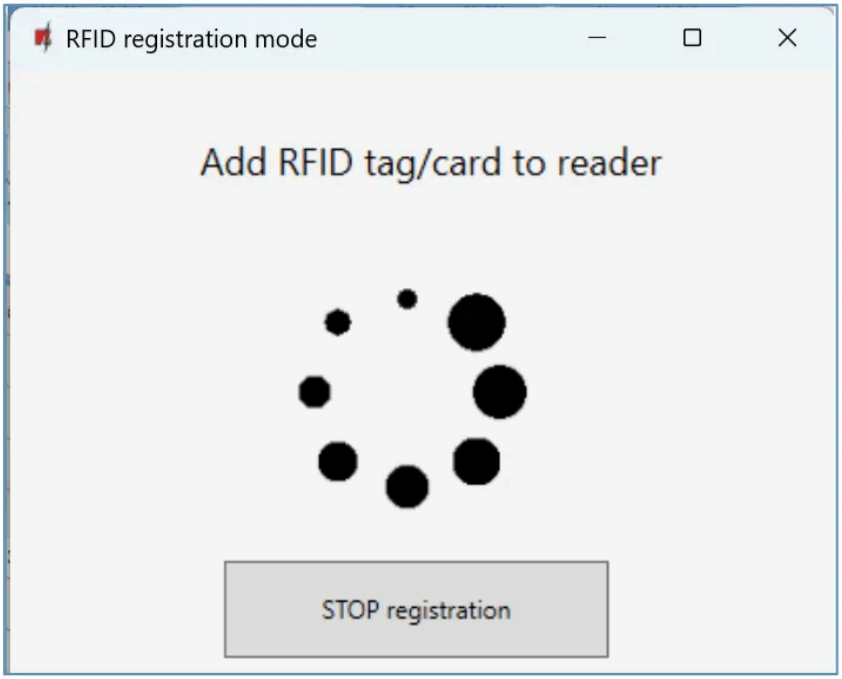


Figura 42. La ventana de registro RFID: hay que acercar la tarjeta al lector; el botón **STOP registration** termina el registro.

4. Acerca la tarjeta al lector. Cuando el lector la ha leído, se abre una ventana nueva: escribe el nombre del usuario (**Enter user name**), marca la salida que puede controlar (**User can control PGM Output 5**; con la casilla **Device administrator** pasa a ser administrador) y haz clic en el botón **ADD**. Repite con las demás tarjetas y después pulsa el botón **STOP registration**.
5. Con el botón **Write [F5]**, escribe la lista de tarjetas en el equipo.

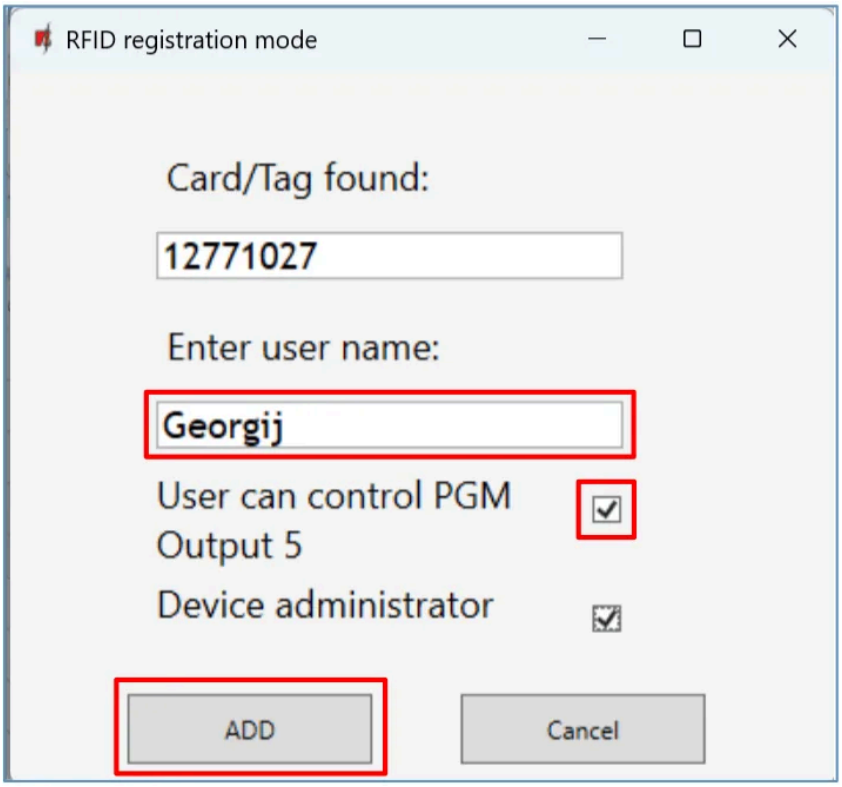


Figura 43. La ventana de la tarjeta leída: nombre, **User can control PGM Output 5**, **Device administrator** y después **ADD**.

Alta de una tarjeta por su número: el número de identificación impreso en la tarjeta también se puede escribir directamente en el campo **Phone/RFID**; introduce el nombre, marca la casilla **En** y la salida que puede controlar y, después, **Write [F5]**.

