mobilamb
TRIKDIS Official Distributor

GV17 GATOR Torsteuerung – Installations- und Programmieranleitung

Installations- und Programmieranleitung für die Trikdis GV17 GATOR Torsteuerung: Anschluss, SIM-Karte und Einrichtung in TrikdisConfig, Benutzer und Berechtigungen, Steuerung per Anruf, SMS und über die App Protegus 2.



Ausgabe: 2026-11-18
Immer aktuelle Webversion: https://trikdis.at/gv17-anleitung

Inhalt

1. Übersicht

1.1 Wofür er gedacht ist und wie er funktioniert
1.2 Varianten
1.3 Technische Daten
1.4 Teile und Klemmen des Geräts
1.5 LED-Anzeigen
1.6 Lieferumfang und benötigtes Werkzeug

2. Schnellinbetriebnahme

2.1 Inbetriebnahme in drei Schritten
2.2 Nur Berechtigte sollen öffnen können
2.3 App und Leitstelle einrichten

3. Installation und Anschluss

3.1 Befestigung und Einlegen der SIM-Karte
3.2 Stromversorgung
3.3 Eingänge
3.4 Anschluss eines Relais an den Universalausgang
3.5 Anschluss des Torantriebs
3.6 Anschluss eines RFID-Lesers (Wiegand 26/34)
3.7 WLAN-Modul W485
3.8 Ethernet-Modul E485
3.9 RF-LORA und iO-LORA Erweiterungen mit RFID-Leser
3.10 Erweiterung iO8 und iO8-LORA

4. Fernsteuerung

4.1 Steuerung per Telefonanruf
4.2 Steuerung mit der Telefontastatur (DTMF)
4.3 Steuerung aus der App Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.4 Widget auf dem Startbildschirm des Telefons
4.5 Benutzerverwaltung in der App
4.6 Steuerung per SMS-Nachricht
4.7 Programmierung per SMS

5. Einrichtung mit der Software TrikdisConfig

5.1 Die Statusleiste
5.2 Seite „System Options"
5.3 Seite „IN/OUT"
5.3.1 Reiter IN/OUT – die Ein- und Ausgänge
5.3.2 Reiter Scheduler – Zeitpläne der Ausgänge
5.3.3 Reiter Holidays – Feiertage
5.4 Seite „Modules"
5.4.1 Reiter Modules
5.4.2 Reiter Parameters – WLAN-Modul W485
5.4.3 Reiter Parameters – Ethernet-Modul E485
5.5 Seite „IP Reporting"
5.6 Seite „User list"

5.6.1 Reiter Users – die Benutzer
5.6.2 Registrieren einer RFID-Karte (eines Schlüsselanhängers)
5.6.3 Reiter Scheduler – Zeitpläne der Benutzer
5.6.4 Reiter Black list – Sperrliste
5.7 Seite „System events“
5.8 Seite „Events Log“
5.9 Zurücksetzen auf Werkseinstellungen
5.10 Anzeige des Torzustands
6. Fernprogrammierung
7. Funktionsprüfung
8. Firmware-Aktualisierung
9. Fehlersuche und häufige Fragen
10. Sicherheitshinweise
Siehe auch

1. Übersicht

Der **GV17 GATOR** ist die Mobilfunk-Torsteuerung von Trikdis: Er ist für die Fernsteuerung von elektrischen Toren, Schranken, Garagentoren und anderen Geräten ausgelegt. Der Benutzer steuert ihn per **Telefonanruf**, per **SMS-Nachricht** oder aus der App **Protegus 2**; das Gerät verwaltet die Telefonnummern (RFID-Karten, E-Mail-Adressen) von bis zu **7 Administratoren** und **1000 Benutzern**, und für jeden Benutzer lassen sich eine eigene zeitliche Beschränkung (Zeitplan, Gültigkeitsdauer) und ein Zähler einstellen. Über Zustandsänderungen der Eingänge und Ausgänge (Auslösung und Wiederherstellung) benachrichtigt der GATOR per SMS und in der App – den Text der SMS-Nachrichten legen Sie selbst fest –, und er leitet die Ereignisse im Contact-ID-Format auch an die Leitstelle weiter. Mit einem **W485** WLAN- oder einem **E485** Ethernet-Modul funktionieren Steuerung und Übertragung auch über das Internet, ohne mobile Daten; mit einem **RF-LORA** Sende-Empfänger lassen sich bis zu 8 drahtlose **iO-LORA** Erweiterungen und eine **iO8-LORA** Erweiterung anschließen, sodass mit einem Gerät bis zu 8 weit voneinander entfernte Tore oder Schranken gesteuert werden können, jedes mit eigenem RFID-Leser (die an die iO-LORA Erweiterungen angeschlossenen RFID-Leser können bis zu 8 Ausgänge schalten – ein Leser schaltet immer nur einen Ausgang seiner eigenen Erweiterung –, dafür ist GATOR-Firmware 2.13 oder neuer erforderlich). Die Einstellungen nehmen Sie mit der Software **TrikdisConfig** über ein USB-Kabel oder aus der Ferne vor.



Abbildung 1. Die Torsteuerung GV17 GATOR: vorne die Anzeigen NETWORK, DATA, POWER und TROUBLE, oben der Antennenanschluss, unten die abnehmbare Klemmleiste.

1.1 Wofür er gedacht ist und wie er funktioniert

Wofür er am häufigsten eingesetzt wird

- **Fernöffnen von Tor, Schranke oder Garagentor** für die Familie, die Hausgemeinschaft, die Mitarbeiter eines Unternehmens oder die Mieter eines Parkplatzes: Der Benutzer ruft die Nummer der SIM-Karte des GATOR an, und das Tor öffnet sich – das Gerät weist den Anruf ab, daher ist der Anruf kostenlos. Dasselbe geht auch aus der App mit einer Taste, mit einem Widget auf dem Startbildschirm des Telefons oder per SMS.
- **Zutrittskontrolle mit RFID-Karte und Code**: mit einem oder zwei Wiegand-26/34-Lesern (Ein- und Ausgang), Ausgang per Taster, mit Zeitplan je Benutzer (wer wann eintreten darf), Gültigkeitsdauer und Zutrittszähler; aus den Ein- und Ausgängen lässt sich in Protegus 2 auch eine **Arbeitszeiterfassung** erstellen – dazu gibt es einen eigenen Artikel: GV17 als Zutrittskontroll- und/oder Arbeitszeiterfassungssystem.
- **Beliebige andere Geräte** aus der Ferne ein- und ausschalten, im Impuls- oder im Dauerbetrieb (zwei Schaltzustände), auch nach Zeitplan: Beleuchtung, Bewässerung, Pumpe, Heizung.
- **Mehrere Tore in einem System**: mit den Modulen RF-LORA und iO-LORA drahtlos, bis zu 8 Standorte, jeder mit eigenem Relais, Eingang und RFID-Leser – Flexible drahtlose Zutrittskontrolle mit dem GATOR RF-LoRa-System.

Wie er funktioniert

- **Steuerung**: per Telefonanruf (werkseitig jeder, der anruft; mit Benutzerliste nur die Berechtigten), während des Anrufs mit der Telefontastatur (DTMF), per SMS-Befehl, aus der mobilen und der Web-App Protegus 2, mit einem Android-Widget, mit RFID-Karte und Code.
- **Benachrichtigung des Benutzers**: per SMS an die Administratoren (über Ereignisse der Eingänge und Ausgänge, Test, neuer Benutzer), per Push-Nachricht in der App Protegus 2.
- **Übertragung an die Leitstelle**: mit Contact-ID-Ereigniscodes an die Software- und Hardware-IP-Empfänger von Trikdis, die mit jeder Leitstellensoftware zusammenarbeiten; Haupt- und Ersatzempfänger (bricht die Verbindung zum Hauptempfänger ab, gehen die Nachrichten automatisch an den Ersatzempfänger), SMS-Ersatzweg; die Ereignisse können gleichzeitig an die Leitstelle und an Protegus 2 gehen.
- **Eingänge und Ausgänge**: 2 Eingänge (NO, NC oder EOL 10 kΩ), 2 Universalklemmen (Eingang oder Open-Collector-Ausgang, 50 mA), 1 Relaisausgang (1 A / 30 V DC, 0,5 A / 125 V AC). Jede iO-LORA Erweiterung ergänzt das System um 1 Eingang und 1 Relaisausgang (bis zu 8 Erweiterungen, also insgesamt 8 weitere Eingänge und 8 Ausgänge), die Erweiterung iO8 oder iO8-LORA um weitere Ein- und Ausgänge (eine davon lässt sich an den GATOR anschließen).
- **Installation und Einrichtung**: ab Werk betriebsbereit; Benutzer fügen Sie aus der App Protegus 2 (als Administrator), per SMS oder mit der Software TrikdisConfig hinzu und löschen sie dort; die Einrichtung erfolgt mit einem USB-Mini-B-Kabel oder aus der Ferne; die Firmware lässt sich auch aus der Ferne aktualisieren; zwei Zugriffsebenen (Errichter und Administrator).

1.2 Varianten

Den GATOR gibt es in zwei Mobilfunk-Varianten; Anschluss, Einrichtung und Steuerung sind bei beiden gleich, nur das Modem unterscheidet sich. In der Statusleiste von TrikdisConfig sehen Sie den genauen Typ in der Form **GV17_xxxx** (Abschnitt 5.1).

Variante	Modem	Frequenzbänder
GV17-4G	4G (LTE)	In Europa LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 (für Lateinamerika gibt es eine Variante mit anderer Bandbelegung)
GV17-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis GV17 - GATOR smarter 4G GSM / IP Torcontroller

Trikdis GV17 – GATOR Smart 2G GSM / IP Torsteuerung

Da die 2G-Netze schrittweise abgeschaltet werden, empfehlen wir für neue Installationen die 4G-Variante. Bei Geräten mit dem Typcode **GV17_2E70** und **GV17_2S70** funktioniert die Steuerung mit der Tastatur während des Anrufs (DTMF) nicht (Abschnitt 4.2); die Steuerung per Anruf, per SMS und aus der App funktioniert auch bei diesen genauso.

1.3 Technische Daten

Merkmal	Wert
Frequenzbänder des 2G-Modems (GSM)	850 / 900 / 1800 / 1900 MHz
Frequenzbänder des 4G-Modems (LTE)	Europa: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28; Lateinamerika: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Versorgungsspannung	9–32 V DC oder 12–24 V AC
Stromaufnahme	100 mA
Eingänge	2, wählbarer Typ: NC, NO, EOL = 10 kΩ
Universal-Ein-/Ausgänge	2; als Eingang NC, NO, EOL = 10 kΩ, als Ausgang Open Collector (OC), höchstens 50 mA
Ausgang	1 Relais, 1 A / 30 V DC, 0,5 A / 125 V AC
Speicher für nicht gesendete Ereignisse	bis zu 60 Ereignisse
Ereignisprotokoll	bis zu 5000 Ereignisse
Benutzer, die Nachrichten erhalten und steuern dürfen (Administratoren)	7
Benutzer mit Steuerberechtigung	1000
Betriebsumgebung	–20 … +50 °C, höchstens 80 % relative Luftfeuchtigkeit bei +20 °C
Abmessungen	92 × 62 × 26 mm
Gewicht	80 g

1.4 Teile und Klemmen des Geräts

Die Zahlen in der Abbildung bezeichnen die Teile des Geräts; die Bedeutung der Klemmen steht in der Tabelle.

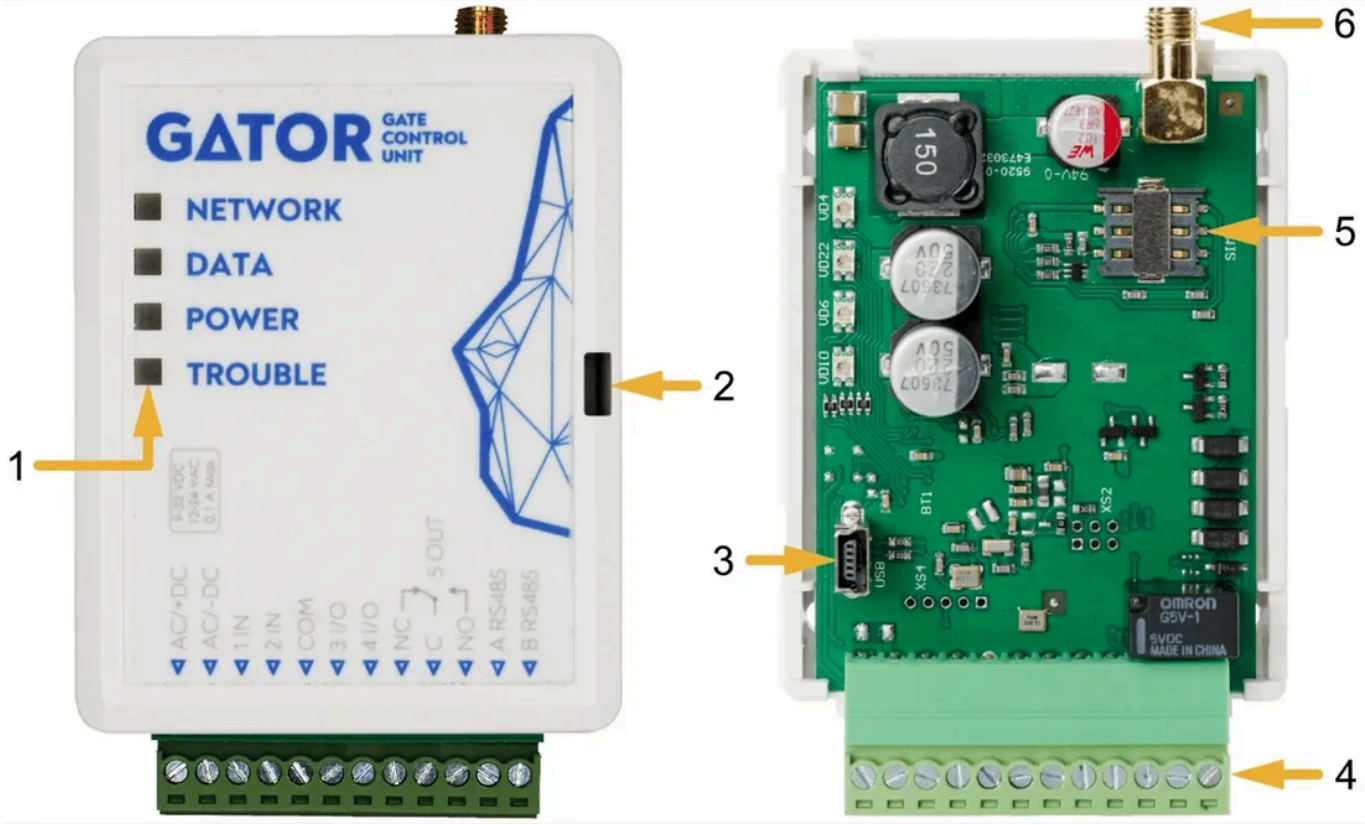


Abbildung 2. Die Teile des GATOR.

- 1 LED-Anzeigen
- 2 Öffnung zum Abnehmen der Frontabdeckung
- 3 USB-Mini-B-Anschluss zum Programmieren
- 4 abnehmbare Klemmleiste
- 5 Halter für die Nano-SIM-Karte
- 6 SMA-Anschluss der Mobilfunkantenne

Klemme	Funktion
AC/+DC	Versorgungsspannung: Pluspol von 9–32 V DC oder 12–24 V AC
AC/−DC	Versorgungsspannung: Minuspol von 9–32 V DC oder 12–24 V AC
1 IN	Eingang 1, Typ NO, NC oder EOL (werkseitig: NO-Eingang)
2 IN	Eingang 2, Typ NO, NC oder EOL (werkseitig: deaktiviert)
COM	gemeinsamer Bezugspunkt für die Eingänge
3 I/O	Eingang oder Ausgang (werkseitig: deaktiviert)
4 I/O	Eingang oder Ausgang (werkseitig: deaktiviert)
NC	Öffnerkontakt des Relais (in Ruhe geschlossen)
C	gemeinsamer Kontakt des Relais
NO	Schließerkontakt des Relais (in Ruhe offen)
A RS485	Ader A des RS485-Busses
B RS485	Ader B des RS485-Busses

Die Software und die SMS-Befehle bezeichnen den Relaisausgang als **5 OUT** (OUTPUT5) und die beiden Universalklemmen, wenn sie als Ausgang dienen, als **3 OUT** und **4 OUT**. Die 12-polige Klemmleiste lässt sich vom Gerät abziehen und ist auch einzeln erhältlich:

1.5 LED-Anzeigen

Anzeige	Licht	Bedeutung
NETWORK	grün, dauerhaft	mit dem Mobilfunknetz verbunden
	gelb blinkend	Signalstärke des Mobilfunknetzes mit 0–5 Blinkimpulsen; 3 reichen bereits aus
DATA	grün, dauerhaft	Nachricht wird gesendet
	gelb, dauerhaft	im Speicher warten Ereignisse auf das Senden
POWER	grün blinkend	die Versorgungsspannung ist in Ordnung
	gelb blinkend	die Versorgungsspannung ist nicht in Ordnung
	rot und gelb blinkend	Konfigurationsmodus
TROUBLE	aus	kein Betriebsfehler
	1 Blinkimpuls	keine SIM-Karte
	2 Blinkimpulse	der PIN-Code der SIM-Karte ist falsch
	3 Blinkimpulse	keine Verbindung zum Mobilfunknetz möglich
	4 Blinkimpulse	keine Verbindung zur Protegus-Cloud oder zum primären IP-Empfänger möglich
	5 Blinkimpulse	keine Verbindung zum Ersatz-IP-Empfänger möglich
	6 Blinkimpulse	die interne Uhr ist nicht gestellt
	7 Blinkimpulse	die Versorgungsspannung ist nicht in Ordnung

Wenn keine der LEDs leuchtet, prüfen Sie die Versorgungsspannung und die Verdrahtung.

Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

1.6 Lieferumfang und benötigtes Werkzeug

Im Karton: 1 Torsteuerung GV17 GATOR, 1 Mobilfunkantenne, 3 Widerstände 10 kΩ, 1 Stück doppelseitiges Klebeband (5 cm) und 2 Schrauben.

Was Sie benötigen

Prüfen Sie vor Beginn der Installation, ob Sie alles zur Hand haben: USB-Mini-B-Kabel für die Einrichtung · Kabel mit mindestens 4 Adern für den Anschluss · Schlitzschraubendreher 2,5 mm · aktivierte Nano-SIM-Karte (PIN-Abfrage ausschalten) mit mobilem Datendienst, wenn Sie auch die App oder die Leitstelle nutzen · externe Antenne, wenn das Signal am Standort schwach ist · die Errichteranleitung des gesteuerten Geräts (Torantrieb, Schranke) mit dem Anschluss seines Steuereingangs und seines Torzustandsausgangs. Die aufgeführten Zubehörteile müssen Sie separat beschaffen – bestellen Sie sie bei Ihrem Händler.

Bei schwachem Signal, in einem Metallgehäuse oder hinter einer dicken Wand verwenden Sie statt der Antenne aus dem Lieferumfang eine abgesetzt montierbare Antenne mit 2,5 m Kabel:

Trikdis ME301M Magnetantenne mit 2,5 m Draht

Trikdis Ant04 GSM Stick-On-Antenne mit 2,5 m Draht

2. Schnellinbetriebnahme

Der GATOR ist ab Werk betriebsbereit

Wenn jemand die Telefonnummer der eingelegten SIM-Karte anruft, weist der GATOR den Anruf ab und schaltet den Relaisausgang **5 OUT** für **3 Sekunden** ein. Wenn Ihnen diese Funktionsweise genügt, kann das Gerät ohne weitere Einstellungen in Betrieb genommen werden.

2.1 Inbetriebnahme in drei Schritten

1. **Legen Sie die Nano-SIM-Karte** in den Halter des GATOR ein (Abschnitt 3.1). Schalten Sie vorher in einem Telefon die PIN-Abfrage der Karte aus, sonst meldet sich das Gerät nicht im Netz an (oder Sie müssen die PIN in TrikdisConfig eingeben, Abschnitt 5.2).
2. **Schließen Sie Versorgung und Torantrieb an** gemäß den Zeichnungen in Kapitel 3: die Versorgung an die Klemmen **AC/+DC** und **AC/−DC**, den Steuereingang des Torantriebs an die Kontakte **C** und **NO** des Relais.
3. **Schalten Sie die Versorgung ein.** Bei korrektem Betrieb blinkt die LED **POWER** grün, die LED **NETWORK** leuchtet grün und blinkt zwischendurch entsprechend der Signalstärke gelb. Rufen Sie die Nummer der SIM-Karte an: Das Gerät weist den Anruf ab, und das Relais zieht für 3 Sekunden an.

2.2 Nur Berechtigte sollen öffnen können

Ab Werk kann **jeder** den GATOR steuern, der seine Nummer anruft. Wenn Sie das nur bestimmten Personen erlauben möchten, senden Sie eine SMS mit der Telefonnummer der Benutzer (senden Sie den Befehl von Ihrem eigenen Telefon, denn wer das Gerät als Erster anruft oder ihm als Erster eine SMS sendet, wird sein Administrator, Abschnitt 4.1):

```
SETU 123456 +436641234567#Peter#peter@beispiel.at
```

Nach dem Anlegen der ersten Nummer reagiert der GATOR nur noch auf Anrufe von Nummern auf der Liste, alle anderen ignoriert er. Weitere Benutzer fügen Sie auf die gleiche Weise einzeln hinzu; den vollständigen SMS-Befehlssatz beschreibt Abschnitt 4.7, die Liste können Sie auch in TrikdisConfig und in der App Protegus 2 verwalten (Abschnitte 5.6 und 4.5).

Ändern Sie das Administratorpasswort

Mit dem werkseitigen Passwort `123456` kann jeder, der die Nummer des Geräts kennt, den GATOR umprogrammieren. Ändern Sie es bei der ersten Inbetriebnahme per SMS (`PSW 123456 neuespasswort`, 6 Zeichen) oder in TrikdisConfig (**System Options** → **Administrator Code**).

2.3 App und Leitstelle einrichten

- **App Protegus 2:** Schalten Sie in TrikdisConfig auf der Seite **IP Reporting** den Cloud-Dienst ein (**Enable cloud service**, Abschnitt 5.5) und ändern Sie den werkseitigen Code `123456` unter **Cloud Access Code**; dasselbe per SMS: `CONNECT 123456 PROTEGUS=ON`. Danach kann das System gemäß Abschnitt 4.3 zur App hinzugefügt werden. Dafür braucht die SIM-Karte einen mobilen Datendienst (oder ein W485 / E485 Modul).
- **Leitstelle:** Geben Sie auf der Seite **IP Reporting** die Adresse, den Port und den Verschlüsselungsschlüssel des Empfängers ein, auf der Seite **System Options** die Objektkennung (Abschnitte 5.2 und 5.5).
- **Empfohlene Reihenfolge der Einstellungen in TrikdisConfig:** Administratorpasswort und SIM-Daten (APN) → Funktion der Ein- und Ausgänge, Impulsdauer → Benutzer, RFID-Karten, Zeitplan → Cloud und Leitstelle → Prüfung gemäß Kapitel 7.

Wenn Sie die Werkseinstellungen ändern oder weitere Funktionen des Geräts einschalten möchten, finden Sie die Einstellungen der Software TrikdisConfig in Kapitel 5.

3. Installation und Anschluss

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.

Dieses Kapitel beschreibt die Befestigung des GATOR, die Stromversorgung, den Anschluss der Eingänge, des Relais und des Torantriebs sowie danach den Anschluss der RFID-Leser und der Erweiterungsmodule (W485, E485, RF-LORA + iO-LORA, iO8 / iO8-LORA). In den Zeichnungen stimmen die Klemmennamen des GATOR mit der Beschriftung des Geräts überein (Abschnitt 1.4).

3.1 Befestigung und Einlegen der SIM-Karte

1. Nehmen Sie die Frontabdeckung ab (stecken Sie den Schraubendreher in die seitliche Öffnung und hebeln Sie sie ab), und ziehen Sie dann die Klemmleiste ab.
2. Nehmen Sie die Leiterplatte aus dem Gehäuse: Drücken Sie die Haltelasche und heben Sie die Platine heraus.
3. Befestigen Sie die Gehäuserückwand mit Schrauben (oder mit dem beiliegenden doppelseitigen Klebeband) an der gewünschten Stelle.
4. Setzen Sie die Leiterplatte und die Klemmleiste wieder ein.
5. Schrauben Sie die Mobilfunkantenne auf den SMA-Anschluss.
6. Legen Sie die Nano-SIM-Karte in den Halter ein.
7. Setzen Sie die Frontabdeckung wieder auf.

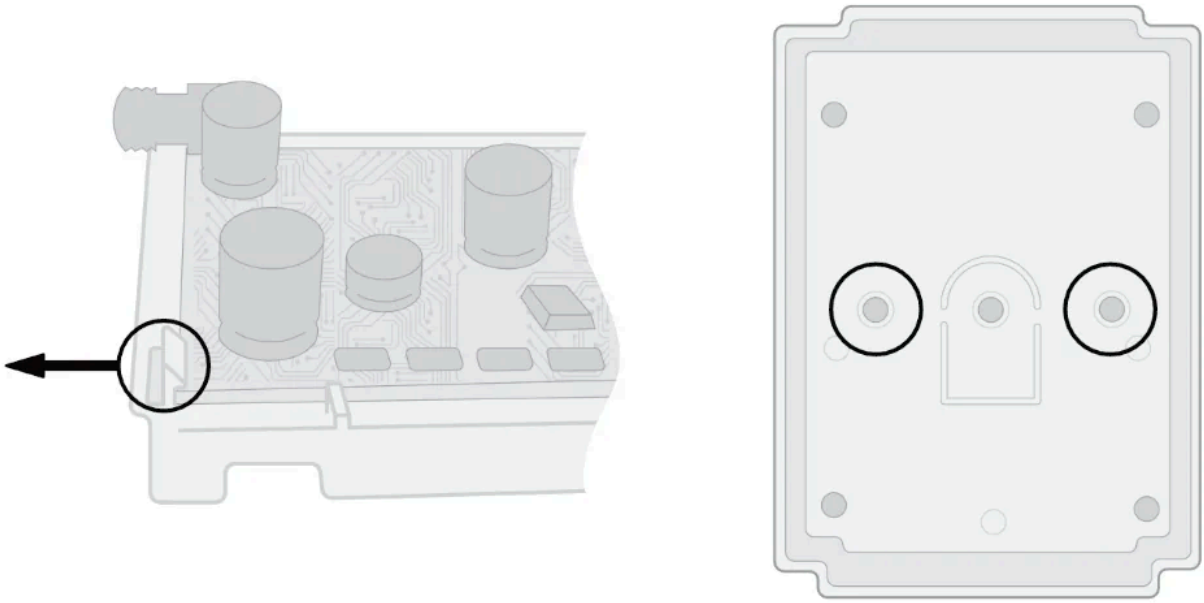


Abbildung 3. Links die Haltelasche der Leiterplatte (in Pfeilrichtung gedrückt, gibt sie die Platine frei), rechts die beiden Schraubenlöcher der Rückwand.

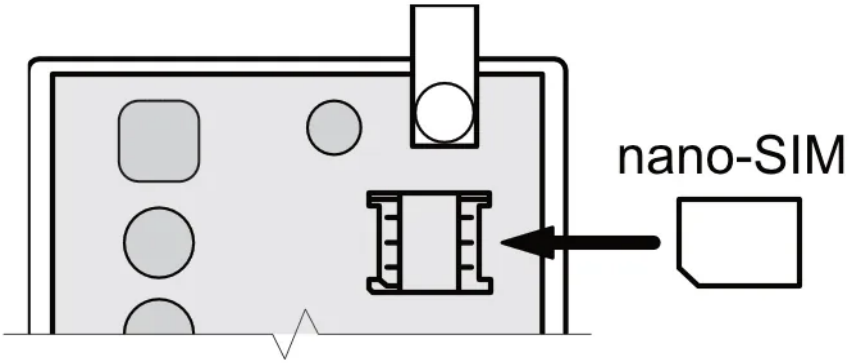


Abbildung 4. Einlegen der Nano-SIM-Karte in Pfeilrichtung in den Halter auf der Leiterplatte.

Die Klemmleiste ist abziehbar: So lässt sich das Gerät mit einem Handgriff spannungsfrei machen oder neu starten, beim Anschließen ist es leichter zu handhaben, und für die Programmierung über USB kann das Gerät zum Computer gebracht werden.

3.2 Stromversorgung

Der GATOR arbeitet mit **9–32 V DC** oder **12–24 V AC**; die beiden Versorgungsklemmen (**AC/+DC**, **AC/–DC**) nehmen beide Versorgungsarten an. In den meisten Fällen genügt der Zubehör-Versorgungsausgang der Steuereinheit des Torantriebs (typischerweise 24 V AC oder DC), sodass kein eigenes Netzteil nötig ist. Bei eigener Versorgung eignet sich ein Transformator ~230 V / 16 V mit mindestens 10 VA (auf der 230-V-Seite mit einer Sicherung 125 mA) oder ein Gleichspannungsnetzteil 9–32 V mit mindestens 0,2 A. Das Gerät hat keinen Notstromakku: Wenn sich das Tor auch bei Stromausfall öffnen muss, betreiben Sie es an einer unterbrechungsfreien Stromversorgung. Schließen Sie die Leitungen gemäß der folgenden Zeichnung an.

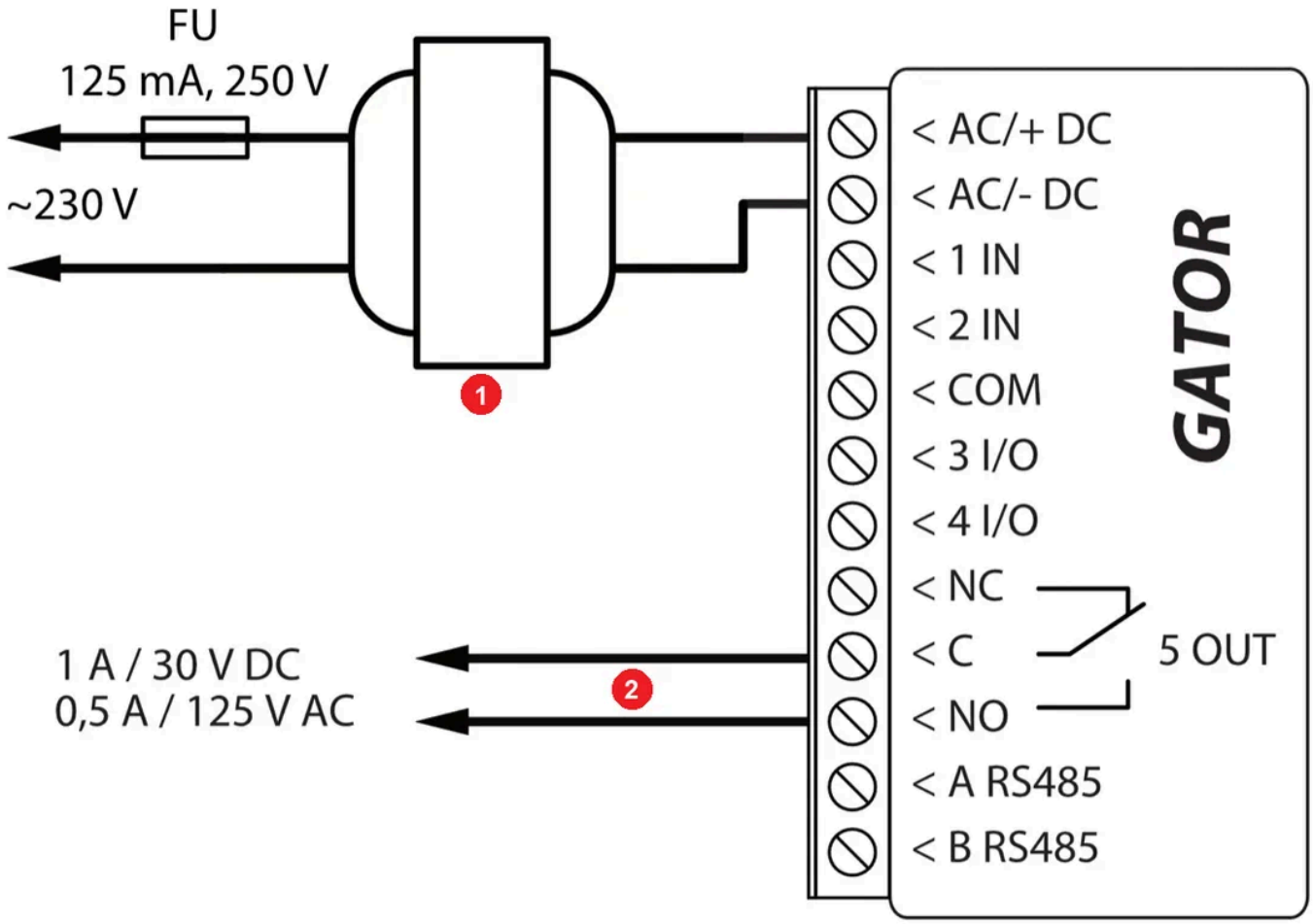


Abbildung 5. Anschluss der Stromversorgung und des Torantriebs: Netzversorgung über einen Transformator ~230 V / 16 V, 10 VA, 50 Hz (Sicherung 125 mA, 250 V) oder über ein Gleichspannungsnetzteil 9–32 V, 0,2 A an die Klemmen AC/+DC und AC/−DC; der Steuereingang des Torantriebs an die Kontakte C und NO des Relais; Belastbarkeit des Relais 1 A / 30 V DC oder 0,5 A / 125 V AC.

- 1 Transformator, ~230 V / 16 V, 10 VA, 50 Hz („Transformer“) oder Gleichspannungsnetzteil, 9–32 V, 0,2 A („or DC power supply source“)
- 2 Torsteuerung („Gate control“) – der Steuereingang des Torantriebs

Die Versorgung der RFID-Leser, der Relais und der Erweiterungsmodule nehmen die Zeichnungen von der Klemme **AC/+DC** ab: Das ist nur bei **Gleichspannungsversorgung** möglich (in den Zeichnungen 9–16 V DC, 0,5 A, beim W485 / E485 und beim iO8 Modul 10–28 V DC). Bei Wechselspannungsversorgung brauchen der Leser und das Modul ein eigenes DC-Netzteil.

3.3 Eingänge

Der GATOR hat **vier Eingänge**: **1 IN** und **2 IN** sind immer Eingänge, **3 I/O** und **4 I/O** sind Universalklemmen, die als Eingang oder als Ausgang eingestellt werden können. Alle arbeiten gegenüber der Klemme **COM** und können vom Typ **NO**, **NC** oder **EOL** (mit 10-kΩ-Abschlusswiderstand) sein; drei Abschlusswiderstände liegen dem Gerät bei. An einen Eingang können Sie den Endschalter oder den Zustandsausgang des Tors anschließen (Torzustandsanzeige, Abschnitte 3.5 und 5.10), einen Ausgangstaster (Abschnitt 3.6) oder einen beliebigen Melder oder Kontakt, über dessen Änderung Sie eine SMS oder Push-Nachricht erhalten möchten oder mit dem Sie einen Ausgang schalten wollen (**CTRL by IN**, Abschnitt 5.3). Typ und Reaktionszeit stellen Sie in TrikdisConfig auf der Seite **IN/OUT** ein; ab Werk ist nur 1 IN aktiv (NO). Schließen Sie die Eingänge entsprechend dem eingestellten Typ (NC, NO, EOL) gemäß der folgenden Zeichnung an.

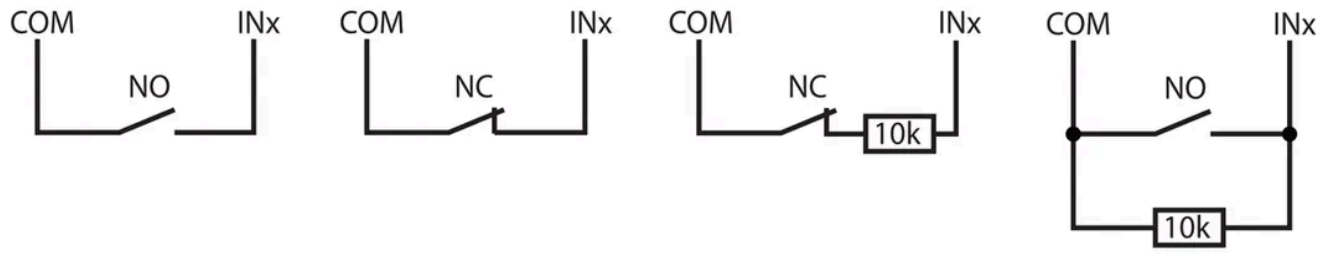


Abbildung 6. Die vier Anschlussarten der Eingänge zwischen der Klemme COM und der Klemme IN. Von links nach rechts: **NO** – Schließerkontakt (in Ruhe offen) – Schließen = Alarm, Öffnen = Wiederherstellung; **NC** – Öffnerkontakt (in Ruhe geschlossen) – Öffnen = Alarm, Schließen = Wiederherstellung; **NC + EOL** – Öffnerkontakt mit in Reihe geschaltetem 10-kΩ-Widerstand – Kurzschluss und Unterbrechung = Alarm, 10 kΩ = Ruhe; **NO + EOL** – Schließerkontakt mit parallel geschaltetem 10-kΩ-Widerstand – Kurzschluss und Unterbrechung = Alarm, 10 kΩ = Ruhe.

3.4 Anschluss eines Relais an den Universalausgang

Die Klemmen **3 I/O** und **4 I/O** sind als Ausgang Open-Collector-Ausgänge mit einer Belastbarkeit von höchstens **50 mA**: Direkt können sie nur die Spule eines kleinen Relais schalten. Mit den Kontakten des Relais lässt sich ein beliebiges Gerät aus der Ferne ein- und ausschalten. Die Zeichnung gilt für Gleichspannungsversorgung: Ein Ende der Spule geht an die Klemme **AC/+DC**, das andere an den Ausgang; in TrikdisConfig muss die Funktion der Klemme auf **Output** gestellt werden (Abschnitt 5.3).

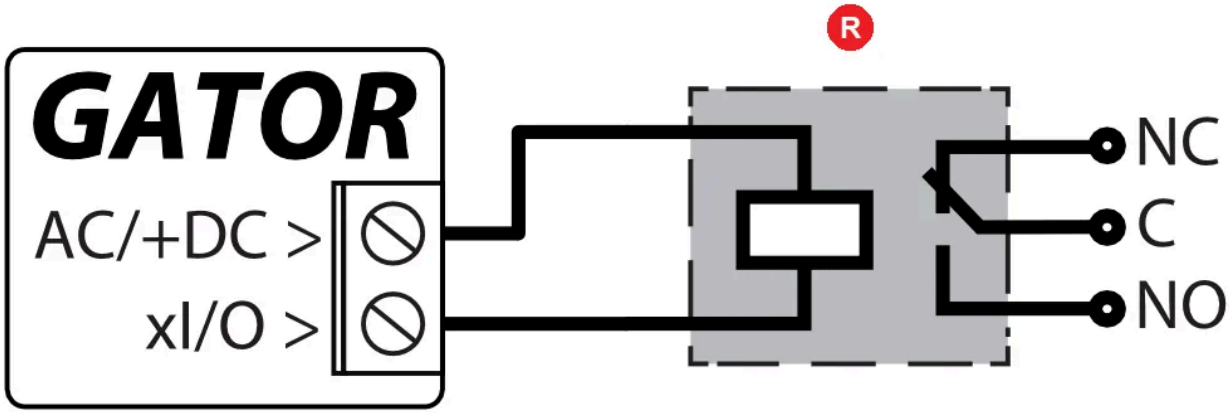


Abbildung 7. Externes Relais am Universalausgang: die Spule zwischen AC/+DC und der als Ausgang eingestellten Klemme 3 I/O oder 4 I/O; die Kontakte NC, C und NO des Relais schalten das Gerät.

- R Relais („Relay“)

3.5 Anschluss des Torantriebs

Führen Sie den Anschluss in jedem Fall im spannungsfreien Zustand durch. Die Klemmen der Steuereinheit des Torantriebs und ihre Nennspannung sind in der Dokumentation des Torantriebs beschrieben – die Zeichnung zeigt nur die typische Anordnung.

Das Tor wird über die (Steuer-)Klemmen **IN** und **COM** des Torantriebs geöffnet: Hierher kommen die Kontakte **C** und **NO** des GATOR-Relais, der Impuls des Relais bewirkt dasselbe wie die Taste der Fernbedienung. Die meisten Torantriebe haben einen **Torzustandsausgang** (OUT), der anzeigt, ob das Tor offen oder geschlossen ist; das kann ein Spannungsausgang oder ein Relaisausgang sein. In der Zeichnung ist das Hilfsrelais K1 an einen Torantrieb mit Spannungsausgang angeschlossen: Bei offenem Tor liegen zwischen den Klemmen OUT und N des Torantriebs ~230 V an, das Relais K1 zieht an und aktiviert den Eingang **1 IN** des

GATOR. So folgt der Zustand von 1 IN genau der Stellung des Tors, die auch Protegus 2 und das Symbol des Widgets anzeigen – die zugehörige Einstellung steht in Abschnitt 5.10. Bei einem Torantrieb mit Relaisausgang entfällt K1, der Zustandskontakt kann direkt zwischen 1 IN und COM angeschlossen werden.

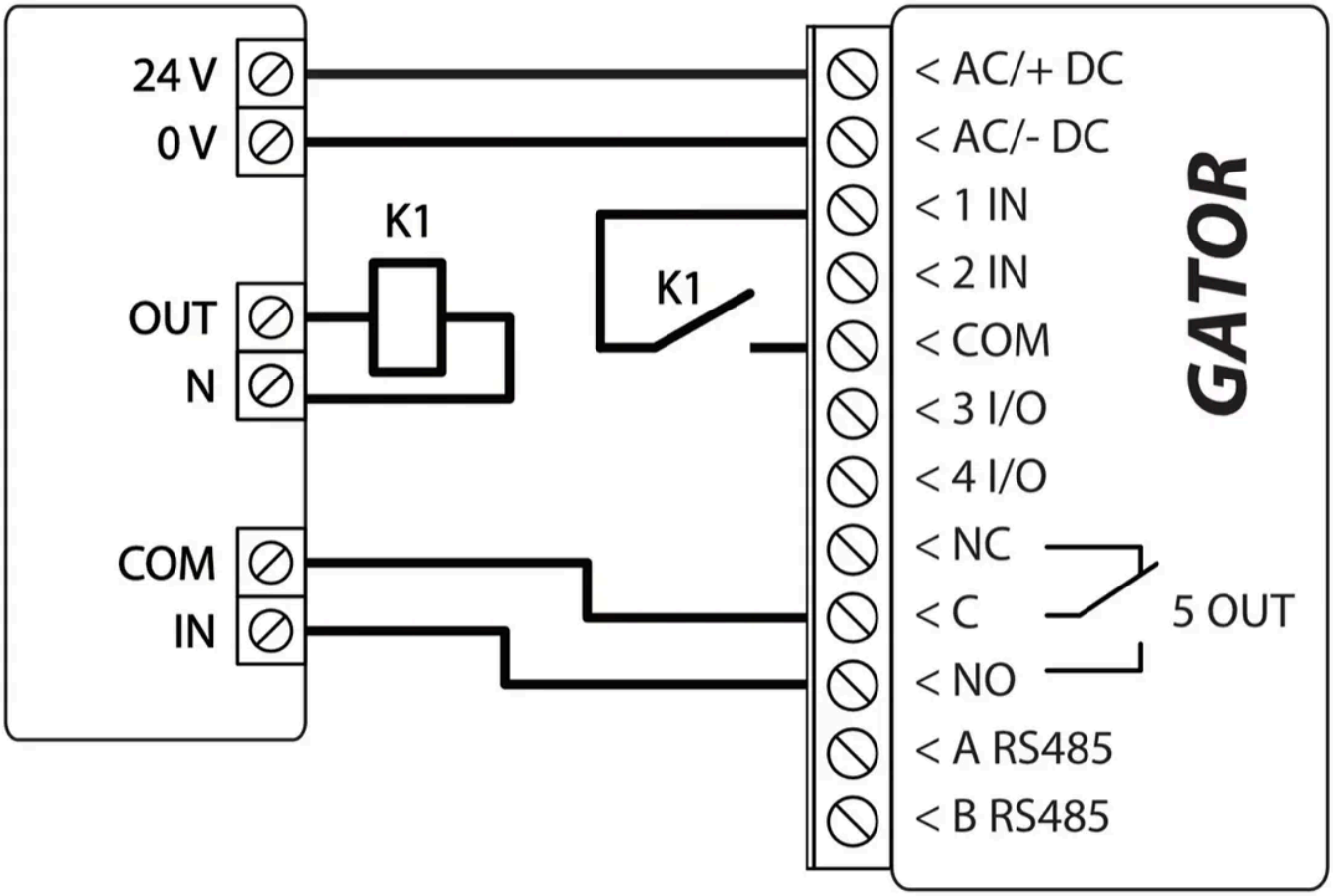


Abbildung 8. Verbindung der Steuereinheit des Torantriebs („Gate control unit“) mit dem GATOR über das Hilfsrelais K1. Stromversorgung („Power“): der 24-V-Versorgungsausgang des Torantriebs an die Klemme AC/+DC des GATOR, 0 V an AC/−DC; Torzustand („Gate status“): die Klemmen OUT und N des Torantriebs an die Spule des Relais K1, der Kontakt von K1 zwischen den Klemmen 1 IN und COM des GATOR; Torsteuerung („Gate control“): die Klemme COM des Torantriebs an den Kontakt C von 5 OUT des GATOR, die Klemme IN an den Kontakt NO von 5 OUT.