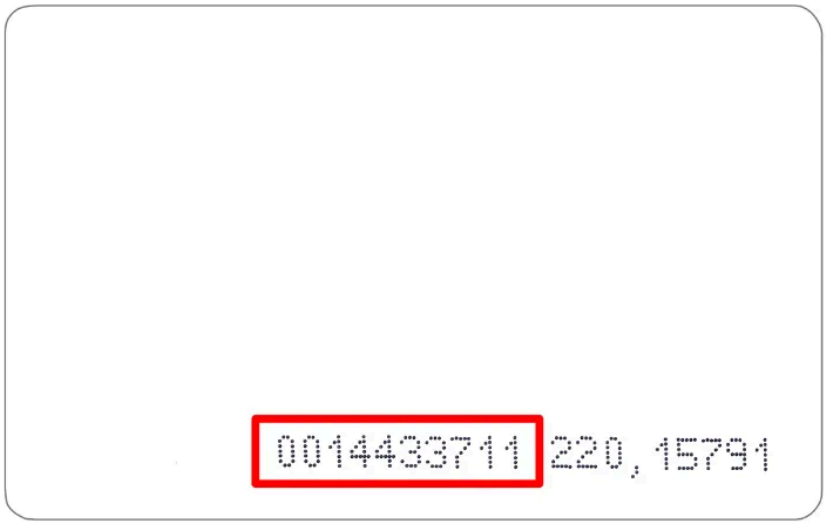


Figura 44. El número de identificación impreso en la tarjeta RFID (en el borde inferior de la tarjeta).

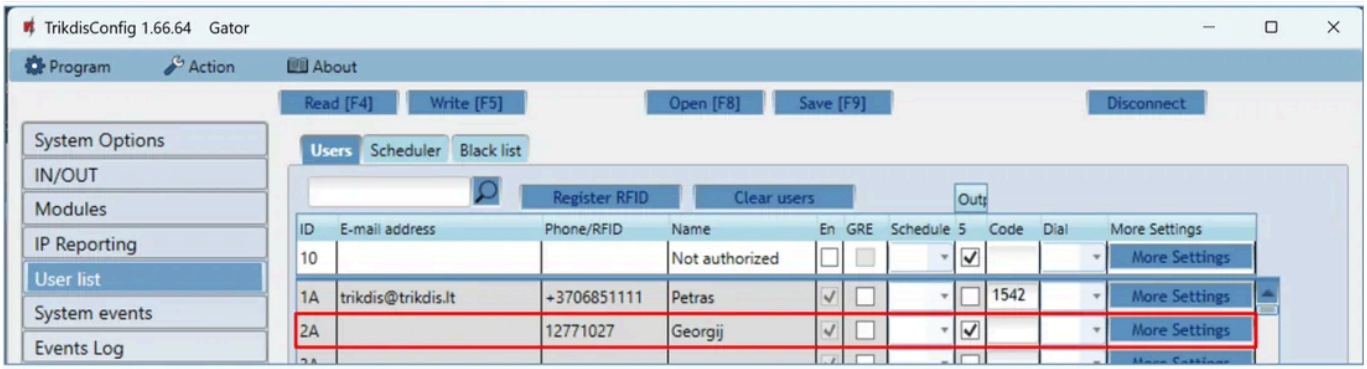


Figura 45. TrikdisConfig – User list: la fila del nuevo usuario con el número de la tarjeta en el campo **Phone/RFID**, el nombre, **En** marcado y la salida 5 seleccionada.

Alta de una tarjeta desde Protegus 2: en la lista de usuarios, elige añadir un usuario nuevo, introduce la dirección de correo electrónico, el nombre, el número de identificación de la tarjeta (en el campo del número de teléfono) y, con un lector de código, el código de 4 dígitos; marca la salida y guarda (apartado 4.5).

5.6.3 Pestaña Scheduler – horarios de los usuarios

El usuario solo puede controlar durante el horario asignado (por ejemplo, el personal de limpieza los días laborables entre las 6 y las 8). El horario se asigna en la columna **Schedule** del usuario o en el campo **More settings → Assign schedule**.

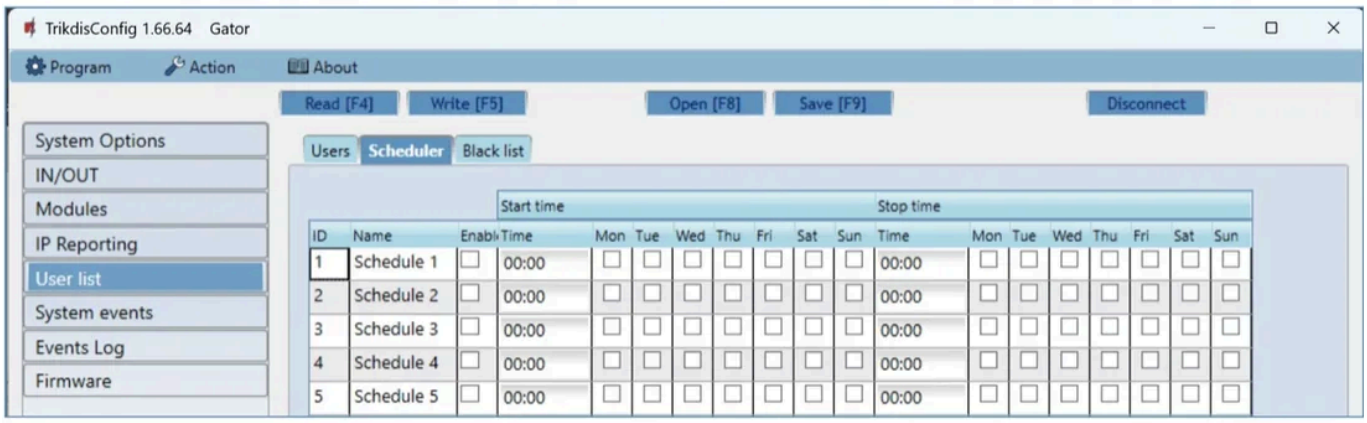


Figura 46. TrikdisConfig – User list, pestaña **Scheduler**: cinco horarios, cada uno con **Enable**, hora de inicio y de fin con los días de la semana.