3.6 Anschluss eines RFID-Lesers (Wiegand 26/34)

Der GATOR nimmt einen oder zwei RFID-Leser mit **Wiegand-26/34**-Protokoll auf (Kartenleser und Leser mit Codetastatur). Der Leser schaltet mit den in der Benutzerliste angelegten Karten und Codes den Ausgang **5 OUT** (Berechtigung, Zeitplan und Zähler je Benutzer gelten auch für den Leser). Der Leser wird in TrikdisConfig auf der Seite **IN/OUT** eingestellt (Abschnitt 5.3), die Karten werden auf der Seite **User list** angelegt (Abschnitt 5.6); die Farbcodierung der Adern folgt dem Wiegand-Standard: rot +U, schwarz GND, grün D0, weiß D1.

Ein Leser: D0 geht an die Klemme **1 IN**, D1 an **2 IN**, der Ausgangstaster zwischen **COM** und **3 I/O**. In der Software muss **Wiegand reader mode** auf **Single Reader** stehen, und wenn ein Ausgangstaster vorhanden ist, setzen Sie das Häkchen bei **IO3 as exit button (5 OUT)**: Beim Drücken des Tasters schaltet 5 OUT für die eingestellte Impulsdauer ein. Ohne Taster bleibt das Kästchen leer.

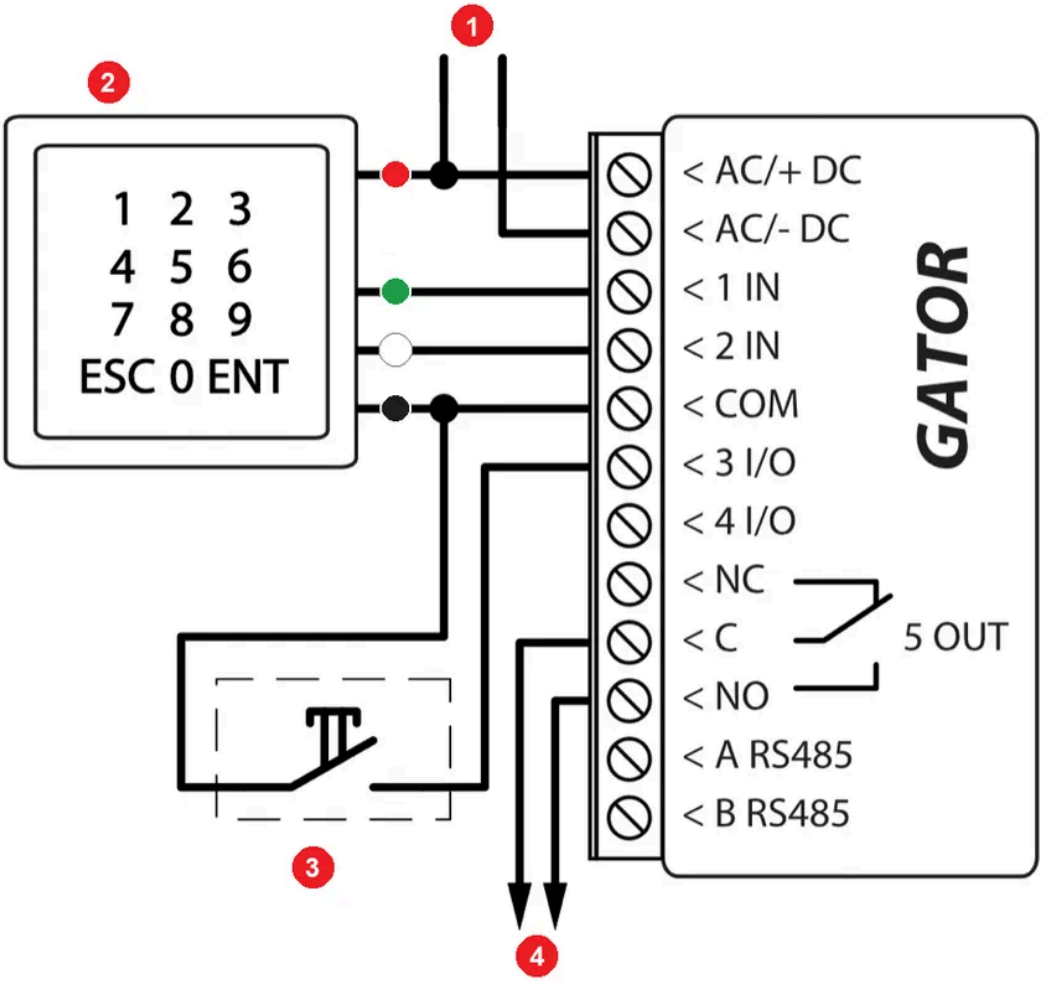


Abbildung 9. Anschluss eines Wiegand-26/34-Lesers und eines Ausgangstasters: Gleichspannungsversorgung, 9–16 V, 0,5 A, an die Klemmen AC/+DC und AC/−DC; beim Eingangsleser die rote Ader (+U) an AC/+DC, die grüne (D0) an 1 IN, die weiße (D1) an 2 IN, die schwarze (GND) an COM; der Ausgangstaster zwischen den Klemmen COM und 3 I/O; der Torantrieb an den Kontakten C und NO des Relais (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 Gleichspannungsnetzteil („DC power supply“), 9–16 V, 0,5 A
- 2 Eingangsleser („Entry reader“) – RFID-Leser mit Tastatur, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)“)
- 3 Ausgangstaster („»Exit« button“)
- 4 Torsteuerung („Gate control“) – der Steuereingang des Torantriebs; Belastbarkeit des Relais 1 A / 30 V DC, 0,5 A / 125 V AC
- rote Ader, +U („R - red (+U)“)
- schwarze Ader, GND („B - black (GND)“)
- weiße Ader, D1 („W - white (D1)“)
- grüne Ader, D0 („G - green (D0)“)

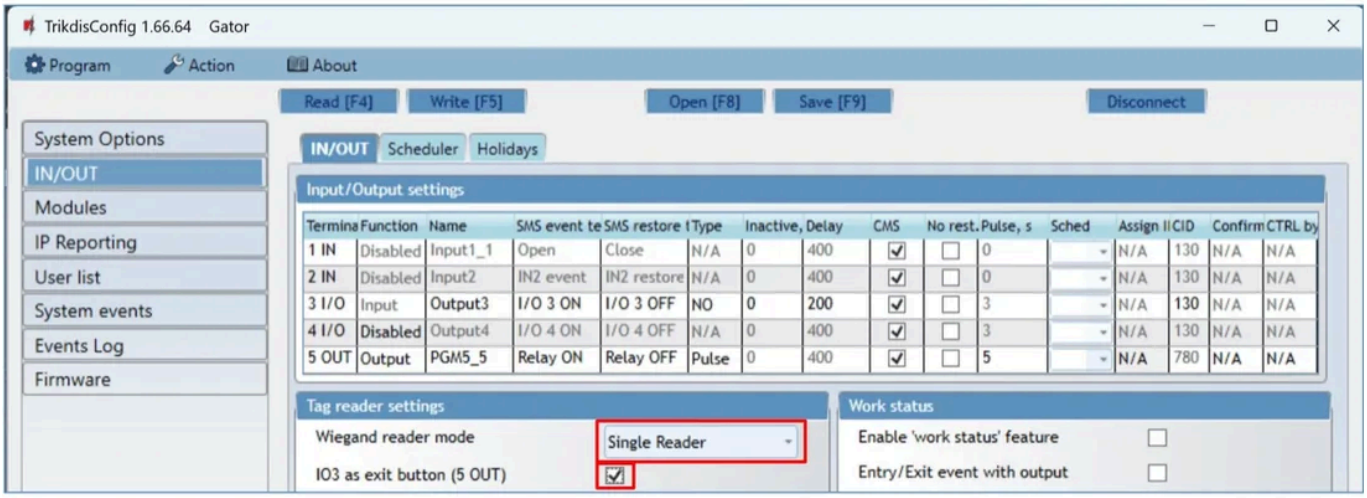


Abbildung 10. TrikdisConfig – IN/OUT, **Tag reader settings**: bei einem Leser **Wiegand reader mode = Single Reader**, mit Ausgangstaster **IO3 as exit button (5 OUT)** angehakt.

Zwei Leser (Eingang und Ausgang): Die Adern D0 / D1 des ersten Lesers gehen an die Klemmen **1 IN** / **2 IN**, die des zweiten an **3 I/O** / **4 I/O**; in der Software **Wiegand reader mode = Dual Reader**. Bei zwei Lesern ist 3 I/O belegt, ein Ausgangstaster kann dort nicht angeschlossen werden.

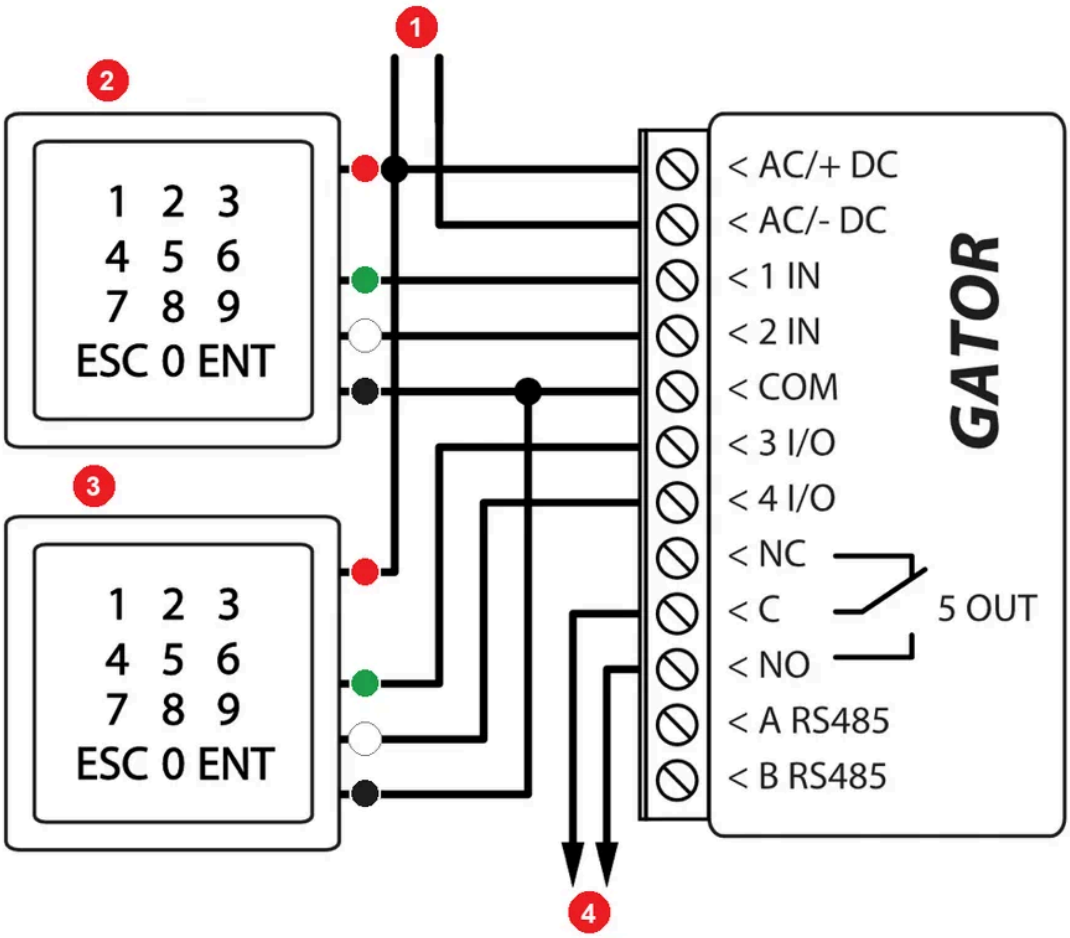


Abbildung 11. Anschluss von zwei Wiegand-26/34-Lesern, beide RFID-Leser mit Tastatur („RFID reader with keypad (Wiegand 26/34)“): Gleichspannungsversorgung, 9–16 V, 0,5 A; beim Eingangsleser die grüne Ader (D0) an 1 IN, die weiße (D1) an 2 IN; beim Ausgangsleser die grüne Ader (D0) an 3 I/O, die weiße (D1) an 4 I/O; bei beiden Lesern die rote Ader (+U) an AC/+DC, die schwarze (GND) an COM; der Torantrieb an den Kontakten C und NO des Relais (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 Gleichspannungsnetzteil („DC power supply“), 9–16 V, 0,5 A
- 2 Eingangsleser („Entry reader“)
- 3 Ausgangsleser („Exit reader“)
- 4 Torsteuerung („Gate control“) – der Steuereingang des Torantriebs; Belastbarkeit des Relais 1 A / 30 V DC, 0,5 A / 125 V AC
- rote Ader, +U („R - red (+U)“)
- schwarze Ader, GND („B - black (GND)“)
- weiße Ader, D1 („W - white (D1)“)
- grüne Ader, D0 („G - green (D0)“)

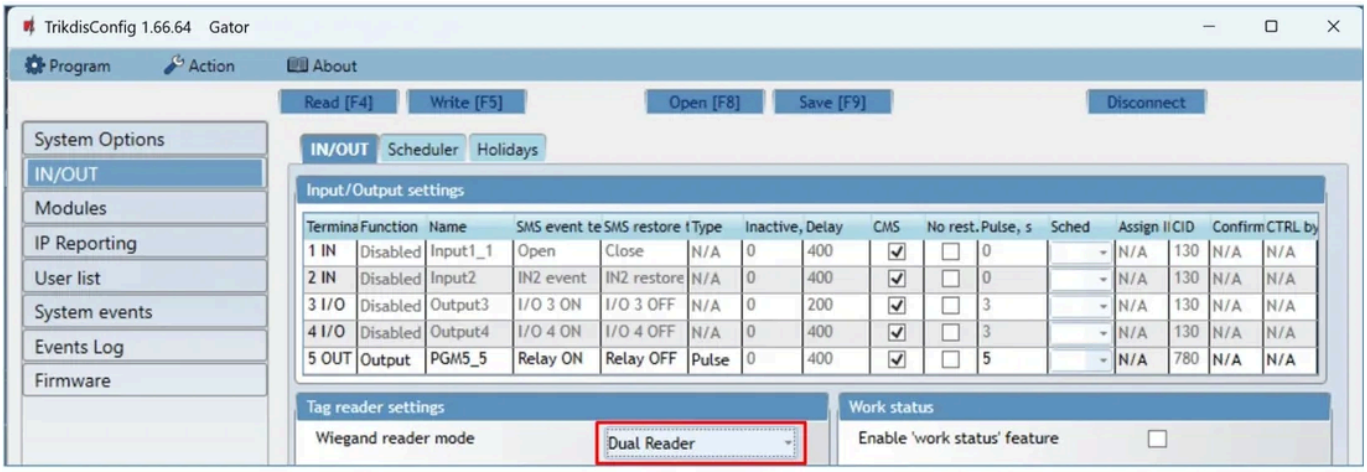


Abbildung 12. TrikdisConfig – IN/OUT, **Tag reader settings**: bei zwei Lesern **Wiegand reader mode = Dual Reader**.

Hat der Leser einen 5-V-Ausgang (Niederspannung), setzen Sie das Häkchen bei **Low voltage reader**; liefert der Leser sehr kurze Impulse und wird die Karte nicht erkannt, schalten Sie mit dem Kästchen **Disable reader filter** den internen Filter aus (Abschnitt 5.3).

3.7 WLAN-Modul W485

Das Modul **W485** sendet die Nachrichten des GATOR über das lokale WLAN und den Internet-Router an die Leitstelle und an die App Protegus 2, sodass keine mobilen Daten verbraucht werden. Fällt das WLAN aus, wechselt das Gerät von selbst ins Mobilfunknetz und kehrt nach der Rückkehr des WLAN wieder zum W485 zurück. Die Funktion ist ab GATOR-Firmware **1.06** verfügbar. Das Modul wird an den **RS485**-Bus angeschlossen (A–A, B–B), mit Alarmkabel auf **bis zu 100 m** Entfernung, und wird aus der gemeinsamen 10–28-V-DC-Versorgung mit dem GATOR betrieben. **Mit dem W485 kann der GATOR auch ohne SIM-Karte verwendet werden** – dann lässt er sich nur aus der App steuern, Anruf und SMS gibt es nicht. Die Einstellung des Moduls steht in Abschnitt 5.4.

Trikdis W485 WiFi -Modul (RS485)

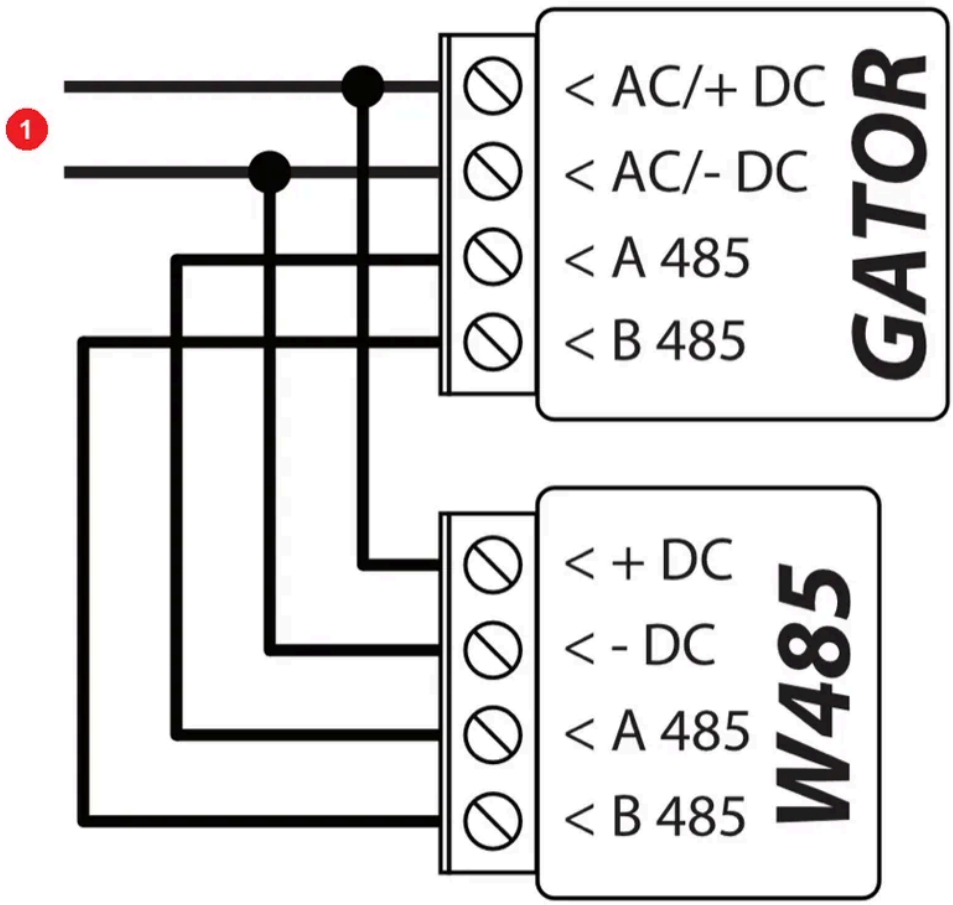


Abbildung 13. Anschluss des Moduls W485: der Pluspol des Netzteils 10–28 V DC, 0,5 A an die Klemme AC/+DC des GATOR und +DC des W485, der Minuspol an AC/−DC und −DC; RS485-Verbindung („RS485 connection"), bis zu 100 m („up to 100m"): A 485 – A 485, B 485 – B 485.

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

Die Entfernungsangaben „bis … m" sind theoretische Höchstwerte, die unter idealen Bedingungen erreichbar sind. In der Praxis ergeben Qualität und Verlegung des Kabels, Störquellen und bei Funkverbindungen Wände und Gelände eine deutlich geringere Reichweite. Planen Sie mit Reserve, und prüfen Sie bei langen Strecken die Verbindung bei der Inbetriebnahme.

3.8 Ethernet-Modul E485

Das Modul **E485** leistet dasselbe über kabelgebundenes Internet: Die Nachrichten des GATOR gehen über das am Router eingesteckte Ethernet-Kabel an die Leitstelle und an die App Protegus 2, das mobile Internet nutzt das Gerät nicht, das Mobilfunknetz dient nur als Ersatzweg: Fällt das kabelgebundene Internet aus, sendet es die Nachrichten über das mobile Internet und nach der Rückkehr der kabelgebundenen Verbindung wieder über das E485. Ab Firmware **1.06**; RS485-Bus bis zu 100 m; gemeinsame 10–28-V-DC-Versorgung; auch ohne SIM-Karte verwendbar. Einstellung in Abschnitt 5.4.

Trikdis E485 Ethernet -Modul (RS485)

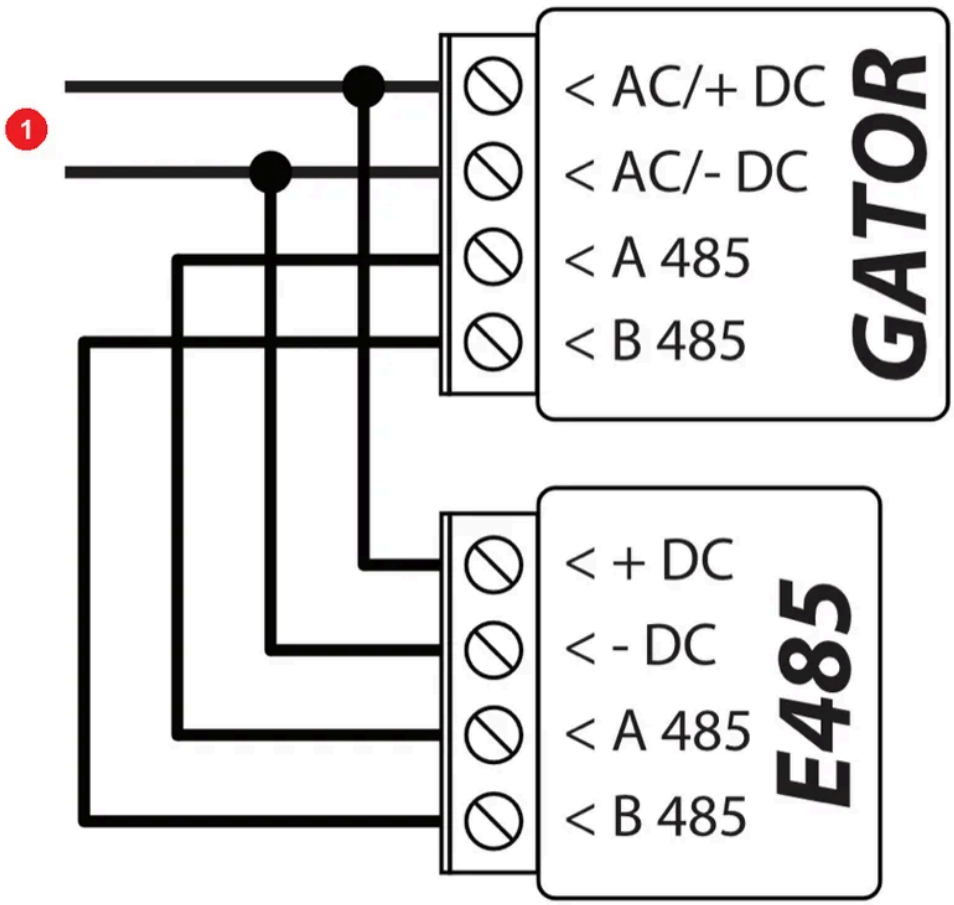


Abbildung 14. Anschluss des Moduls E485: der Pluspol des Netzteils 10–28 V DC, 0,5 A an die Klemme AC/+DC des GATOR und +DC des E485, der Minuspol an AC/−DC und −DC; RS485-Verbindung („RS485 connection“), bis zu 100 m („up to 100m“): A 485 – A 485, B 485 – B 485.

- 1 Netzteil („Power supply“), 10–28 V DC, 0,5 A

Die Entfernungsangaben „bis … m“ sind theoretische Höchstwerte, die unter idealen Bedingungen erreichbar sind. In der Praxis ergeben Qualität und Verlegung des Kabels, Störquellen und bei Funkverbindungen Wände und Gelände eine deutlich geringere Reichweite. Planen Sie mit Reserve, und prüfen Sie bei langen Strecken die Verbindung bei der Inbetriebnahme.

3.9 RF-LORA und iO-LORA Erweiterungen mit RFID-Leser

Ab GATOR-Firmware **2.13** lässt sich das System drahtlos erweitern: Der Sende-Empfänger **RF-LORA** wird an den RS485-Bus angeschlossen und hält per Funk die Verbindung zu bis zu **8 iO-LORA** Erweiterungen (im Freien bis zu 5000 m). Jede iO-LORA Erweiterung ergänzt den GATOR um einen Eingang und einen Relaisausgang, und an jede kann ein eigener Wiegand-26/34-RFID-Leser angeschlossen werden: Der Leser schaltet **nur den Relaisausgang seiner eigenen Erweiterung**, keinen entfernten Ausgang. So lassen sich mit einem GATOR bis zu 8 weit voneinander entfernte Tore oder Schranken steuern, jedes mit eigenem Kartenleser und Ausgangstaster – Details zur Lösung: Flexible drahtlose Zutrittskontrolle mit dem GATOR RF-LoRa-System.

Trikdis RF-Lora Wireless Expander-Modul | **Trikdis io-lora Wireless Expander-Modul**

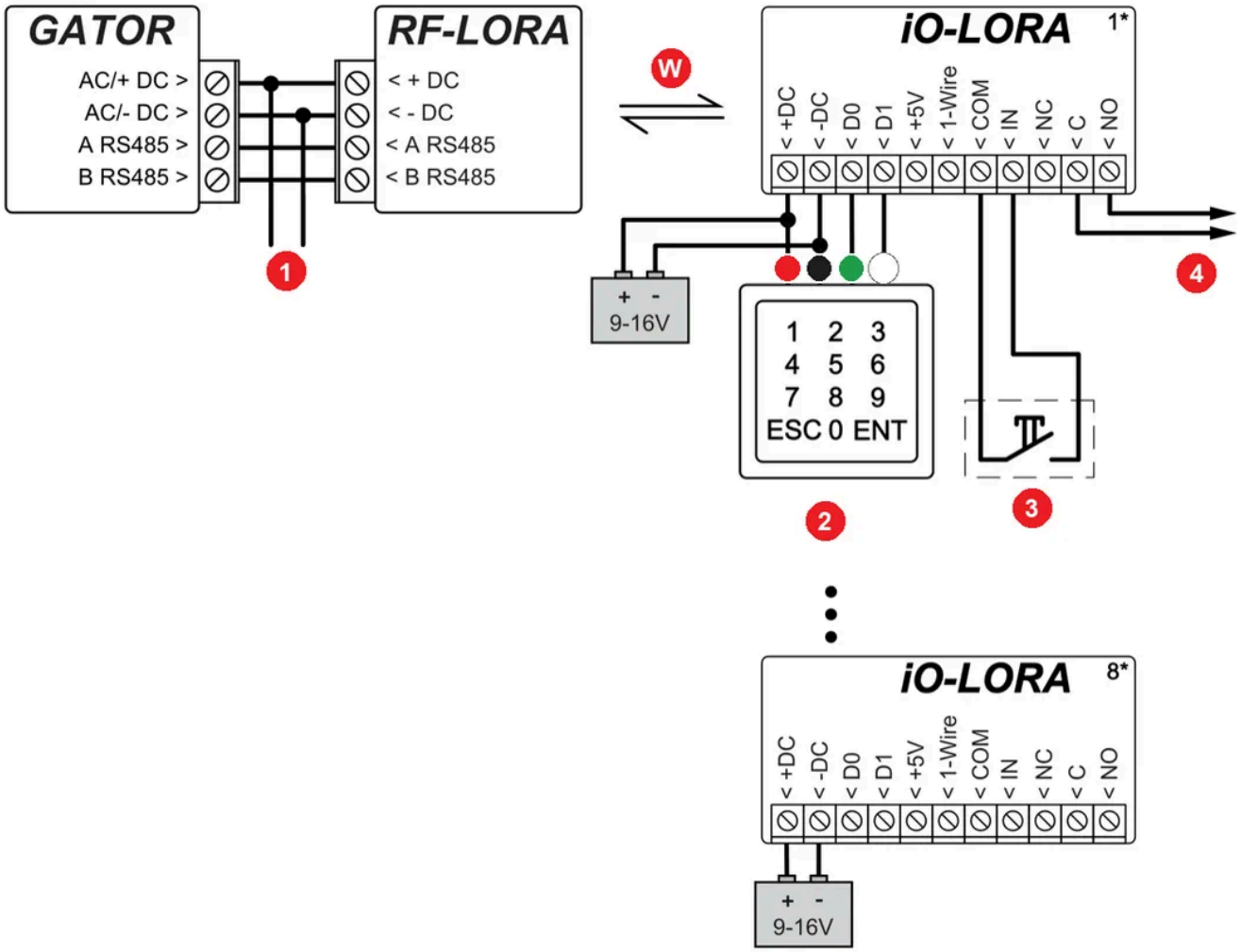


Abbildung 15. Sende-Empfänger RF-LORA am GATOR und iO-LORA Erweiterungen mit RFID-Leser: gemeinsame Versorgung 9–16 V DC, 0,5 A für GATOR und RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A–A, B–B; Funkverbindung zwischen RF-LORA und den Erweiterungen iO-LORA 1…8, bis zu 5000 m; jede iO-LORA erhält eine eigene Versorgung 9–16 V; der Leser an der iO-LORA: rot (+U) an +DC, schwarz (GND) an −DC, grün an D0, weiß an D1; Ausgangstaster zwischen den Klemmen COM und IN der iO-LORA; der Torantrieb an den Kontakten C und NO des Relais der iO-LORA (2 A / 230 V AC).

- 1 Gleichspannungsnetzteil („DC power supply“), 9–16 V, 0,5 A
- W drahtlose Verbindung („Wireless connection“), bis zu 5000 m („up to 5000 m“)
- 2 RFID-Leser mit Tastatur, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)“)
- 3 Ausgangstaster („»Exit« button“)
- 4 Torsteuerung („Gate control“) – der Steuereingang des Torantriebs; Belastbarkeit des Relais der iO-LORA 2 A / 230 V AC
- rote Ader, +U („R - red (+U)“)
- schwarze Ader, GND („B - black (GND)“)
- grüne Ader, D0 („G - green (D0)“)
- weiße Ader, D1 („W - white (D1)“)

Die Entfernungsangaben „bis … m“ sind theoretische Höchstwerte, die unter idealen Bedingungen erreichbar sind. In der Praxis ergeben Qualität und Verlegung des Kabels, Störquellen und bei Funkverbindungen Wände und Gelände eine deutlich geringere Reichweite. Planen Sie mit Reserve, und prüfen Sie bei langen Strecken die Verbindung bei der Inbetriebnahme.

Einstellung in TrikdisConfig (die Beschreibung der Fenster steht in Kapitel 5):

1. Starten Sie TrikdisConfig, verbinden Sie den GATOR mit einem USB-Mini-B-Kabel mit dem Computer oder melden Sie sich aus der Ferne an, und lesen Sie die Einstellungen aus (**Read [F4]** – die Software zeigt die aktuellen Einstellungen des Geräts). Wenn die Software danach fragt, geben Sie im eingeblendeten Fenster den 6-stelligen Administrator- oder Errichtercode ein. Wählen Sie auf der Seite

Modules in der Liste den Eintrag **iO-LORA controller** und geben Sie in das Feld **Serial No.** die sechsstellige Seriennummer der Erweiterung ein (auf dem Aufkleber der Erweiterung). Das RF-LORA muss nicht eigens angelegt werden.



Abbildung 16. TrikdisConfig – Modules: die iO-LORA Erweiterung ausgewählt, in das Feld **Serial No.** kommt die Seriennummer.

2. Für jede angelegte iO-LORA Erweiterung erscheinen in der Liste der Seite **IN/OUT** ein Eingang (zum Beispiel **6 IN iO-LORA 1**) und ein Ausgang (**7 OUT iO-LORA 1**). Die Funktion des Eingangs sollte **Exit button** sein (hier schließen die Klemmen IN und COM der Erweiterung den Ausgangstaster an): Beim Drücken schaltet das Relais der Erweiterung (im Beispiel **7 OUT**) für die eingestellte Impulsdauer ein. Der Typ des Ausgangs ist **Pulse**, die Impulsdauer entspricht dem Torantrieb (im Beispiel 3 s).

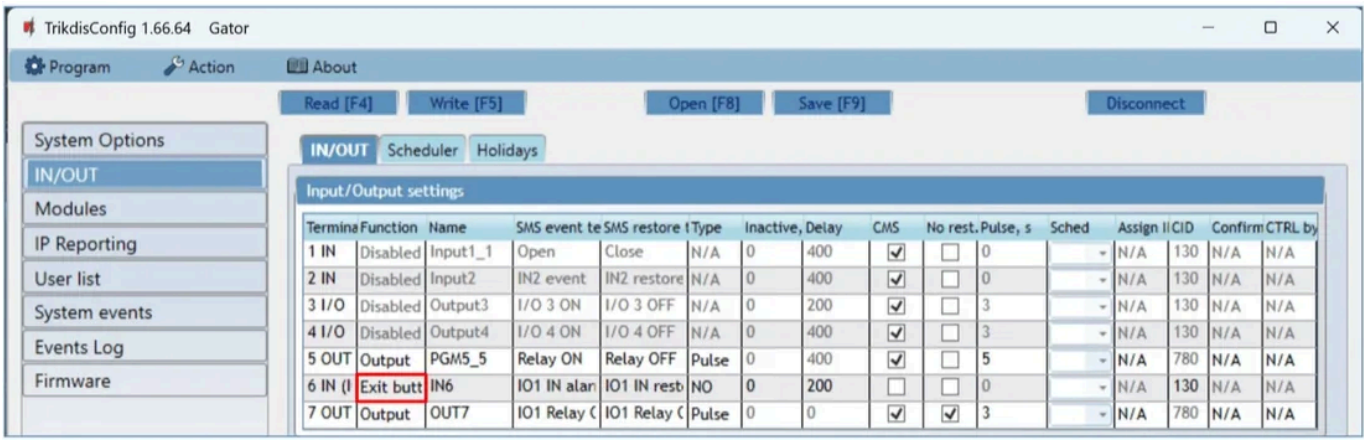


Abbildung 17. TrikdisConfig – IN/OUT: die Funktion von **6 IN** ist **Exit button**, der Ausgang **7 OUT** ist vom Typ **Pulse** mit 3 s Impuls.

3. Geben Sie auf der Seite **User list** den Namen des Benutzers und die Nummer der RFID-Karte (**Phone/RFID**) ein, bei einem Leser mit Codetastatur den Code, setzen Sie das Häkchen bei **En** und markieren Sie, welchen Ausgang er steuern darf (im Beispiel den 7.). Schreiben Sie die Einstellungen (**Write [F5]**), warten Sie das Ende der Aktualisierung ab, klicken Sie dann auf **Disconnect** und ziehen Sie das USB-Kabel ab.

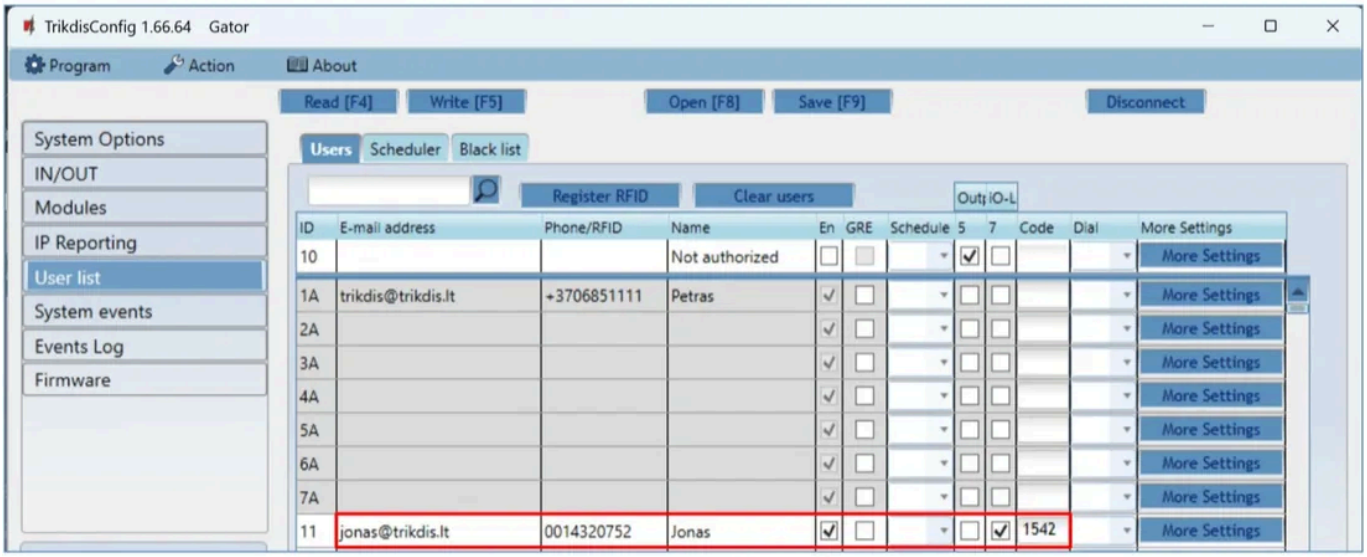


Abbildung 18. TrikdisConfig – User list: beim Benutzer RFID-Nummer, Name und Code ausgefüllt, **En** angehakt, der Ausgang 7 markiert.

4. **Prüfung:** Schalten Sie den Ausgang mit der Karte oder dem Code ein und drücken Sie danach den Ausgangstaster – das Relais muss beide Male für die eingestellte Impulsdauer anziehen.

3.10 Erweiterung iO8 und iO8-LORA

Wenn Sie an einer Stelle mehr Eingänge oder Ausgänge brauchen, lässt sich an den GATOR **eine** Erweiterung **iO8** (kabelgebunden, RS485) oder **iO8-LORA** (drahtlos, über das RF-LORA) anschließen. Die Ein- und Ausgänge der Erweiterung erscheinen in der Liste der Seite **IN/OUT** und lassen sich genauso verwenden wie die des GATOR selbst; das Modul muss auf der Seite **Modules** mit seiner Seriennummer angelegt werden (Abschnitt 5.4).

Trikdis IO8 Wired Expander Modul | **Trikdis io8-lora Wireless Expander-Modul**

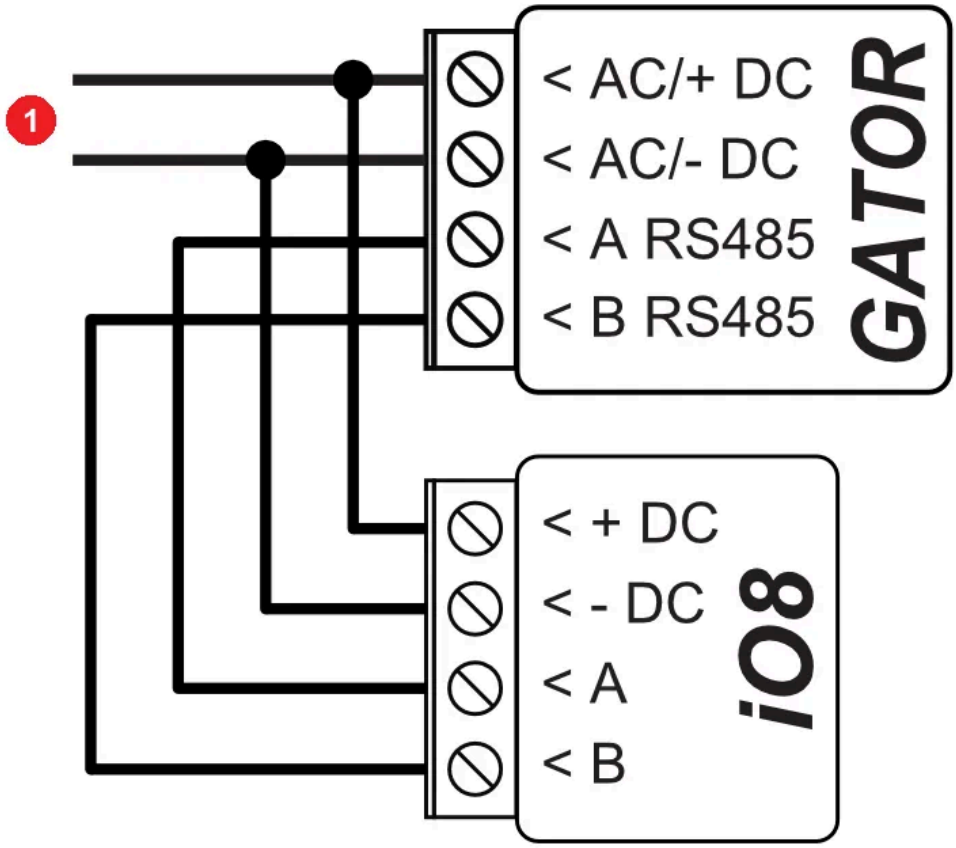


Abbildung 19. Anschluss der Erweiterung iO8: der Pluspol des Netzteils 10–28 V DC, 0,5 A an die Klemme AC/+DC des GATOR und +DC des iO8, der Minuspol an AC/−DC und −DC; RS485-Verbindung („RS485 connection"), bis zu 100 m („up to 100m"): die Klemme A RS485 des GATOR an A des iO8, B RS485 an B.

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

Der iO8 arbeitet mit 10–26 V DC: Liefert das Netzteil mehr als 26 V, erhält der iO8 ein eigenes Netzteil, wobei die Minuspole der beiden Netzteile miteinander verbunden werden.