- **Name** – el nombre del horario.
- **Enable** – activación del horario.
- **Start time** – los días de la semana y la hora a partir de la cual puede controlar el usuario.
- **Stop time** – los días de la semana y la hora hasta la cual puede controlar.

5.6.4 Pestaña Black list – lista negra

Quien esté aquí no puede controlar el equipo de ninguna manera.

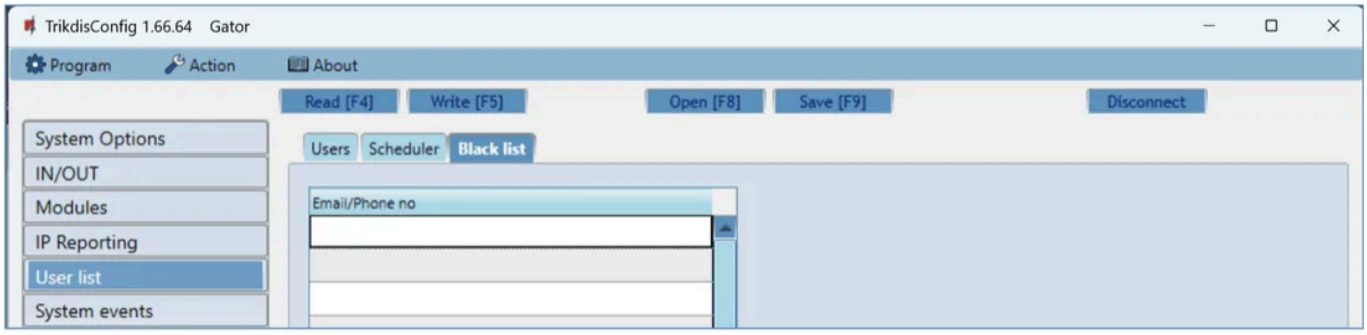


Figura 47. TrikdisConfig – User list, pestaña **Black list**: la tabla de direcciones de correo electrónico, números de teléfono y números de tarjeta bloqueados.

En la lista negra están las direcciones de correo electrónico, los números de teléfono y los números de tarjeta RFID a los que está prohibido controlar el GATOR. También se pueden añadir entradas directamente desde el registro de eventos: haz clic con el botón derecho en el número de teléfono, la dirección de correo electrónico o el número de tarjeta y elige la opción de menú **Add to black list**. Por SMS, la lista se gestiona con los comandos `SETB` y `DELB` (apartado 4.7).

5.7 Página «System events»

Aquí ajustas cuáles de los eventos propios del sistema del GATOR se envían a la CRA y a la aplicación Protegus 2.

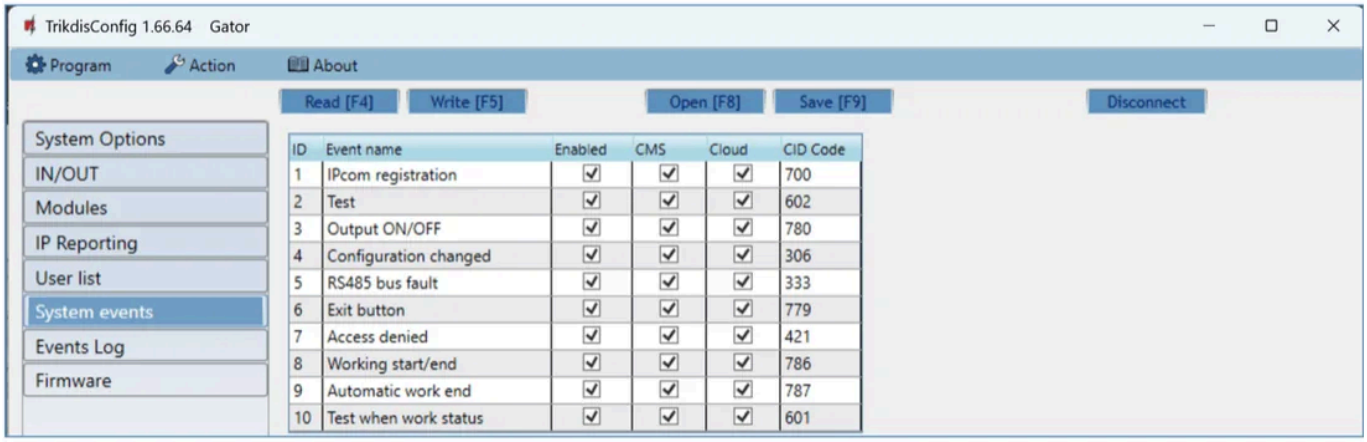


Figura 48. TrikdisConfig – **System events**: la lista de eventos con el código Contact ID (por ejemplo IPcom registration 700, Test 602, Output ON/OFF 780, Configuration changed 306, RS485 bus fault 333, Exit button 779, Access denied 421, Working start/end 786, Automatic work end 787), cada uno con las casillas **Enabled**, **CMS** y **Cloud**.

- **ID** – el número de orden del evento.
- **Event name** – el nombre del evento.
- **Enabled** – supervisión del evento.
- **CMS** – el evento se envía a la CRA.
- **Cloud** – el evento se envía a la aplicación Protegus 2.
- **CID Code** – el código Contact ID del evento.

5.8 Página «Events Log»

El registro de eventos propio del equipo, para la búsqueda de fallos y para consultar los accesos.