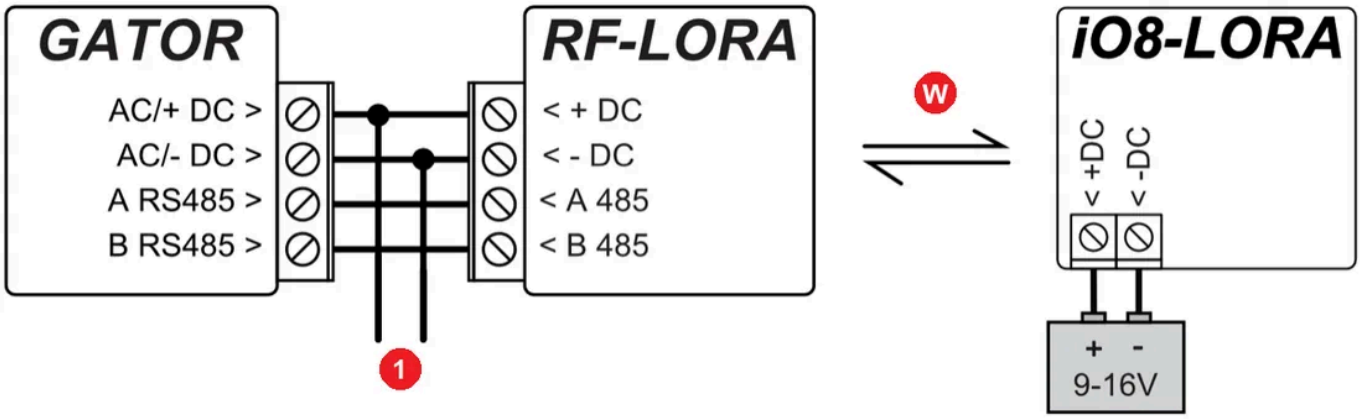


Abbildung 20. Die Erweiterung iO8-LORA über den Sende-Empfänger RF-LORA: Versorgung 9–16 V DC, 0,5 A für GATOR und RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A RS485 – A 485, B RS485 – B 485; Funkverbindung zwischen RF-LORA und iO8-LORA, bis zu 5000 m; der iO8-LORA erhält eine eigene Versorgung 9–16 V.

- 1 Gleichspannungsnetzteil („DC power supply"), 9–16 V, 0,5 A
- W drahtlose Verbindung („Wireless connection"), bis zu 5000 m („up to 5000 m")

Die Entfernungsangaben „bis … m" sind theoretische Höchstwerte, die unter idealen Bedingungen erreichbar sind. In der Praxis ergeben Qualität und Verlegung des Kabels, Störquellen und bei Funkverbindungen Wände und Gelände eine deutlich geringere Reichweite. Planen Sie mit Reserve, und

prüfen Sie bei langen Strecken die Verbindung bei der Inbetriebnahme.

4. Fernsteuerung

Den GATOR können Sie auf vier Arten steuern: per **Telefonanruf** (kostenlos, weil das Gerät den Anruf nicht annimmt), während des Anrufs mit der **Telefontastatur** (DTMF), aus der App **Protegus 2** oder mit einem **Widget** auf dem Startbildschirm des Telefons sowie per **SMS-Befehl**. Bei allen vier Arten entscheidet die Benutzerliste (Abschnitt 5.6), wer was tun darf; mit den SMS-Befehlen kann der Administrator auch die Einstellungen ändern.

4.1 Steuerung per Telefonanruf

Rufen Sie die Nummer der SIM-Karte im GATOR an. Das Gerät **weist den Anruf automatisch ab** und schaltet den Relaisausgang **5 OUT** für **3 Sekunden** ein – der Anruf kostet nichts. Ab Werk kann jeder das Gerät so steuern, der seine Nummer kennt.

- **Nur Berechtigte**: Wenn Sie auch nur eine einzige Nummer in die Benutzerliste aufnehmen (per SMS: `SETU …`, Abschnitt 4.7; in TrikdisConfig oder in der App), reagiert der GATOR nur noch auf Anrufe von Nummern auf der Liste. In TrikdisConfig schaltet dasselbe das Kästchen **En** des Eintrags Nr. 10 mit dem Namen **Not authorized** in der **User list** (Abschnitt 5.6): angehakt kann jeder anrufen, leer nur die Mitglieder der Liste.
- **Welcher Ausgang öffnet**: Darf ein Benutzer mehrere Ausgänge steuern, schalten beim Anruf die in der Spalte **Dial** markierten Ausgänge, danach beendet das Gerät den Anruf.
- **Dauer des Anrufs**: Beim Wert 0 unter **System Options** → **Hang-up after** weist das Gerät den Anruf sofort ab; bei einem größeren Wert nimmt es ihn an und beendet ihn nach der angegebenen Zeit – das ist für die Steuerung per Tastatur nötig (Abschnitt 4.2).

Wer den GATOR im Werkszustand **als Erster** anruft oder ihm als Erster eine SMS sendet, wird **Administrator** des Geräts: Von da an kann nur er ihn mit SMS-Befehlen bedienen. Starten Sie den ersten Anruf deshalb vom Telefon des Eigentümers oder des Errichters.

4.2 Steuerung mit der Telefontastatur (DTMF)

Wenn der GATOR den Anruf annimmt (**Hang-up after** größer als 0), kann der Benutzer mit der Telefontastatur mehrere Ausgänge schalten:

1. Rufen Sie die Nummer der SIM-Karte des GATOR an – das Gerät nimmt den Anruf an.
2. Geben Sie den Steuerbefehl gemäß der Tabelle auf der Telefontastatur ein.

DTMF-Code	Funktion	Beschreibung
`AUSGANG*ZUSTAND#`	Steuerung eines Ausgangs	**AUSGANG** – die Nummer des Ausgangs. **ZUSTAND** – 0: ausschalten; 1: einschalten; 2: für die Impulsdauer ausschalten; 3: für die Impulsdauer einschalten (die Impulsdauer lässt sich in der Tabelle **IN/OUT** von TrikdisConfig einstellen). **#** – Ende des Befehls. Beispiel – Ausgang 5 einschalten: `5*1#`; Ausgang 4 für die Impulsdauer einschalten: `4*3#`
`#`	Ende des Befehls	wenn Sie sich beim Befehl vertippt haben, drücken Sie die Taste **#** und geben Sie ihn erneut ein

Die Steuerung per Tastatur (DTMF) funktioniert bei Geräten mit dem Typcode **GV17_2E70** und **GV17_2S70** nicht. Den genauen Typ sehen Sie in der Statusleiste von TrikdisConfig (Abschnitt 5.1).

4.3 Steuerung aus der App Protegus 2

In Protegus 2 öffnet der Benutzer das Tor von überall, sieht den Zustand des Systems und den Zustand des Tors (wenn der Torzustand angeschlossen ist, Abschnitte 3.5 und 5.10), erhält alle Systemereignisse als Push-Nachricht und verwaltet als Administrator auch die Benutzer. Die App ist kostenlos; auf das Telefon laden Sie sie aus den App-Stores, im Browser öffnet sie sich unter https://web.protegus.app.

Bevor Sie das System hinzufügen

In TrikdisConfig muss auf der Seite **IP Reporting** das Kästchen **Enable cloud service** angehakt sein (Abschnitt 5.5; per SMS: `CONNECT 123456 PROTEGUS=ON`), die Versorgung muss in Ordnung sein (die LED **POWER** blinkt grün), und das Gerät muss im Netz sein (die LED **NETWORK** leuchtet grün und blinkt gelb). Die SIM-Karte braucht einen mobilen Datendienst, oder es muss ein W485 / E485 Modul vorhanden sein.

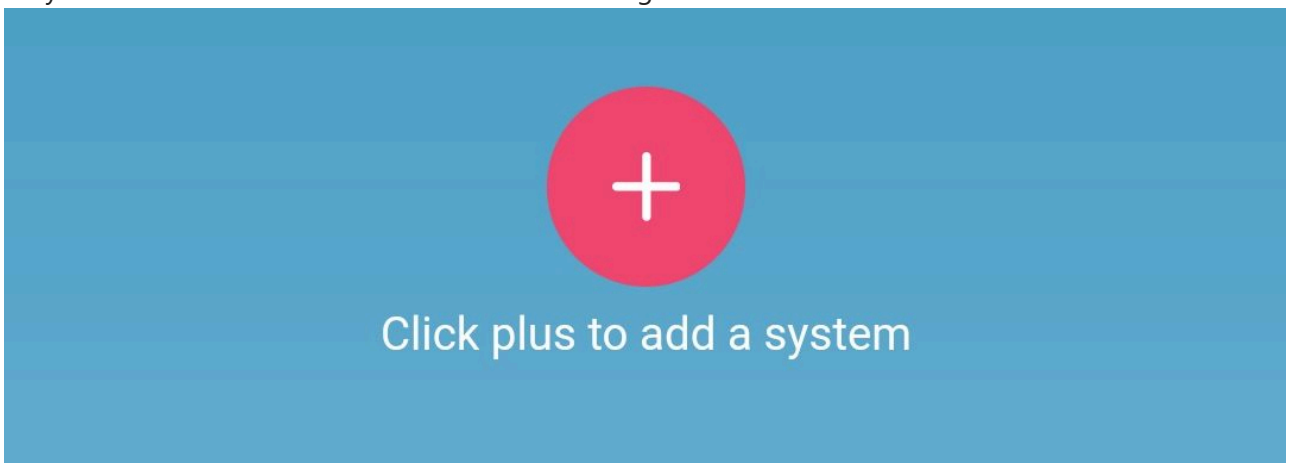
Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



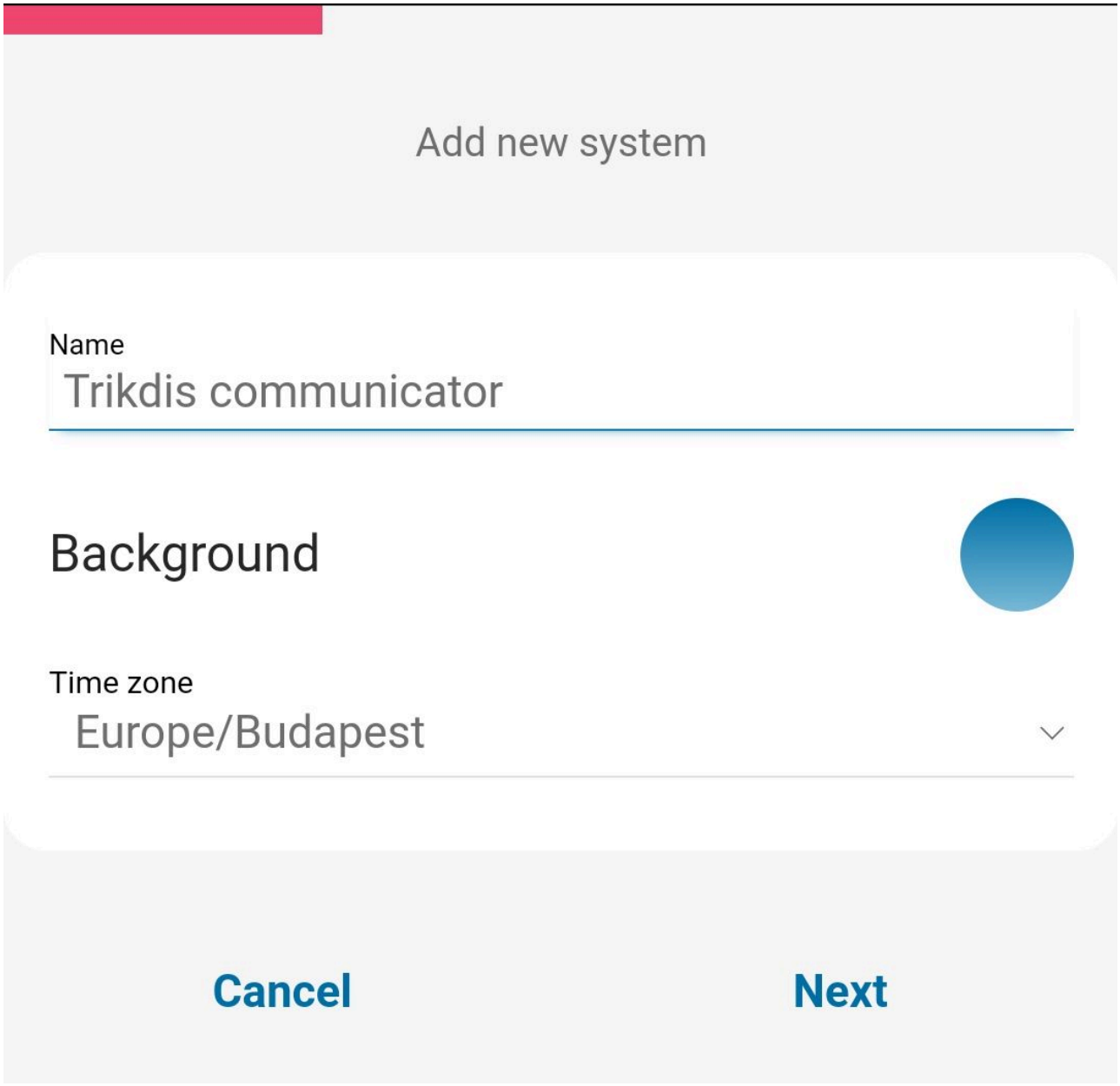
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



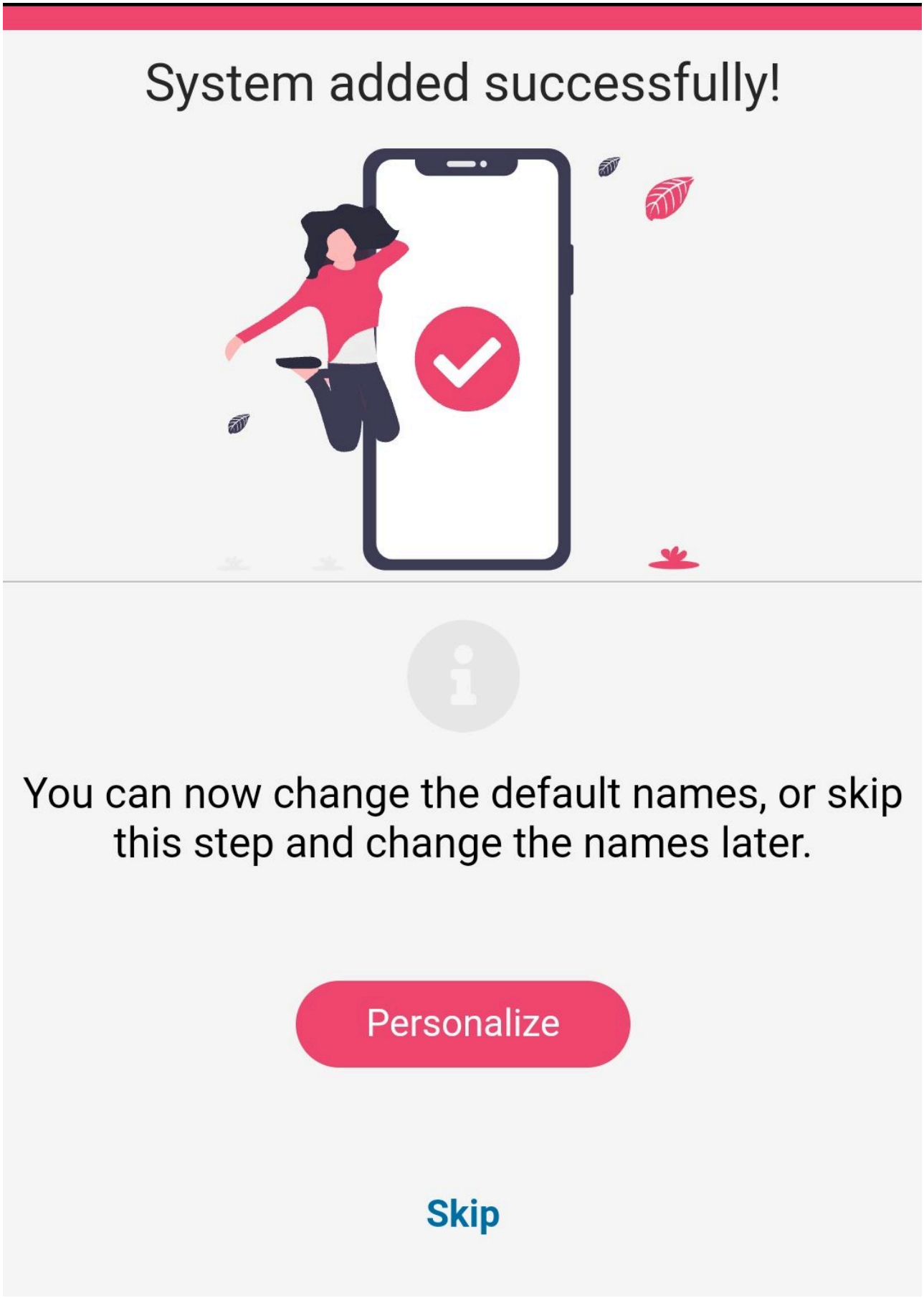
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



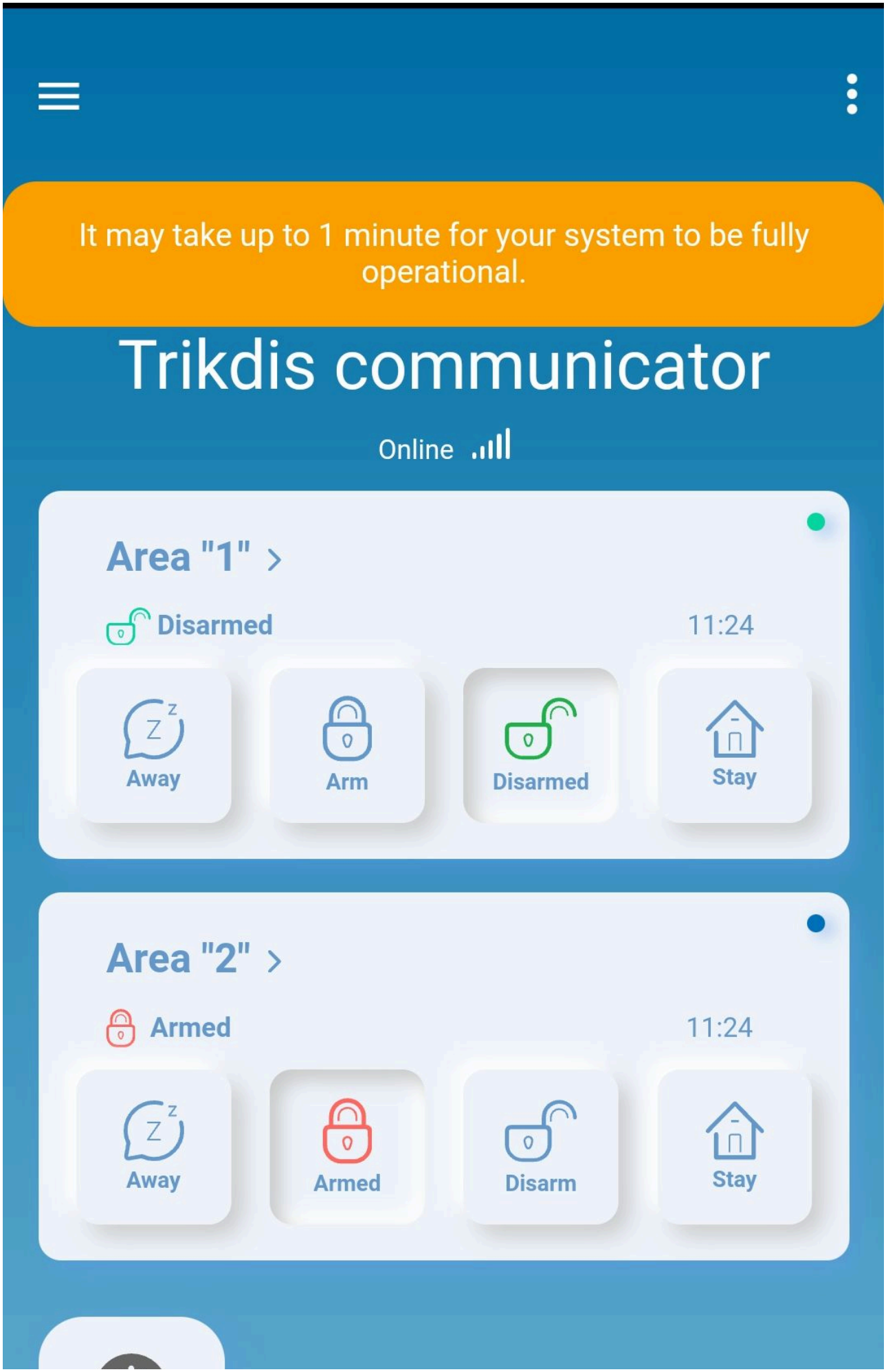
6. Add meg a rendszer nevét és válassz idozónát



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



Beim GATOR achten Sie beim Hinzufügen auf Folgendes:

1. Die eindeutige Kennung ist die **IMEI**-Nummer des GATOR: Sie steht auf dem Aufkleber an der Unterseite des Geräts und auf dem Karton, und Sie sehen sie auch in der Statusleiste von TrikdisConfig; den QR-Code des Aufklebers können Sie auch mit der Kamera des Telefons einlesen. Hat der Errichter den werkseitigen Wert `123456` des **Cloud Access Code** geändert, fragt die App auch danach.
2. Nach der Eingabe des Systemnamens können Sie den Schritt **Personalize** mit der Taste **Skip** überspringen: Die Namen der Ausgänge und Eingänge können Sie auch später ändern.
3. Warten Sie, bis der Hinweis mit gelbem Hintergrund verschwindet – das System ist innerhalb von höchstens 1 Minute einsatzbereit.

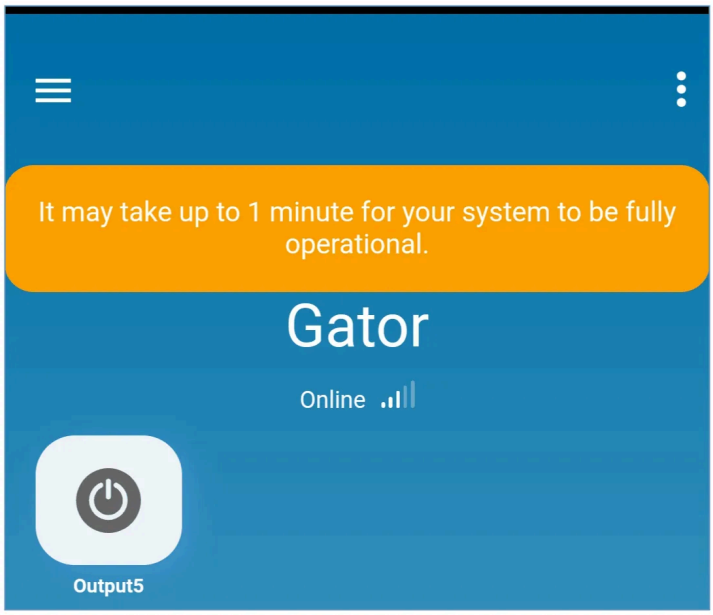


Abbildung 21. Der GATOR in Protegus 2 nach dem Hinzufügen: das System ist **Online**, der gelbe Balken zeigt, dass bis zur vollen Funktion höchstens 1 Minute zu warten ist.

4. Das Tor öffnen Sie mit der Taste **Output5**. **Tipp:** Halten Sie die Taste gedrückt, wählen Sie Bearbeiten, tippen Sie dann auf das Symbol, wählen Sie ein zur Verwendung passendes Symbol (Tor, Schranke, Garage) und speichern Sie. Wenn der Torzustand angeschlossen ist, zeigt das Symbol auch den offenen und den geschlossenen Zustand des Tors.

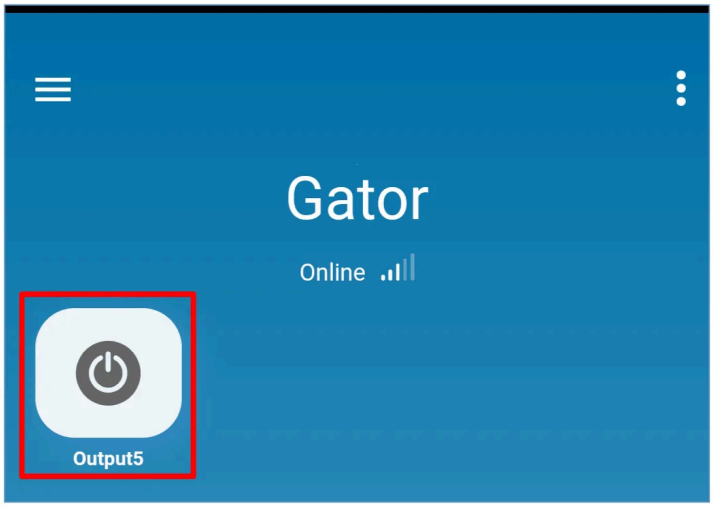


Abbildung 22. Der Startbildschirm des Systems mit der Taste **Output5** – sie schaltet das Relais des GATOR.

Siehe auch

Das Torautomatisierungsgerät GV17 kann mit Protegus 2 verwendet werden · Protegus: Android-, iPhone- und Web-App · Push-Benachrichtigung im Browser in der App Protegus 2

4.4 Widget auf dem Startbildschirm des Telefons

Die Taste zum Öffnen des Tors können Sie auch auf den Startbildschirm des Telefons legen, so öffnen Sie mit einer Berührung, ohne die App zu öffnen. Das funktioniert **nur unter Android**; wie ein Widget platziert wird, kann von Telefon zu Telefon etwas abweichen. Der GATOR muss zu Protegus 2 hinzugefügt sein, und Sie müssen in der App angemeldet sein; schließen Sie danach das App-Fenster.

1. Berühren Sie lange eine leere Stelle des Startbildschirms und wählen Sie in der erscheinenden Leiste den Eintrag **Widgets**.
2. Suchen Sie in der Liste **Protegus 2** und wählen Sie das Widget **Switch Protegus 2**.
3. Wählen Sie den zu steuernden Ausgang (zum Beispiel **Gator Output5**) und drücken Sie die Taste **ADD WIDGET**.
4. Die Taste erscheint auf dem Startbildschirm. Probieren Sie sie aus: Kehren Sie zum Startbildschirm zurück und drücken Sie die Taste – nach dem Drücken zeigt eine kreisförmige Rückmeldung, dass der Ausgang eingeschaltet hat; bei angeschlossenem Torzustand zeigt die Farbe der Taste den offenen und den geschlossenen Zustand des Tors.



Abbildung 23. Schritt 1 – nach langem Berühren des Startbildschirms der Menüpunkt **Widgets**.

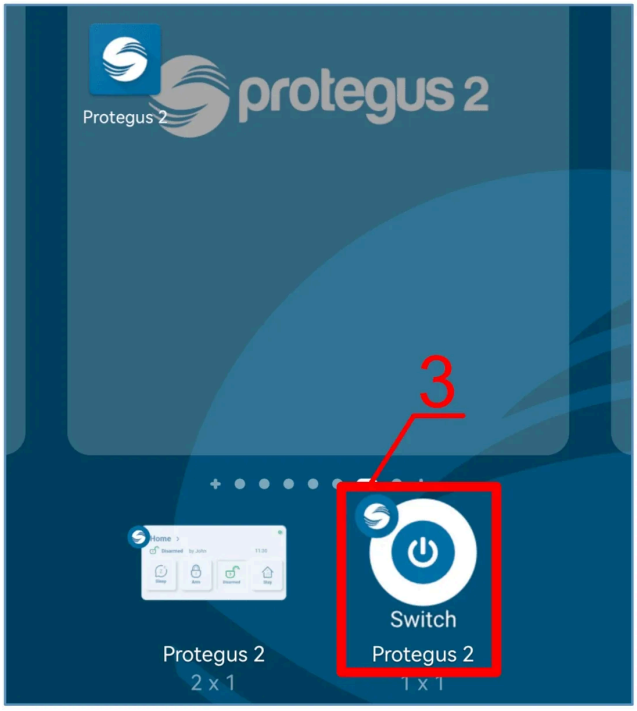


Abbildung 24. Schritt 2 – unter den Widgets von Protegus 2 das Widget **Switch Protegus 2**.



Abbildung 25. Schritt 3 – Auswahl des Ausgangs **Gator Output5** und die Taste **ADD WIDGET**.



Abbildung 26. Schritt 4 – das Widget **Output5** auf dem Startbildschirm; die grüne Taste zeigt den eingeschalteten Ausgang (offenes Tor).

4.5 Benutzerverwaltung in der App

Als Administrator können Sie auch in Protegus 2 Benutzer anlegen und löschen; der angelegte Benutzer sieht und öffnet das Tor aus seinem eigenen Konto und kann auch per SMS benachrichtigt werden (wenn die Begrüßungsnachricht **HELLO** eingeschaltet ist, erhält er über das Hinzufügen eine SMS).

1. Starten Sie die App Protegus 2 auf Ihrem Telefon und melden Sie sich mit Ihrem Benutzernamen und Passwort an. Öffnen Sie auf dem Bildschirm des Systems das Menü **Settings** (Einstellungen) und dann den Punkt **System configuration**.
2. Wählen Sie die Liste **Users** (Benutzer) und drücken Sie die Taste **+** (**Add new user** – neuer Benutzer).
3. Geben Sie die **E-Mail-Adresse**, den **Namen** und die **Telefonnummer** des Benutzers ein (oder die Nummer der RFID-Karte, Abschnitt 5.6), bei einem Leser mit Codetastatur seinen 4-stelligen **Code**, und markieren Sie, welchen Ausgang er steuern darf (**Output5**).
4. Drücken Sie die Taste **Add user** (Benutzer hinzufügen): Der neue Benutzer erscheint in der Liste. Mit der Taste **Back** kehren Sie zum Hauptfenster zurück.

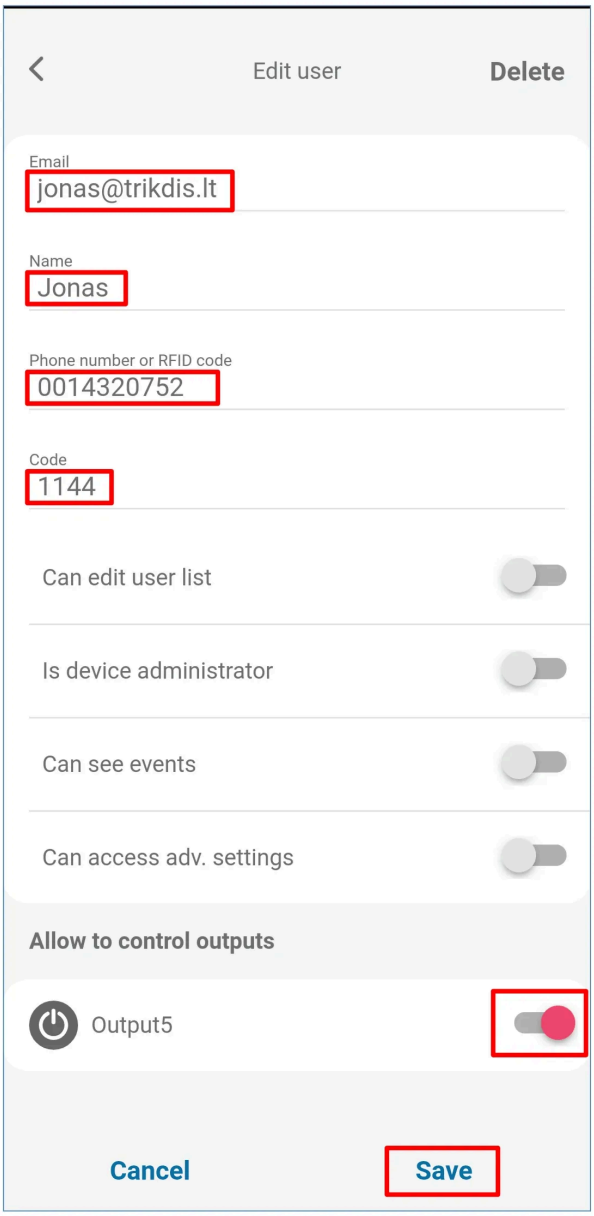


Abbildung 27. Bearbeiten eines Benutzers in Protegus 2: E-Mail-Adresse, Name, Telefonnummer oder RFID-Kartennummer, Code und die Freigabe zur Steuerung von **Output5**.

4.6 Steuerung per SMS-Nachricht

Den Relaisausgang (**OUTPUT5**) schalten Sie mit diesen SMS-Befehlen; `xxxxxx` ist das 6-stellige Administratorpasswort (werkseitig `123456`). Auch andere Ausgänge können Sie per SMS schalten, diese müssen aber vorher in TrikdisConfig als Ausgang eingestellt werden (Abschnitt 5.3).

Befehl	Parameter	Beschreibung
`OUTPUTx xxxxxx ON`	ON	Einschalten des Ausgangs; **x** ist die Nummer des Ausgangs. Beispiel: `OUTPUT5 123456 ON`
`OUTPUTx xxxxxx OFF`	OFF	Ausschalten des Ausgangs. Beispiel: `OUTPUT5 123456 OFF`
`OUTPUTx xxxxxx PULSE=ttt`	PULSE=ttt	Einschalten des Ausgangs für **ttt** Sekunden (1–999, mit drei Ziffern). Beispiel: `OUTPUT5 123456 PULSE=002`

4.7 Programmierung per SMS

SMS-Befehle nimmt das Gerät nur von den **Administrator**-Nummern (1A–7A) an; jeder Befehl enthält das 6-stellige Administratorpasswort. Das Gerät sendet über die Ausführung eine Antwort-SMS, wenn beim Administrator **ACK for SMS message** eingeschaltet ist (Abschnitt 5.6).

Ändern des Administratorpassworts – aus Sicherheitsgründen sollte das Ihr erster Schritt sein:

```
PSW 123456 xxxxxx
```

`123456` – das werkseitige Passwort; `xxxxxx` – das neue, 6-stellige Passwort.

Nur Berechtigte sollen steuern können – senden Sie die Daten der Benutzer vom Telefon des Administrators:

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

`PHONENO` – die Telefonnummer des Benutzers im internationalen Format (+43…); `NAME` – sein Name; `EMAIL` – seine E-Mail-Adresse (für Protegus 2). Nach dem Anlegen der ersten Nummer reagiert der GATOR nur noch auf Anrufe von Nummern auf der Liste.

Administratorrecht für eine weitere Person – weitere Administratoren erhalten die Systemnachrichten und können Benutzer anlegen:

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

`Nox` – die Position des Administrators in der Liste (1–7); wenn Sie **1** eingeben, übertragen Sie Ihr eigenes Administratorrecht.

Liste der SMS-Befehle (in jedem steht das Passwort nach dem Befehlswort, in den Beispielen das werkseitige `123456`):

Befehl	Parameter	Beschreibung
`INFO`	–	Daten des Geräts: Typ, IMEI, Signalstärke, Versorgungsspannung, Firmware-Version, Seriennummer, Datum und Uhrzeit. Beispiel: `INFO 123456`
`ASKI`	–	Zustand der Eingänge. Beispiel: `ASKI 123456`
`ASKO`	–	Zustand der Ausgänge. Beispiel: `ASKO 123456`
`SETA`	`NoX=Telefonnummer#Name#E-Mail`	Anlegen eines Administrators in Zeile X (1A–7A); die Nummer muss mit + und der Ländervorwahl beginnen, die Felder werden durch # getrennt. Beispiel: `SETA 123456 No3=+436641234567#Johann#johann@beispiel.at`
`SETA`	`NoX=DEL`	Löschen des Administrators X. Beispiel: `SETA 123456 No2=DEL`
`SETU`	`Telefonnummer#Name#E-Mail`	Anlegen eines neuen Benutzers (Zeile 11–1010); auch hier muss die Nummer mit + und der Ländervorwahl beginnen, die Felder werden durch # getrennt. Beispiel: `SETU 123456 +436641234567#Peter#peter@beispiel.at`
`DELU`	`Telefonnummer` oder `Name`	Löschen eines Benutzers anhand der Telefonnummer oder des Namens. Beispiel: `DELU 123456 +436641234567`, `DELU 123456 Peter`
`SETB`	`E-Mail` oder `Telefonnummer`	Aufnahme in die Sperrliste (E-Mail-Adresse oder Telefonnummer). Beispiel: `SETB 123456 johann@beispiel.at`, `SETB 123456 +436641234567`

Befehl	Parameter	Beschreibung
`DELB`	`ALL`	Löschen der gesamten Sperrliste. Beispiel: `DELB 123456 ALL`
`DELB`	`E-Mail` oder `Telefonnummer`	Löschen eines Eintrags aus der Sperrliste (bei der E-Mail-Adresse zählt Groß- und Kleinschreibung). Beispiel: `DELB 123456 johann@beispiel.at`, `DELB 123456 +436641234567`
`RESET`	–	Neustart des Geräts. Beispiel: `RESET 123456`
`PSW`	`neues Passwort`	Ändern des Administratorpassworts. Beispiel: `PSW 123456 654123`
`TXTA`	`Objektname`	Festlegen des Objektnamens. Beispiel: `TXTA 123456 Haus`
`TXTE`	`N1=Text` … `N5=Text`	Text der SMS, die beim Auslösen des Eingangs oder Ausgangs gesendet wird; N1…N5 ist die Nummer der Klemme. Beispiel: `TXTE 123456 N1=Tor offen`
`TXTR`	`N1=Text` … `N5=Text`	Text der SMS, die bei der Wiederherstellung gesendet wird. Beispiel: `TXTR 123456 N5=Relais aus`
`SETD`	`IDx=yy`	Inaktivitätszeit des Eingangs x in Minuten (0–2880): nach dem Auslösen benachrichtigt das Gerät und reagiert für diese Zeit nicht auf weitere Änderungen des Eingangs; 0 = ausgeschaltet. Beispiel: `SETD 123456 ID1=30`
`RESD`	`IDx`	Löschen der bereits laufenden Inaktivitätszeit des Eingangs x. Beispiel: `RESD 123456 ID1`
`TIME`	`JJJJ/MM/TT,hh:mm:ss`	Einstellen von Datum und Uhrzeit. Beispiel: `TIME 123456 2026/10/30,12:23:00`
`RDR`	`Telefonnummer#Text`	Weiterleiten einer SMS an die angegebene Nummer (zum Beispiel Guthabenaufladung beim Netzbetreiber). Beispiel: `RDR 123456 +436641234567#Aufladung 10 EUR`
`HELLO`	`ON` / `OFF`	SMS-Benachrichtigung eines neuen Benutzers über das Hinzufügen (bei einem aus der App oder per SMS angelegten Benutzer) ein / aus. Beispiel: `HELLO 123456 ON`
`NATH`	`ON` / `OFF`	Ein- und Ausschalten des Modus **Not authorized** (jeder kann anrufen), ohne die übrigen Einstellungen zu ändern; bei mehreren Ausgängen mit Aufzählung der beim Anruf geschalteten Ausgänge (schaltet den Modus **Not authorized** und die aufgezählten Ausgänge ein, die übrigen Ausgänge aus). Beispiel: `NATH 123456 ON`, `NATH 123456 ON=5,7,22`, `NATH 123456 OFF`
`UUSD`	`*Code#`	Senden eines USSD-Codes an den Mobilfunkanbieter (Guthabenabfrage, Aufladung). Beispiel: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON` / `Protegus=OFF`	Verbinden mit der Protegus-Cloud bzw. Trennen. Beispiel: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`APN=Name`, `USER=Name`, `PSW=Passwort`	APN-Name, Benutzername und Passwort der mobilen Datenverbindung. Beispiel: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`Code=Passwort`	Ändern des Zugangscodes der Protegus-Cloud (**Cloud Access Code**). Beispiel: `CONNECT 123456 Code=123456`

Statt der Ländervorwahl und der E-Mail-Adressen der Beispiele setzen Sie Ihre eigenen Daten ein. Vermeiden Sie in der SMS Umlaute und andere Sonderzeichen, wenn die Einstellung **System Options → Text language** nicht auf den passenden Zeichensatz steht (Abschnitt 5.2). Die Liste der APNs: APN-Einstellungen – Liste der europäischen Mobilfunkanbieter.

5. Einrichtung mit der Software TrikdisConfig

Alle Einstellungen des GATOR erreichen Sie mit der Windows-Software **TrikdisConfig** – über USB-Kabel oder aus der Ferne (Kapitel 6). Mit den Werkseinstellungen öffnet das Gerät auf Anruf (Kapitel 2); die Software brauchen Sie, wenn Sie Benutzer, RFID-Karten, Zeitpläne, SMS-Texte, Module, die Protegus-Cloud oder die Leitstelle einrichten.

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. Nehmen Sie die Frontabdeckung des GATOR mit einem Schlitzschraubendreher gemäß der Abbildung ab.
2. Verbinden Sie den GATOR mit einem **USB-Mini-B**-Kabel mit dem Computer.
3. Starten Sie TrikdisConfig. Die Software erkennt das Gerät und öffnet das Programmierfenster des GATOR.
4. Klicken Sie auf die Taste **Read [F4]**: Die Software liest die aktuellen Einstellungen des Geräts aus. Wenn sie danach fragt, geben Sie im eingeblendeten Fenster den 6-stelligen **Administrator**- oder **Errichtercode** ein (der Administratorcode ist werkseitig `123456`).



Abbildung 28. Abnehmen der Frontabdeckung: Den Schraubendreher in die seitliche Öffnung stecken und nach unten bewegen, dann springt die Abdeckung ab; darunter der USB-Mini-B-Anschluss.

Warnung

Solange das Gerät per USB-Kabel mit dem Computer verbunden ist, befindet es sich im Programmiermodus: Der Normalbetrieb ist unterbrochen, es überwacht nicht, meldet nicht, lässt sich nicht steuern, wird über USB versorgt und startet nach dem Abziehen des Kabels neu. Das Gerät darf daher nicht frei zugänglich sein: Es gehört in ein verschlossenes Metallgehäuse mit Sabotageschutz (Tamper) oder mit einem Bewegungsmelder, der das Gehäuse überwacht. Details in den FAQ

Zu den Werkseinstellungen führt die Taste **Restore** unten links im Programmierfenster zurück (Abschnitt 5.9).

5.1 Die Statusleiste

Nach dem Anschließen und Auslesen des Geräts (**Read [F4]**) werden unten im Fenster die wichtigsten Daten des Geräts angezeigt:

Beschriftung	Bedeutung
IMEI / Unique ID, bei einem Ethernet-Gerät **MAC / Unique ID**	Die eindeutige Kennung des Geräts: bei einem Gerät mit SIM-Karte die IMEI, bei einem Ethernet-Gerät die MAC-Adresse. Dieselbe steht auf der Verpackung und auf der Rückseite des Geräts.
Status	Der aktuelle Betriebszustand.
Device	Der Gerätetyp (Typbezeichnung). Prüfen Sie, ob hier der Typ Ihres eigenen Geräts steht.
SN	Seriennummer.
BL	Die Version des Bootloaders.
FW	Die Version der Firmware.
HW	Die Version der Hardware.
State	Die Verbindungsart: USB oder Fernzugriff (remote).
Administrator / Installer	Die Zugriffsebene der programmierenden Person (nach Eingabe des Passworts).

Nach Abschluss der Einstellungen schreiben Sie sie mit der Schaltfläche **Write [F5]** in das Gerät; mit den Schaltflächen **Open [F8]** und **Save [F9]** können Sie den gesamten Einstellungssatz in einer Datei speichern und in ein anderes Gerät laden. **Save [F9]** speichert die Einstellungen in einer Einstellungsdatei, **Open [F8]** öffnet die gespeicherte Datei; die gespeicherten Einstellungen können Sie später auch in andere Geräte laden und so mehrere Geräte schnell mit identischen Einstellungen einrichten.



Abbildung 29. Die Statusleiste des GATOR: im linken Feld die **IMEI/Unique ID**, unten **Status: reading done**, **Device: GV17_2200** (der Typcode), die Seriennummer, die Version **BL** und **FW**, die Verbindungsart (USB). Beim GATOR muss das Feld **Device** die Form **GV17_xxxx** haben.

5.2 Seite „System Options“

Die allgemeinen Einstellungen des Geräts: Kennung, Uhrzeit, Administratorcode, Anrufannahme, Test, SIM-Karte und Zeitzone.