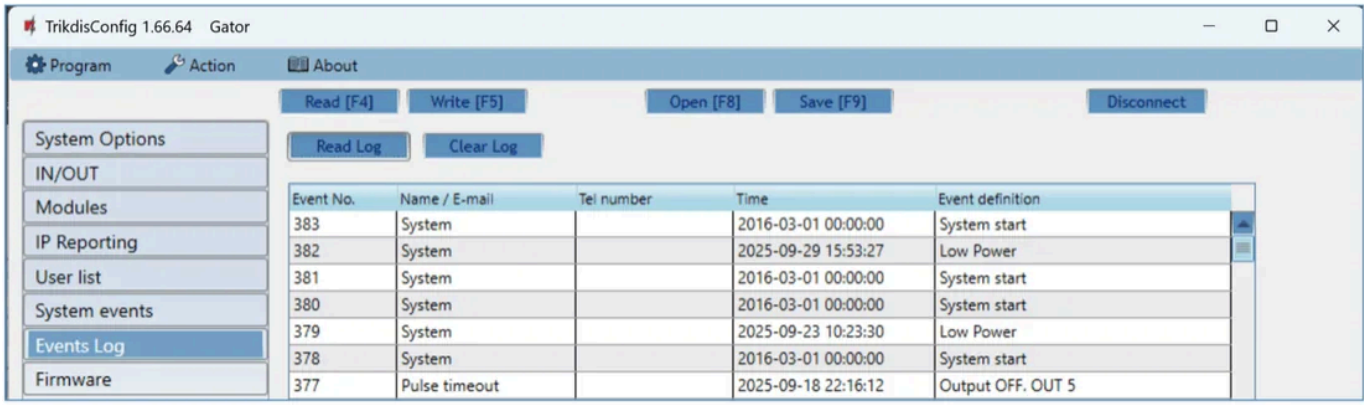


Figura 49. TrikdisConfig – **Events Log**: los botones **Read Log** y **Clear Log**; en los eventos, el número de orden, el nombre o la dirección de correo electrónico del usuario, el número de teléfono, la hora y la descripción del evento.

Haz clic en el botón **Read Log**: el programa lee los eventos de la memoria del equipo (hasta 5000). El registro muestra todas las operaciones y los eventos internos del GATOR con datos detallados: quién abrió la puerta, cuándo y con qué (llamada, SMS, aplicación, tarjeta), y qué entradas cambiaron. El botón **Clear Log** borra el registro.

5.9 Restablecimiento de la configuración de fábrica

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

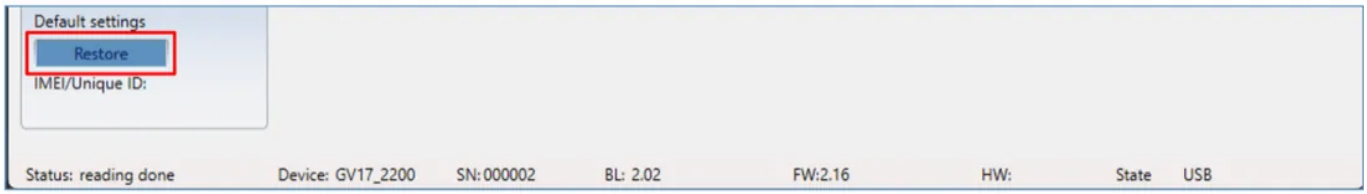


Figura 50. TrikdisConfig – el botón **Restore** del grupo **Default settings**, encima de la barra de estado.

5.10 Indicación del estado de la puerta

La aplicación Protegus 2 y el widget pueden mostrar el estado real de la puerta (abierta o cerrada). Para ello, la entrada **1 IN** del GATOR debe conectarse a la salida de estado del automatismo o al final de carrera de la puerta (apartado 3.5) y, en el programa, la entrada debe asignarse a la salida que conmuta la puerta:

1. En la página **IN/OUT**, la **1 IN** debe tener la función **Input**, con el tipo adecuado al contacto (en el ejemplo NO). En la fila de la **5 OUT**, en la columna **Assign IN**, elige la entrada **1 IN**.
2. Si también quieres un SMS sobre la apertura y el cierre de la puerta, escribe el **SMS event text** y el **SMS restore text** de la 1 IN (por ejemplo «Puerta abierta» / «Puerta cerrada»).