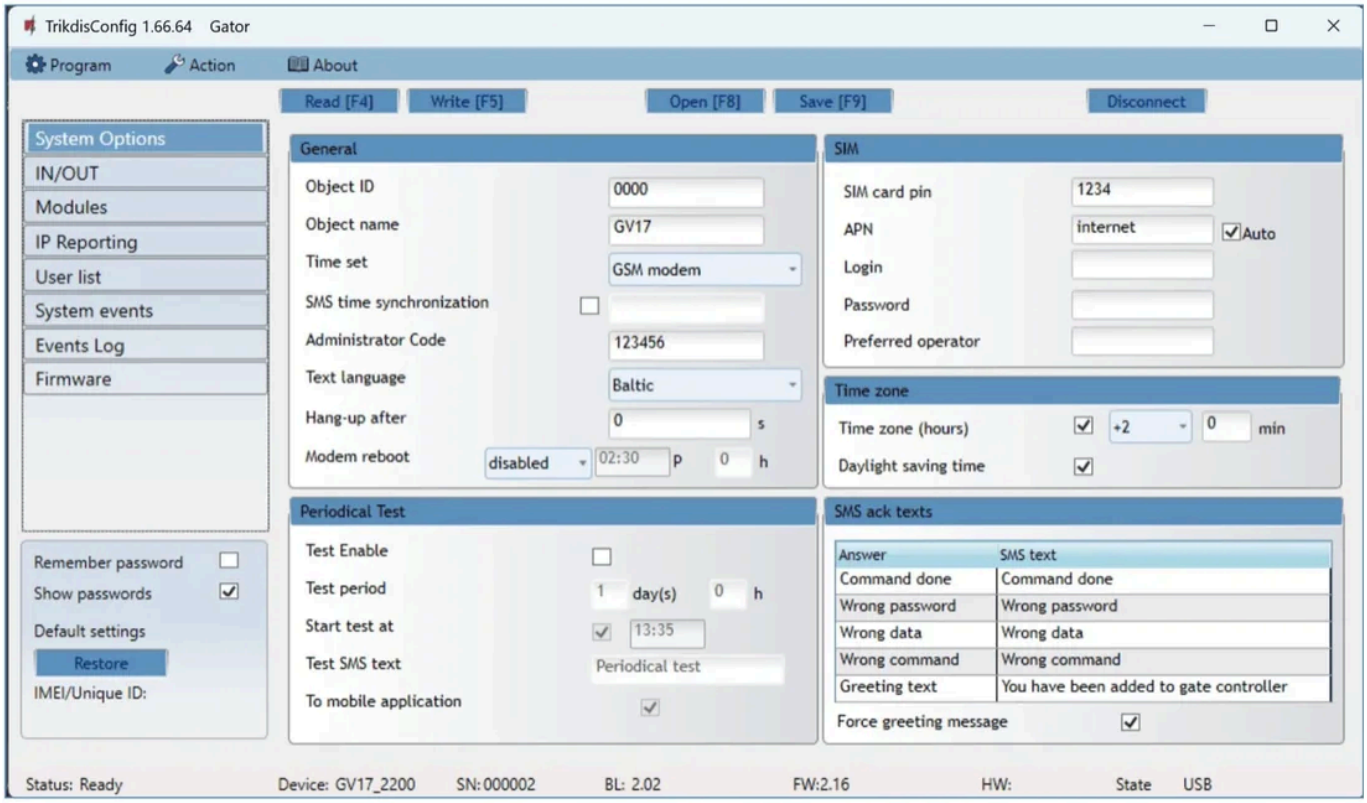


Abbildung 30. TrikdisConfig – **System Options**: die Gruppen **General**, **Periodical test**, **SIM**, **Time zone** und **SMS ack texts**.

Gruppe General

- **Object ID** – die von der Leitstelle vergebene Objektkennung (4-stellige Hexadezimalzahl, 0–9, A–F). Verwenden Sie nicht die Werte FFFE und FFFF.
- **Object name** – unter diesem Namen sendet das Gerät alle Ereignisse.
- **Time set** – die Quelle der Zeitsynchronisierung (zum Beispiel das Mobilfunknetz).
- **SMS time synchronization** – setzen Sie das Häkchen und geben Sie die Nummer der SIM-Karte des GATOR im internationalen Format ein (+43…), wenn die Uhrzeit per SMS synchronisiert werden soll.
- **Administrator Code** – der Administratorcode: damit lassen sich alle Parameter des GATOR ändern (werkseitig `123456` – ändern Sie ihn).
- **Text language** – der Zeichensatz der SMS-Nachrichten.
- **Hang-up after** – bei 0 weist das Gerät den Anruf ab (öffnet auf Anruf); bei einem anderen Wert nimmt es ihn an und beendet ihn nach der angegebenen Anzahl Sekunden – für die Steuerung per Tastatur (DTMF) (Abschnitt 4.2).
- **Modem reboot** – täglicher Neustart des Modems zu einer festgelegten Uhrzeit.

Gruppe Periodical test

- **Test Enable** – angehakt sendet das Gerät regelmäßige Testmeldungen.
- **Test period** – die Zeit zwischen den Testmeldungen.
- **Start test at** – der Zeitpunkt des ersten Tests.
- **Test SMS text** – der Text der Test-SMS.
- **To mobile application** – angehakt geht die Testmeldung auch an die App Protegus 2.

Gruppe SIM

- **SIM card PIN** – der PIN-Code der SIM-Karte, wenn Sie die Abfrage nicht ausgeschaltet haben.

- **APN** – der Zugangspunkt der mobilen Datenverbindung. Mit dem Kästchen **Auto** wählt das Gerät den APN aus der eingebauten Liste (Daten mehrerer internationaler und nationaler Anbieter) und verwendet den in das Feld eingetragenen Wert nur, wenn es den Anbieter nicht findet. Wenn die Datenverbindung nicht zustande kommt, geben Sie den APN des Anbieters ein: APN-Einstellungen – Liste der europäischen Mobilfunkanbieter.
- **Login**, **Password** – Benutzername und Passwort des APN, wenn der Anbieter sie verlangt.
- **Preferred operator** – wenn Sie einen Anbietercode (MCC + MNC) angeben, verbindet sich der GATOR nur mit diesem Netz; das ist bei internationalen (Roaming-)SIM-Karten von Bedeutung.

Gruppe Time zone – hier stellen Sie die genaue Uhrzeit des Landes ein: Geben Sie die Zeitzone an und markieren Sie, ob es im Land eine Sommerzeit gibt.

- **Time zone (hours)** – setzen Sie das Häkchen und geben Sie die Zeitzone des Landes an (Österreich und Deutschland: +1).
- **Daylight saving time** – setzen Sie das Häkchen, wenn es im Land eine Sommerzeit gibt.

Gruppe SMS ack texts – die Texte der Antwort-SMS, die der Benutzer nach den SMS-Befehlen erhält.

- **Force greeting message** – angehakt sendet das Gerät einem per SMS oder aus Protegus 2 angelegten neuen Benutzer eine Begrüßungs-SMS (per SMS: `HELLO 123456 OFF` schaltet sie aus).

5.3 Seite „IN/OUT“

Die Einstellungen der Ein- und Ausgänge, der RFID-Leser und der Arbeitszeiterfassung, auf drei Reitern: **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 Reiter IN/OUT – die Ein- und Ausgänge

In der Tabelle steht je Zeile eine Klemme; hier legen Sie fest, welche ein Eingang und welche ein Ausgang ist und wie sie melden soll.

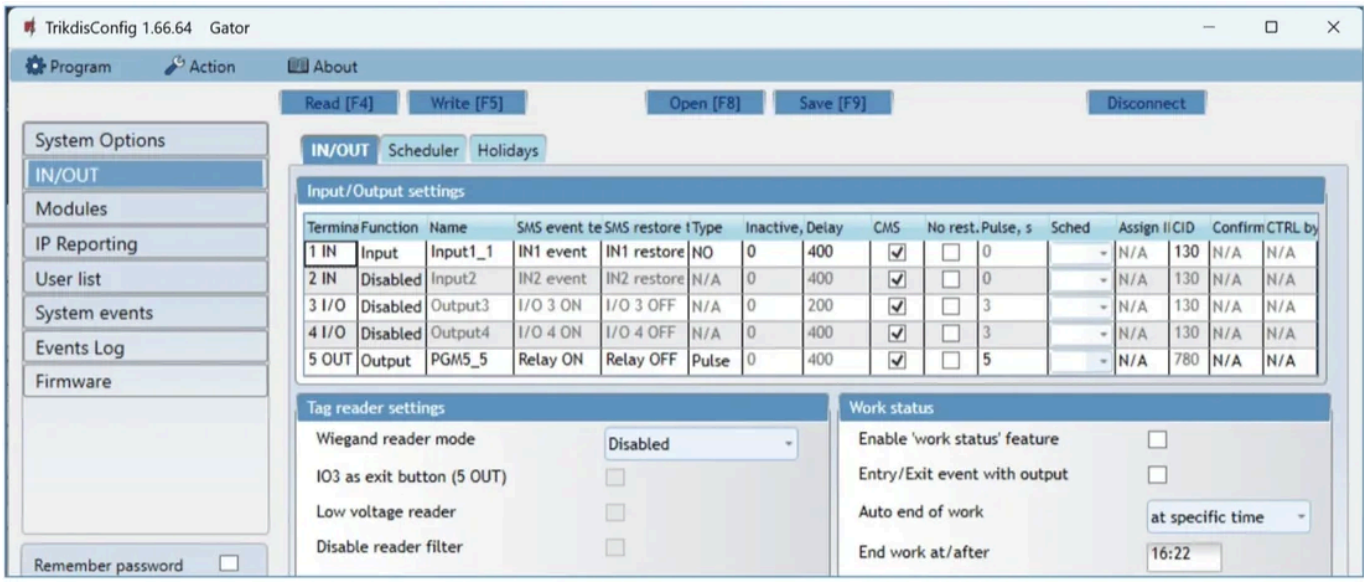


Abbildung 31. TrikdisConfig – **IN/OUT**: die Tabelle **Input/Output settings** (werkseitig der Eingang 1 IN, 2 IN, 3 I/O, 4 I/O deaktiviert, 5 OUT als Ausgang vom Typ **Pulse**), darunter die Gruppen **Tag reader settings** und **Work status**.

Gruppe Input/Output settings

- **Terminal** – die Nummer der Klemmen des GATOR (1 IN … 5 OUT; die Klemmen der Erweiterungen am Ende der Liste).
- **Function** – die Funktion der Klemme: **Input** (Eingang), **Output** (Ausgang) oder **Disabled** (deaktiviert).
- **Name** – der Name des Eingangs oder Ausgangs (so erscheint er in der App und in den SMS).
- **SMS event text** – der Text der beim Auslösen gesendeten SMS.
- **SMS restore text** – der Text der bei der Wiederherstellung gesendeten SMS.
- **Type** – beim Eingang der Schleifentyp (**NC**, **NO**, **EOL = 10 kΩ**), beim Ausgang die Betriebsart: **Pulse** (Impuls) oder **Level** (zwei Schaltzustände).
- **Inactive** – der Eingang meldet nach der ersten Auslösung für diese Zeit nicht erneut; 0 = ausgeschaltet.
- **Delay** – die Reaktionszeit des Eingangs in Millisekunden (werkseitig 400 ms).
- **CMS** – angehakt geht das Ereignis an die Leitstelle und auch an Protegus 2.
- **No rest.** – kein Wiederherstellungsereignis senden.
- **Pulse** – die Impulslänge in Sekunden, wenn der Ausgang vom Typ **Pulse** ist (werkseitig 3 s an 5 OUT; für einen Torantrieb genügen meist 1–3 s).
- **Sched** – die Nummer des Zeitplans, der den Ausgang steuert (vom Reiter **Scheduler**).
- **Assign IN** – der dem Ausgang zugeordnete Eingang: Die App zeigt statt des Zustands des Ausgangs den tatsächlichen Zustand des Eingangs (des Tors) (Abschnitt 5.10).
- **CID** – der Contact-ID-Code des Ereignisses.
- **Confirm** – die Nummer des Eingangs, dessen aktiver Zustand Voraussetzung für das Schalten des Ausgangs ist.
- **CTRL by IN** – die Auslösung des gewählten Eingangs schaltet den Ausgang (lokale Automatik, funktioniert auch ohne Netz).

Gruppe Tag reader settings – die Einstellungen der RFID-Leser (Anschluss in Abschnitt 3.6)

- **Wiegand reader mode** – die Anzahl der angeschlossenen Wiegand-Leser: **Single Reader** oder **Dual Reader**.
- **IO3 as exit button (5 OUT)** – setzen Sie das Häkchen, wenn der Ausgangstaster an der Klemme 3 I/O angeschlossen ist: Beim Drücken schaltet 5 OUT für die eingestellte Impulsdauer ein.
- **Low voltage reader** – für einen Leser mit Niederspannung (5-V-Signalpegel).
- **Disable reader filter** – schaltet den internen Filter für kurze Impulse aus, wenn das Gerät die Signale des Lesers nicht erkennt.

Gruppe Work status – Arbeitszeiterfassung in Protegus 2 (Details: GV17 – Zutrittskontroll- und/oder Arbeitszeiterfassungssystem)

- **Enable “work status” feature** – schaltet die Anzeige des Arbeitsstatus in der App ein.
- **Entry/Exit event with output** – angehakt entsteht auch beim Fernschalten des Ausgangs ein Eingangs- / Ausgangsereignis.
- **Auto end of work** – die Art des automatischen Abschlusses der Arbeitszeit.
- **End work at/after** – der Zeitpunkt des Abschlusses oder die Zeit bis zum Abschluss, je nach der vorherigen Einstellung.

5.3.2 Reiter Scheduler – Zeitpläne der Ausgänge

Die Ausgänge können auch nach Zeitplan selbstständig schalten (zum Beispiel das Tor während der Arbeitszeit offen, abends geschlossen). Den Zeitplan ordnen Sie in der Spalte **Sched** des Ausgangs zu.

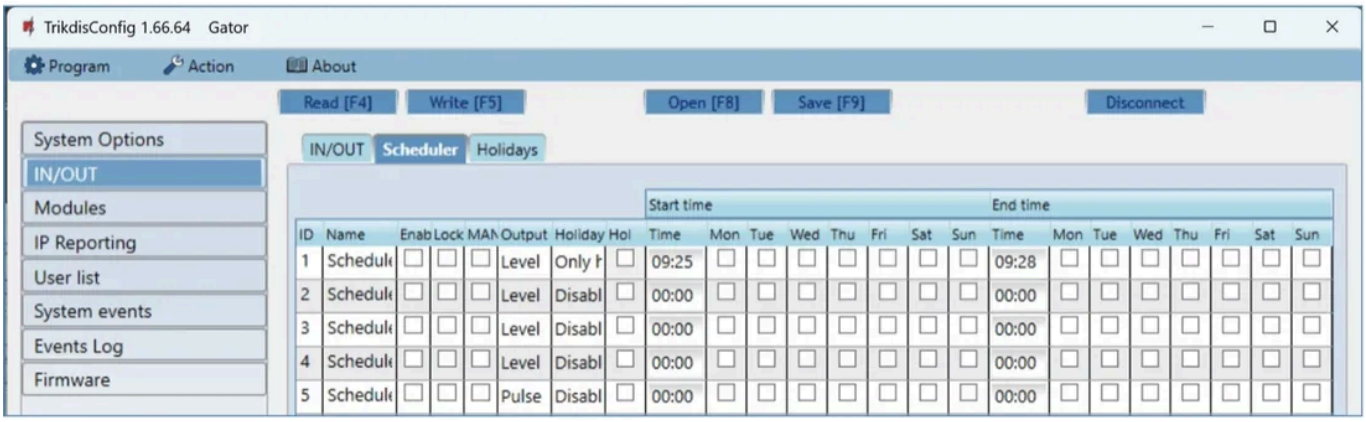


Abbildung 32. TrikdisConfig – IN/OUT, Reiter **Scheduler**: je Zeitplan Freigabe, Sperre, Ausgangsmodus, Feiertagsmodus, Start- und Endzeit mit den Wochentagen.

- **Name** – der Name des Zeitplans.
- **Enable** – Freigabe des Zeitplans.
- **Lock** – angehakt lässt sich der Ausgang während der aktiven Zeit des Zeitplans nicht auf andere Weise (per Anruf, aus der App) schalten.
- **MANUAL** – angehakt schaltet der Ausgang beim Start des Zeitplans nicht von selbst; der Zeitplan startet, wenn der Benutzer den Ausgang einschaltet.
- **Output mode** – die Funktion des Ausgangs während des Zeitplans: **Level** – der Ausgang ist während der angegebenen Dauer durchgehend eingeschaltet; **Pulse** – der Ausgang schaltet am Anfang und am Ende des Zeitplans für die eingestellte Impulsdauer.
- **Holiday mode** – wie der Zeitplan an Feiertagen arbeiten soll; **Hol** – setzen Sie das Häkchen, wenn an Feiertagen die Feiertagszeiten verwendet werden sollen.
- **Start time** – die Wochentage und die Uhrzeit, ab der der Ausgang einschaltet.
- **End time** – die Wochentage und die Uhrzeit, bis zu der der Ausgang eingeschaltet bleibt.

Ist der Modus des Ausgangs **Level** und nur **End time** angegeben, schaltet der Ausgang zur angegebenen Uhrzeit aus, wenn er bis dahin eingeschaltet war.

5.3.3 Reiter Holidays – Feiertage

Hier geben Sie die Kalendertage an, an denen der Zeitplan mit den Feiertagszeiten arbeitet.

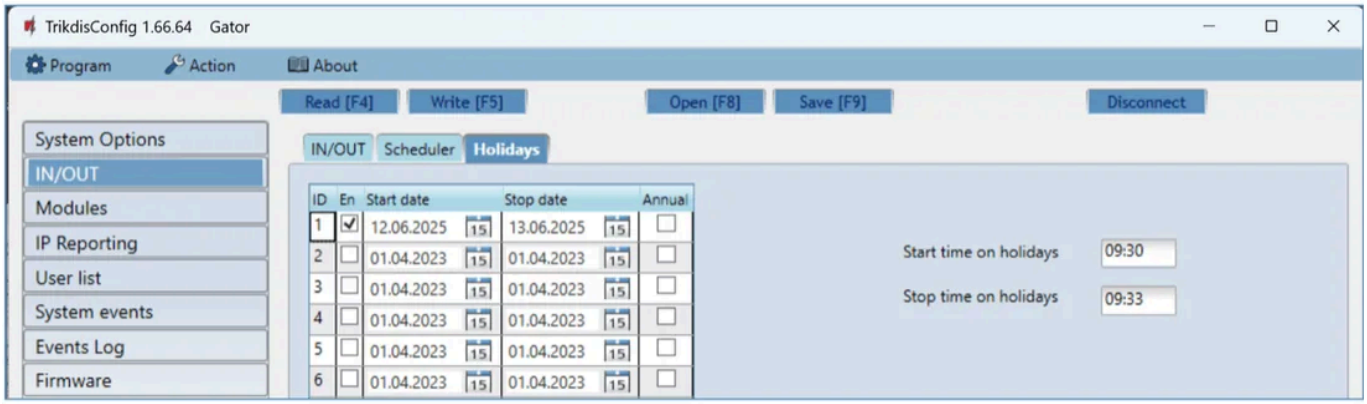


Abbildung 33. TrikdisConfig – IN/OUT, Reiter **Holidays**: Feiertagszeiträume mit Start- und Enddatum, mit Start- und Endzeit für Feiertage.

- **En.** – Freigabe des Feiertagszeitraums.
- **Start date**, **Stop date** – der erste und der letzte Tag des Zeitraums.
- **Annual** – jedes Jahr wiederkehrender Feiertag: Das Gerät berücksichtigt nur Monat und Tag.

- **Start time on holidays**, **Stop time on holidays** – die Start- und Endzeit an Feiertagen.

5.4 Seite „Modules“

5.4.1 Reiter Modules

An den GATOR lassen sich über den RS485-Bus oder per Funk diese Module anschließen: **W485** WLAN-Modul, **E485** Ethernet-Modul, **iO-LORA** drahtlose Erweiterung (über den Sende-Empfänger RF-LORA, bis zu 8; die an die iO-LORA Erweiterungen angeschlossenen RFID-Leser können so bis zu 8 weitere Ausgänge schalten, ein Leser immer nur einen Ausgang seiner eigenen Erweiterung – ab GATOR-Firmware 2.13, Abschnitt 3.9), **iO8** kabelgebundene und **iO8-LORA** drahtlose Erweiterung (über das RF-LORA; von beiden zusammen eine). Den Sende-Empfänger RF-LORA müssen Sie nicht in die Liste aufnehmen. Gibt es am Standort WLAN oder kabelgebundenes Internet, sendet der GATOR mit dem Modul W485 oder E485 die Nachrichten über das Internet an die Protegus-Cloud und an die Leitstelle: Es werden keine mobilen Daten verbraucht (der Datenverkehr der SIM-Karte kann sogar gesperrt werden), und der GATOR kann sogar ohne SIM-Karte, nur aus der App gesteuert, verwendet werden.

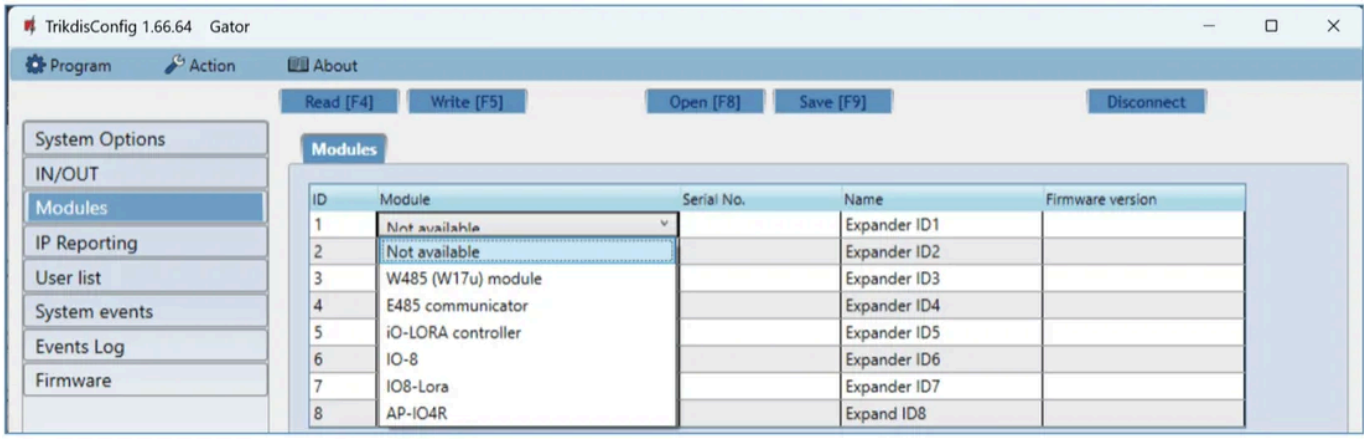


Abbildung 34. TrikdisConfig – **Modules**: in der Auswahlliste **Module** die Module W485, E485, iO-LORA, iO8, iO8-LORA und **AP-IO4R** (iO4R); daneben die Spalten **Serial No.**, **Name** und **Firmware version**.