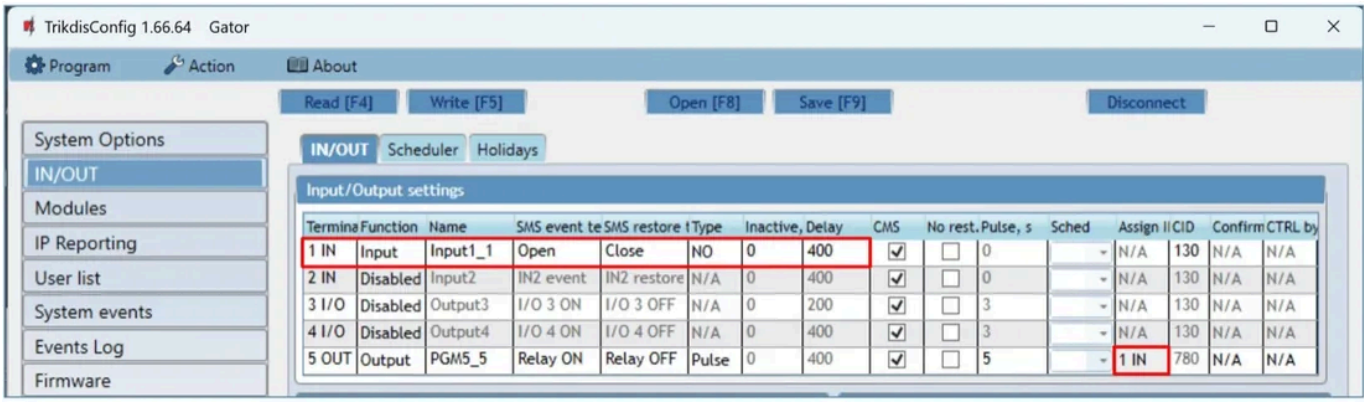


Figura 51. TrikdisConfig – IN/OUT: la entrada **1 IN** (NO, con los textos SMS **Open** / **Close**); en la fila de la **5 OUT**, en la columna **Assign IN**, la **1 IN**.

3. En la página **User list**, en la fila del usuario, haz clic en el botón **More settings** y, en el grupo **SMS notification for**, marca la casilla **IN1** para que el usuario reciba un SMS sobre el estado de la puerta. Haz clic en el botón **Save** y después escribe la configuración (**Write [F5]**).



Figura 52. TrikdisConfig – User list: el botón **More settings** en la fila del usuario.

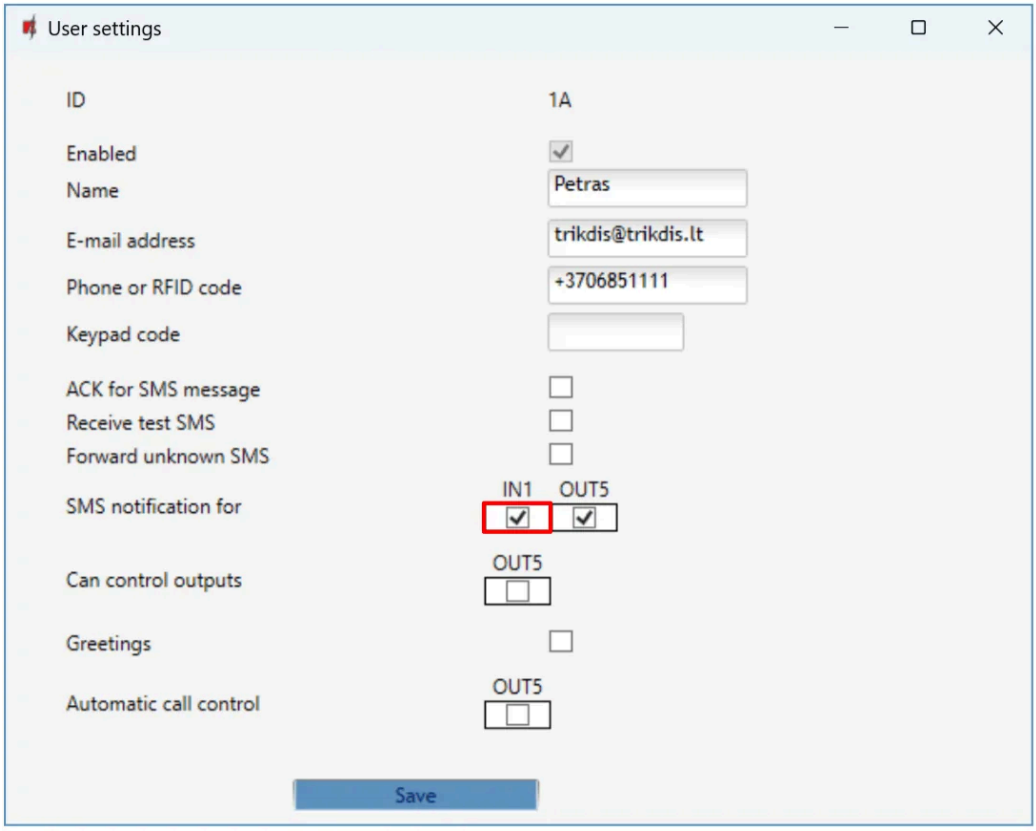


Figura 53. TrikdisConfig – User settings: en el grupo **SMS notification for**, **IN1** (y **OUT5**) marcados; abajo, el botón **Save**.

6. Programación a distancia

La configuración del GATOR también se puede leer y modificar a distancia a través de la nube de Protegus: no hace falta desplazarse al lugar.

Requisitos para la programación a distancia

En TrikdisConfig, en la página **IP Reporting**, debe estar marcado **Enable cloud service** (apartado 5.5; por SMS: `CONNECT 123456 PROTEGUS=ON`), la alimentación debe ser correcta (el LED **POWER** parpadea en verde) y el equipo debe estar en la red (el LED **NETWORK** se enciende en verde y parpadea en amarillo). Si no se cumplen estas condiciones, no se puede acceder al equipo a distancia.

1. Descarga e instala la versión más reciente de TrikdisConfig desde la web de Trikdis (https://www.trikdis.com), si todavía no la tienes en el ordenador.
2. Comprueba que el GATOR está conectado a internet y que la nube de Protegus está activada.
3. Inicia TrikdisConfig. En la parte **Remote access** de la pantalla inicial, escribe en el campo **Unique ID** el número **IMEI** del GATOR (está en la etiqueta de la parte inferior del equipo y de la caja; con conexión USB también lo ves en la barra de estado).
4. En el campo **System Name**, escribe un nombre cualquiera (por ejemplo, el nombre del objeto) y haz clic en el botón **Configure**.

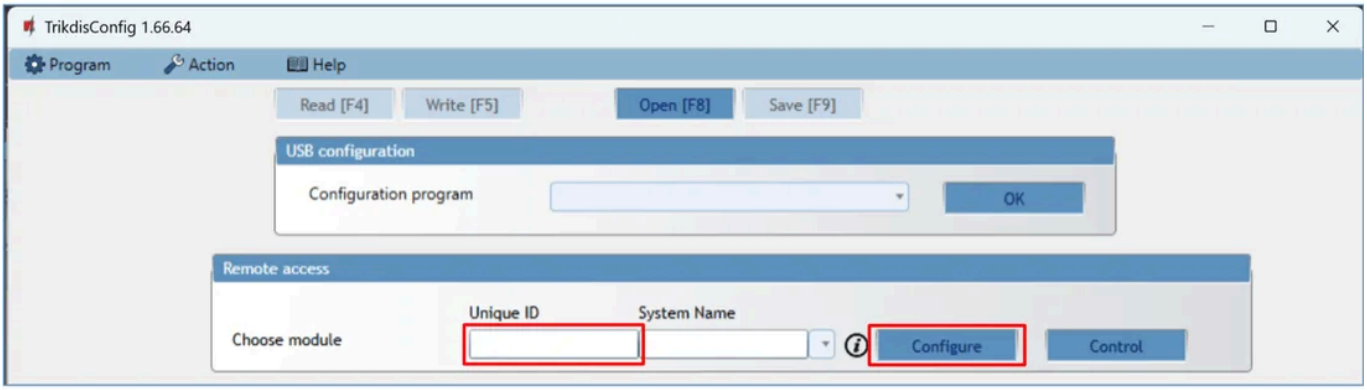


Figura 54. TrikdisConfig – la parte **Remote access**: el campo **Unique ID**, el campo **System Name** y el botón **Configure**.

5. Se abre la ventana de programación del GATOR. Haz clic en el botón **Read [F4]**: el programa lee la configuración actual del equipo. Si el programa pide el código de acceso, introduce el código de **administrador** de 6 dígitos. Si marcas la casilla **Remember password** y haces clic en el botón **Write [F5]**, el programa recuerda el código.
6. Haz los ajustes y escríbelos con el botón **Write [F5]**. Al final, desconéctate con el botón **Disconnect** y cierra el programa.

Para la programación a distancia no hace falta ayuda en el lugar: el cliente solo comprueba la alimentación y la red en los LED. Para modificar la lista de usuarios ni siquiera hace falta TrikdisConfig: el administrador también la gestiona desde Protegus 2 (apartado 4.5) o por SMS (apartado 4.7).

7. Comprobación del funcionamiento

Al final de la instalación y de la configuración, prueba todo el sistema en el lugar, antes de entregarlo:

1. **Alimentación**: el LED **POWER** parpadea en verde. Si parpadea en amarillo, la tensión de alimentación no es correcta: mídela en los bornes de alimentación (9–32 V DC o 12–24 V AC).

2. **Red**: el LED **NETWORK** se enciende en verde y parpadea en amarillo según la intensidad de la señal (3 destellos ya son suficientes). Si el LED **TROUBLE** parpadea, el número de destellos indica el fallo (apartado 1.5).
3. **Entradas**: activa una tras otra las entradas conectadas (contacto de estado de la puerta, pulsador de salida) y comprueba que los destinatarios reciben los mensajes correctos por SMS, en Protegus 2 y en la CRA.
4. **Salidas**: activa las salidas a distancia –con una llamada, desde la aplicación, por SMS y también con la tarjeta, si hay lector– y comprueba que la puerta se abre, que los destinatarios reciben los mensajes y que el estado de la puerta en la aplicación también sigue la realidad (apartado 5.10).

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.

El estado del equipo también se puede consultar por SMS desde el teléfono del administrador: con el comando `INFO 123456`, el GATOR devuelve su tipo, la intensidad de la señal, la tensión de alimentación, la versión del firmware, la fecha y la hora (apartado 4.7). Si no llega el SMS de respuesta, comprueba que en el administrador está activado **ACK for SMS message** (apartado 5.6).

8. Actualización del firmware

Si el GATOR está conectado a TrikdisConfig y hay un firmware más reciente, el programa ofrece la actualización por sí solo; para ello el ordenador debe estar conectado a internet. Si en el ordenador funciona un antivirus, puede bloquear la actualización automática; en ese caso, permite TrikdisConfig en el antivirus.

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.

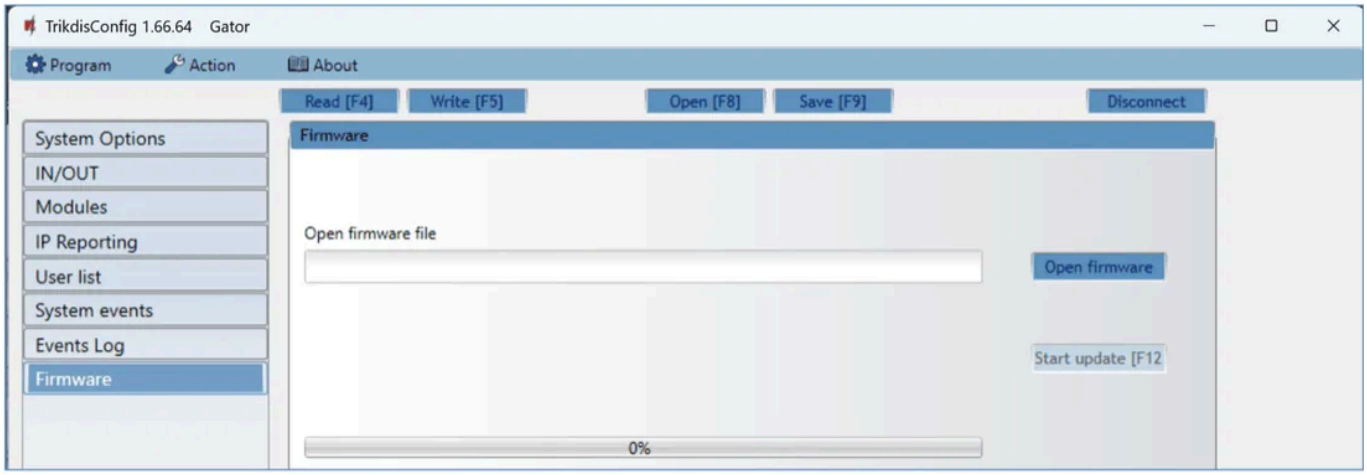


Figura 55. TrikdisConfig – GATOR, página **Firmware**: el botón **Open firmware**, el campo del archivo seleccionado, el botón **Start update [F12]** y el indicador de progreso.

En el GATOR, el botón que inicia la actualización se llama **Start update [F12]**. Para usar los módulos RF-LORA e iO-LORA hace falta como mínimo el firmware **2.13**, y para los módulos W485 y E485 como mínimo el **1.06**; la versión actual la ves en el campo **FW** de la barra de estado (apartado 5.1).

9. Solución de problemas y preguntas frecuentes

Si el equipo no hace lo que esperas, mira primero los LED (apartado 1.5) y después los puntos siguientes.

El LED TROUBLE parpadea: ¿qué significa el número de destellos?

El número de destellos indica la causa del fallo: **1** – no hay tarjeta SIM (o no hace contacto: sácala y vuelve a colocarla); **2** – el código PIN de la tarjeta SIM es incorrecto (desactiva la petición del PIN en un teléfono o escribe el PIN correcto en el campo **System Options** → **SIM card PIN**); **3** – no se puede conectar a la red móvil (intensidad de la señal, antena, si la tarjeta SIM está activa, tarjeta 2G en un equipo 4G); **4** – no se puede conectar a la nube de Protegus ni al receptor IP principal (datos móviles en la SIM, APN, dirección y puerto del receptor); **5** – no se puede conectar al receptor IP de reserva; **6** – el reloj interno no está ajustado (sincronización de la hora, comando `TIME`); **7** – la tensión de alimentación no es correcta.

Llamo, pero el GATOR no reacciona

- Si el LED **NETWORK** no se enciende en verde, el equipo no está en la red: comprueba la tarjeta SIM (activa, PIN desactivado, apta para recibir llamadas), la antena y la intensidad de la señal (el número de destellos amarillos).
- Si ya has añadido usuarios o la casilla **En** de la fila **Not authorized** (10) no está marcada, el equipo solo acepta llamadas de los números de la lista: el número de quien llama debe estar en la lista, en formato internacional (+CC…), habilitado (**En**), con un horario y un periodo de validez vigentes (apartado 5.6).
- El teléfono que llama no debe tener el número oculto; de lo contrario, el equipo no lo puede identificar.
- Comprueba que el número no está en la lista negra (apartado 5.6.4).

No abre con una llamada, pero sí desde la aplicación

Si hay un módulo W485 o E485 conectado al equipo, en la pestaña **Modules** → **Parameters**, en el grupo **SIM parameters**, mira la casilla **Use dial and SMS when working over internet module**: sin marcar, el equipo no usa llamadas ni SMS mientras dura la conexión a internet (apartado 5.4). Márcala si también

necesitas el control por llamada.

No puedo controlar con el teclado del teléfono durante la llamada

Para el control con el teclado (DTMF), el valor de **System Options** → **Hang-up after** debe ser mayor que 0; de lo contrario, el equipo rechaza la llamada al instante (apartado 4.2). En los equipos con código de tipo **GV17_2E70** y **GV17_2S70**, el control DTMF no funciona; el tipo lo muestra el campo **Device** de la barra de estado.

Protegus 2 no encuentra el equipo o no pasa a estado Online

- En la página **IP Reporting** debe estar marcado **Enable cloud service** (por SMS: `CONNECT 123456 PROTEGUS=ON`), y el LED **TROUBLE** no debe dar 4 destellos.
- La tarjeta SIM debe tener servicio de datos móviles y el APN debe ser correcto: en el campo **System Options** → **APN**, la casilla **Auto** elige de la lista incorporada; si no se establece la conexión, escribe el APN del operador (lista).
- En la aplicación, el IMEI debe ser exacto y, si el **Cloud Access Code** no es el de fábrica `123456`, introduce el correcto.
- Si todo está bien, espera como máximo 1 minuto después de añadirlo (apartado 4.3).

El widget no funciona o no lo encuentro

El widget solo está disponible en teléfonos **Android** (apartado 4.4); en iPhone se abre desde la pantalla de inicio de la aplicación. En Android, el GATOR debe estar añadido a los sistemas y debes haber iniciado sesión; si el widget sigue en gris, abre la aplicación una vez y comprueba la conexión a internet.

El lector RFID no lee la tarjeta o el GATOR no reacciona a ella

- Comprueba el conexionado según el esquema del apartado 3.6 (con un lector **D0** → **1 IN**, **D1** → **2 IN**; con el segundo lector **D0** → **3 I/O**, **D1** → **4 I/O**; negativo común) y la alimentación del lector: con un lector de 12 V, el GATOR debe funcionar con **alimentación DC**; con un lector con nivel de señal de 5 V, marca la casilla **Low voltage reader**.
- En la página **IN/OUT**, el **Wiegand reader mode** debe corresponder al número de lectores (**Single** / **Dual**), y la **3 I/O** y la **4 I/O** no deben estar configuradas para otra función.
- Si el equipo no reconoce las señales del lector, prueba la casilla **Disable reader filter**.
- La tarjeta debe estar en la tabla **User list** (registrada o escrita con su número), habilitada y con la salida del lector (apartado 5.6.2). El registro de eventos (apartado 5.8) muestra si la lectura se ha producido y por qué se ha rechazado (**Access denied**).

En la aplicación no se ve el estado real de la puerta

Para la indicación del estado de la puerta, la salida de estado del automatismo o el final de carrera de la puerta debe conectarse a la entrada **1 IN** (apartado 3.5); en la página **IN/OUT**, el tipo de la entrada debe ajustarse según el contacto y, en la fila de la **5 OUT**, en la columna **Assign IN**, debe seleccionarse la entrada **1 IN** (apartado 5.10). Después, en la aplicación, el icono de la salida muestra el estado de la entrada.

El equipo no responde a los comandos SMS

- Solo acepta comandos SMS de los números de **administrador** (1A–7A); el primero que llama o envía un SMS se convierte en el administrador. Si no sabes quién es, lee la tabla **User list** en TrikdisConfig.
- En el comando, la contraseña debe ir después de la palabra de comando, con un espacio (`INFO 123456`); la nueva contraseña tiene 6 caracteres.

- El SMS de respuesta solo llega si en el administrador está marcado **ACK for SMS message** (apartado 5.6).
- Si el equipo funciona con un módulo de internet (W485 / E485) y **Use dial and SMS when working over internet module** no está marcado, no procesa los SMS mientras dura la conexión a internet (apartado 5.4).

He olvidado la contraseña de administrador

La contraseña no se puede consultar. Conéctate al equipo con un cable USB y restablece la configuración de fábrica con el botón **Restore** de la parte inferior izquierda de la ventana de programación (apartado 5.9); así se borran la lista de usuarios y toda la configuración, por lo que después hay que volver a configurar el equipo. Si antes guardaste la configuración en un archivo (**Save [F9]**), después del restablecimiento la puedes cargar con el botón **Open [F8]** y solo tienes que volver a introducir la contraseña.

¿Hace falta una tarjeta SIM si uso un módulo W485 o E485?

No: con el módulo WiFi W485 o Ethernet E485, el GATOR también funciona sin tarjeta SIM; en ese caso el control se hace desde la aplicación (y con tarjeta RFID), sin llamadas ni SMS. En la pestaña **Modules** → **Parameters**, marca la casilla **Disable indication of the absence of a SIM card** para que el equipo no indique como fallo la falta de la tarjeta (apartado 5.4). Si también quieres la reserva por red móvil, coloca una tarjeta SIM y deja sin marcar la casilla **Disable the use of SIM card mobile data**.

Quiero controlar varias puertas desde un equipo

El relé propio del GATOR conmuta una puerta; los bornes **3 I/O** y **4 I/O**, como salidas de colector abierto (50 mA), pueden accionar un relé externo. Para puertas alejadas entre sí, con el transceptor **RF-LORA** se pueden conectar hasta 8 expansores inalámbricos **iO-LORA**, cada uno con su propio relé, entrada y lector RFID (apartado 3.9); para más entradas y salidas por cable, un expansor **iO8** o **iO8-LORA** (apartado 3.10). En los usuarios, en el campo **Can control output**, indicas qué salida pueden conmutar.

10. Instrucciones de seguridad

Figyelem!

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- El GATOR solo lo puede instalar y mantener una persona cualificada.
- Antes de la instalación, lee este manual para evitar errores que pueden provocar un funcionamiento incorrecto o daños en el equipo.
- **Antes de cada conexión eléctrica, desconecta la alimentación**, tanto la del GATOR como la del automatismo de la puerta.
- Los cambios, las modificaciones o las reparaciones no autorizados por el fabricante anulan la garantía.
- Respeta las normas locales de gestión de residuos: no tires el equipo ni sus piezas a la basura doméstica; entrega el equipo desechado como residuo electrónico.

Ver también

- El equipo de automatización de puertas GV17 se puede usar con Protegus 2: el GATOR y la aplicación juntos.
- GV17 como sistema de control de acceso y/o registro de jornada: lectores RFID, entrada y salida, jornada laboral en Protegus 2.
- Comunicación dual-path ahora también para el controlador de puertas GV17 GATOR: módulo W485 / E485 para el GATOR.
- Control de acceso inalámbrico y flexible con el sistema GATOR RF-LoRa: módulos RF-LORA e iO-LORA, varias puertas en un sistema.
- Configuración del APN – lista de operadores móviles europeos: si no se establece la conexión de datos móviles.
- Protegus: aplicación para Android / iPhone y web: sobre la aplicación.
- Documentación en inglés: docs.trikdis.com – Cellular gate controller GATOR.

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

Productos relacionados

Trikdis GV17 - GATOR controlador de acceso 4G GSM / IP

Trikdis GV17 - GATOR controlador de acceso 2G GSM / IP

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

Trikdis RF-LORA módulo expansor inalámbrico

Trikdis IO-LORA módulo expansor inalámbrico **Trikdis iO8 módulo expansor cableado**

Trikdis IO8-LORA módulo expansor inalámbrico

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

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

Derechos de autor

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

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

Versión siempre actualizada de este manual: https://trikdis.es/manual-gv17