- **Module** – wählen Sie das angeschlossene Modul aus der Liste.
- **Serial No.** – die 6-stellige Seriennummer des Moduls (auf dem Aufkleber am Gehäuse und am Karton des Moduls).

Nach der Auswahl des Moduls und der Eingabe der Seriennummer erscheint der Reiter **Parameters** mit den eigenen Einstellungen des Moduls.

Relaiserweiterung iO4R

Das in der Liste aufgeführte **AP-IO4R** ist die Relaiserweiterung **iO4R**: Sie dient zur Überwachung und zum Fernüberbrücken der Sicherheitssensoren der Torautomatik sowie zum Zählen der Torzyklen. Sie wird in der App Protegus 2 eingerichtet, im Modus **Advanced Gator Monitoring**, der beim Hinzufügen der Torsteuerung wählbar ist – siehe die Anleitung zum iO4R.

5.4.2 Reiter Parameters – WLAN-Modul W485

Nach der Auswahl des W485 geben Sie hier die Daten des WLAN und die Art der Nutzung der SIM-Karte an.

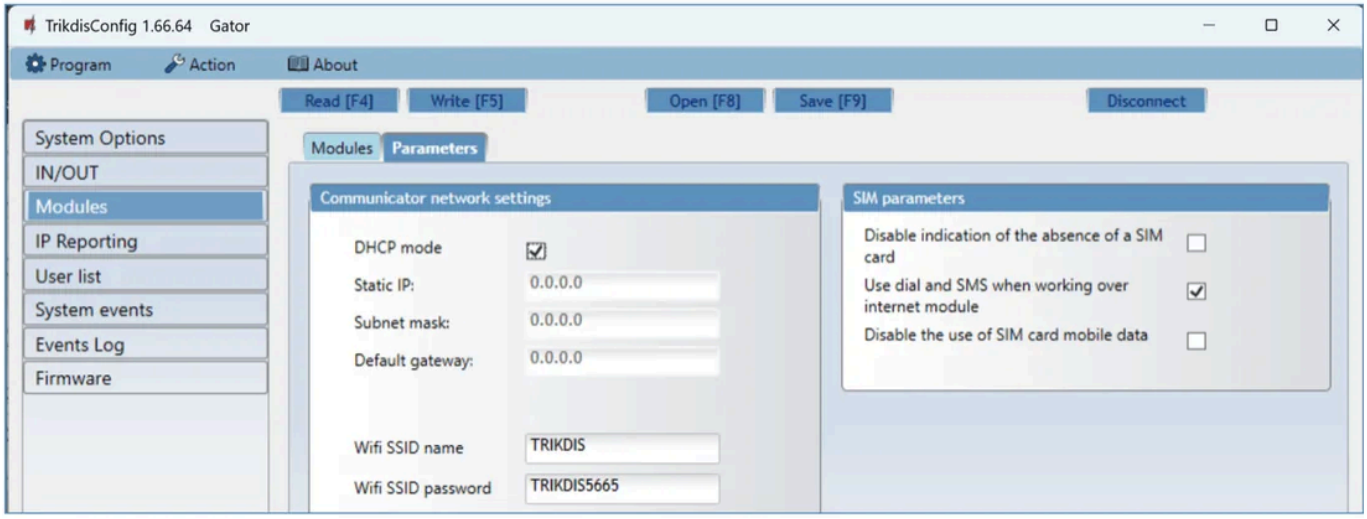


Abbildung 35. TrikdisConfig – Modules, Reiter **Parameters** für das W485: **Communicator network settings** (DHCP, IP-Adresse, Name und Passwort des WLAN) und **SIM parameters**.

Gruppe Communicator network settings

- **DHCP mode** – angehakt erhält das Modul die Netzwerkeinstellungen (IP-Adresse, Subnetzmaske, Gateway) automatisch vom Router; leer geben Sie sie von Hand ein.
- **Static IP**, **Subnet mask**, **Default gateway** – die feste IP-Adresse, die Subnetzmaske und die Adresse des Gateways bei manueller Einstellung.
- **Wifi SSID name** – der Name des WLAN, mit dem sich das W485 verbindet (2,4-GHz-Netz).
- **Wifi SSID password** – das Passwort des WLAN.

Gruppe SIM parameters

- **Disable indication of the absence of a SIM card** – angehakt meldet das Gerät die fehlende SIM-Karte nicht als Fehler (bei Betrieb ohne SIM, nur über Internet).
- **Use dial and SMS when working over internet module** – angehakt funktioniert die Steuerung per Anruf und SMS auch neben dem Modul. Leer verwendet das Gerät, solange die Internetverbindung besteht, keine Anrufe und SMS; fällt das Internet aus, funktionieren Anruf und SMS wieder, und das Gerät sendet den Benutzern eine SMS.
- **Disable the use of SIM card mobile data** – angehakt verwendet das Gerät die mobilen Daten der SIM-Karte nicht, die Daten gehen nur über das W485. Fällt das WLAN aus, speichert das Gerät die Ereignisse und sendet sie, wenn die Verbindung zurückkehrt.

5.4.3 Reiter Parameters – Ethernet-Modul E485

Nach der Auswahl des E485 geben Sie hier die Daten des kabelgebundenen Netzes und die Art der Nutzung der SIM-Karte an.

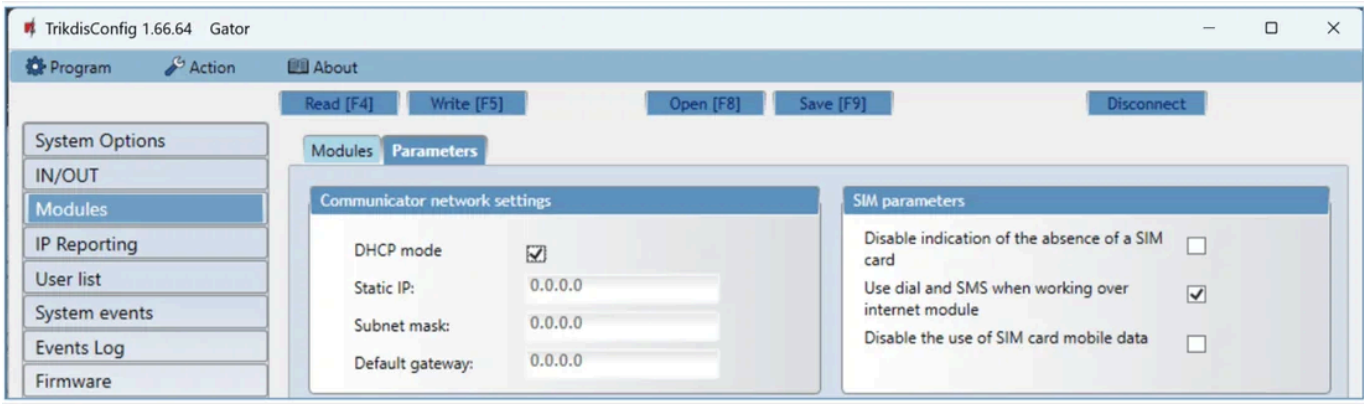


Abbildung 36. TrikdisConfig – Modules, Reiter **Parameters** für das E485: Netzwerkeinstellungen (DHCP oder feste IP-Adresse) und **SIM parameters**.

- **DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway** – wie beim W485: automatische oder manuelle Netzwerkeinstellung.
- **SIM parameters** – die Bedeutung der drei Kästchen ist dieselbe wie beim W485 beschrieben; bei gesperrten mobilen Daten gehen die Daten nur über das E485, während eines Internetausfalls speichert das Gerät die Ereignisse.

5.5 Seite „IP Reporting“

Der GATOR sendet die Ereignisse an den IP-Empfänger der Leitstelle und an die Protegus-Cloud; die Cloud schalten Sie auf dieser Seite ein.

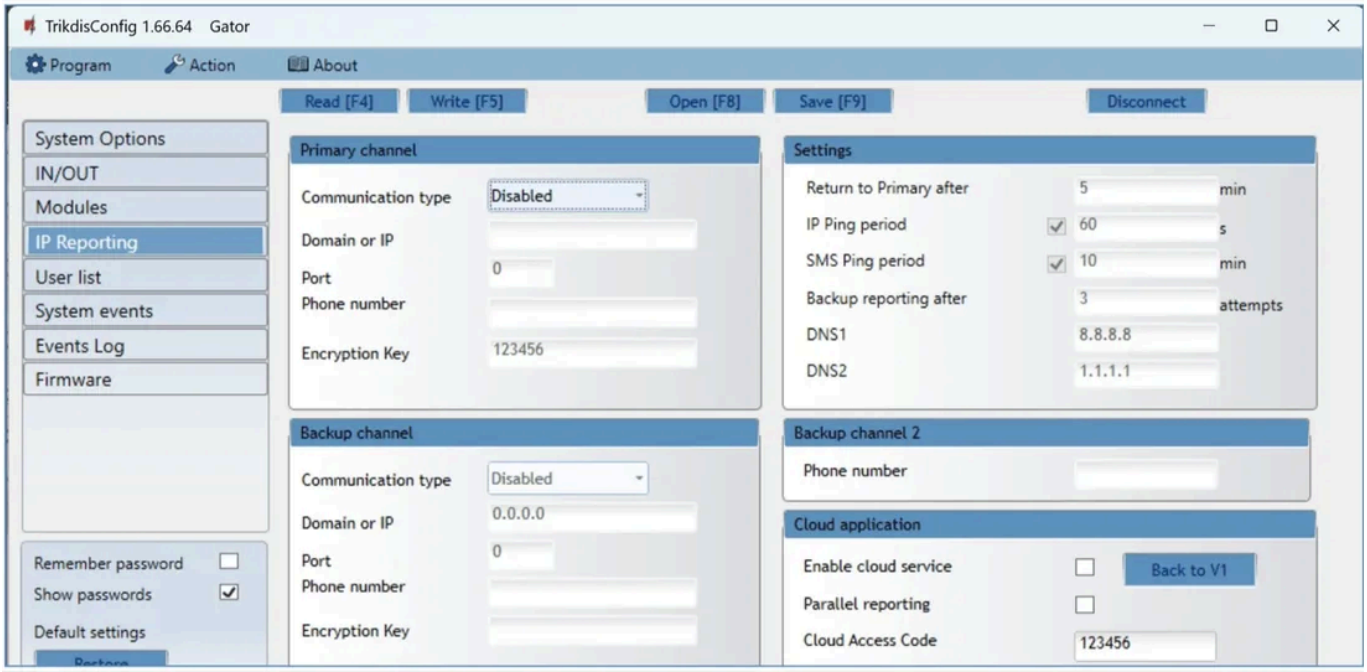


Abbildung 37. TrikdisConfig – **IP Reporting**: **Primary channel** und **Backup channel** (werkseitig ausgeschaltet), **Settings**, der SMS-Ersatzkanal und die Gruppe **Cloud application** mit dem Kästchen **Enable cloud service** und dem **Cloud Access Code**.

Gruppe Primary channel

- **Communication type** – die Art der Verbindung mit dem Empfänger der Leitstelle: **IP** oder **SMS**; **Disabled** = keine Übertragung.
- **Domain or IP** – der Domainname oder die IP-Adresse des Empfängers.
- **Port** – der Netzwerkport des Empfängers.

- **Phone number** – die Telefonnummer des SMS-Empfängers der Leitstelle (+43…), wenn der Typ SMS ist.
- **Encryption Key** – 6-stelliger Verschlüsselungsschlüssel, der mit dem im Empfänger eingestellten übereinstimmen muss.

Gruppe Backup channel – der Ersatzempfänger, mit den gleichen Einstellungen wie der primäre.

Gruppe Settings

- **Return to primary after** – nach dieser Zeit versucht das Gerät, vom Ersatzkanal zum primären Kanal zurückzukehren.
- **IP Ping period** – Freigabe und Intervall der PING-Signale, die die Verbindung aufrechterhalten.
- **SMS Ping period** – dasselbe auf dem SMS-Kanal.
- **Backup reporting after** – nach so vielen erfolglosen Versuchen wechselt das Gerät auf den Ersatzkanal.
- **DNS1**, **DNS2** – die IP-Adressen der Nameserver.

Gruppe Backup channel 2

- **Phone number** – die Nummer des SMS-Empfängers der Leitstelle. Das Gerät sendet hierher eine SMS, wenn die Nachricht weder über den primären noch über den Ersatz-IP-Kanal gesendet werden kann; das funktioniert auch dann, wenn im Netz des Mobilfunkanbieters die IP-Verbindung ausfällt. Es greift nur, wenn beide IP-Kanäle über das Mobilfunknetz laufen; der SMS-Empfänger erhält eine Nachricht beim ersten Einschalten des Geräts und beim Verlust der TCP/IP- oder UDP/IP-Verbindung.

Gruppe Cloud application

- **Enable cloud service** – Einschalten der Protegus-Cloud: Der GATOR kommuniziert mit der App und lässt sich mit TrikdisConfig auch aus der Ferne programmieren (Kapitel 6).
- **Parallel reporting** – angehakt gehen die Ereignisse gleichzeitig an die Leitstelle, an Protegus 2 und an die Benutzer; leer erhalten die App und die Benutzer sie erst nach der Quittung der Leitstelle.
- **Cloud Access Code** – 6-stelliger Code für die Verbindung mit Protegus 2 (werkseitig `123456`); danach fragt die App beim Hinzufügen des Systems, wenn er nicht der werkseitige ist.

5.6 Seite „User list“

Die Liste der Administratoren und Benutzer, die Registrierung der RFID-Karten, die Benutzerzeitpläne und die Sperrliste – auf vier Reitern.

5.6.1 Reiter Users – die Benutzer

In der Tabelle steht je Zeile ein Administrator oder Benutzer mit seinen Berechtigungen.

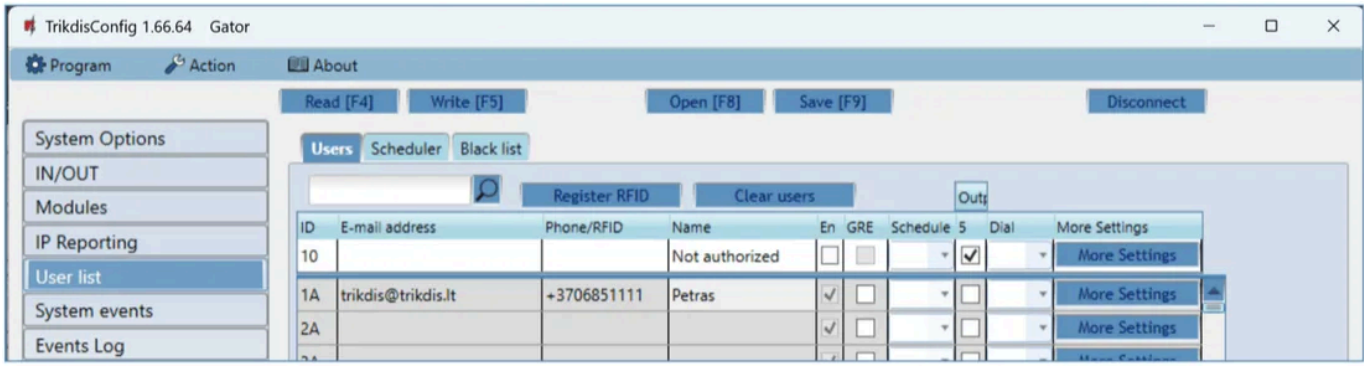


Abbildung 38. TrikdisConfig – **User list**, Reiter **Users**: oben die Tasten **Register RFID** und **Clear users**; in der Tabelle die Spalten **ID**, **E-mail address**, **Phone/RFID**, **Name**, **En**, **GRE**, **Schedule**, **Dial** und die Taste **More settings**; die Zeile 10 ist der Eintrag **Not authorized**.

- **ID** – die Nummer des Benutzers. Die Zeilen mit dem Buchstaben **A** (**1A–7A**) sind die Administratoren: Sie können das Gerät einstellen, die Ausgänge schalten und erhalten die Nachrichten. Die Zeilen mit den Nummern **11–1010** sind die Benutzer: Sie können nur die Ausgänge schalten.
- **E-mail address** – die E-Mail-Adresse des Benutzers (für Protegus 2).
- **Phone/RFID** – die Telefonnummer im internationalen Format (+43…) oder die Kennnummer der RFID-Karte.
- **Name** – der Name des Benutzers.
- **En** – Freigabe des Benutzers: angehakt kann der Benutzer die Ausgänge schalten.
- **GRE** – Senden einer Begrüßungs-SMS an den Benutzer.
- **Schedule** – die Nummer des Zeitplans, nach dem der Benutzer steuern darf (Abschnitt 5.6.3).
- **Output** – der bzw. die vom Benutzer steuerbaren Ausgänge.
- **Code** – bei einem Wiegand-Leser mit Codetastatur der Code des Benutzers.
- **Dial** – der bzw. die beim Anruf schaltenden Ausgänge, wenn der Benutzer mehrere Ausgänge hat; nach dem Schalten beendet das Gerät den Anruf.
- **More settings** – das Fenster der weiteren Einstellungen (unten).

Die Zeile 10 „Not authorized“

Ist beim Benutzer Nr. 10 mit dem Namen **Not authorized** das Kästchen **En angehakt**, kann der GATOR **von jeder beliebigen Telefonnummer** per Anruf gesteuert werden. Ist es leer, können nur die in der Liste Eingetragenen anrufen; jeder Benutzer schaltet den in seiner eigenen Spalte **Dial** markierten Ausgang. Dasselbe stellt per SMS der Befehl `NATH` ein (Abschnitt 4.7).

Nach der Abschaltung des 2G-Netzes kann es vorkommen, dass einige Mobilfunkanbieter dem von uns verwendeten Modem Quectel EG915U-EU keine Sprachanrufe über das 4G-Netz (VoLTE) erlauben. In diesem Fall funktionieren das Öffnen des Tores per Anruf und die Benachrichtigung per Anruf nicht. Der SMS-Versand und die Datenverbindung (Protegus 2 App) sind von dieser Einschränkung nicht betroffen und funktionieren weiterhin.

Weitere Einstellungen – Administrator (1A–7A)

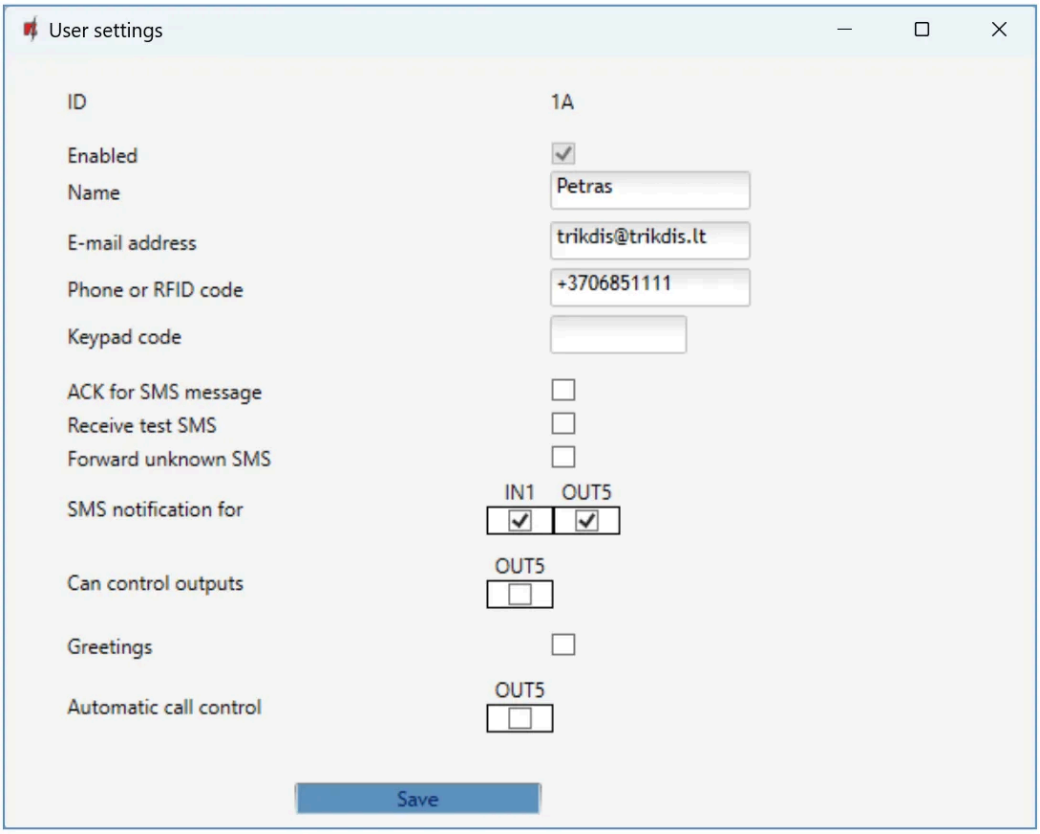


Abbildung 39. TrikdisConfig – **User settings** bei einem Administrator: **Enabled**, die Daten, **ACK for SMS message**, **Receive test SMS**, **Forward unknown SMS**, **SMS notification for** (IN1, IN2, OUT3, OUT4, OUT5), **Can control output**, **Greetings** und **Automatic call control**.

- **ID**, **Enabled**, **Name**, **E-mail address**, **Phone or RFID code**, **Keypad code** – die Daten entsprechend den Spalten der Liste.
- **ACK for SMS message** – der Administrator erhält eine Antwort-SMS über die Ausführung der SMS-Befehle.
- **Receive test SMS** – er erhält die regelmäßige Test-SMS.
- **Forward unknown SMS** – SMS von unbekannten Nummern (zum Beispiel die Guthabenmitteilung des Anbieters) leitet das Gerät an ihn weiter.
- **SMS notification for** – über die Änderung welcher Ereignisse (IN1, IN2, OUT3, OUT4, OUT5) er eine SMS erhält.
- **Can control output** – die von ihm steuerbaren Ausgänge.
- **Greetings** – Senden einer Begrüßungs-SMS.
- **Automatic call control** – die bei seinem Anruf schaltenden Ausgänge, danach beendet das Gerät den Anruf.

Weitere Einstellungen – Benutzer (11–1010)

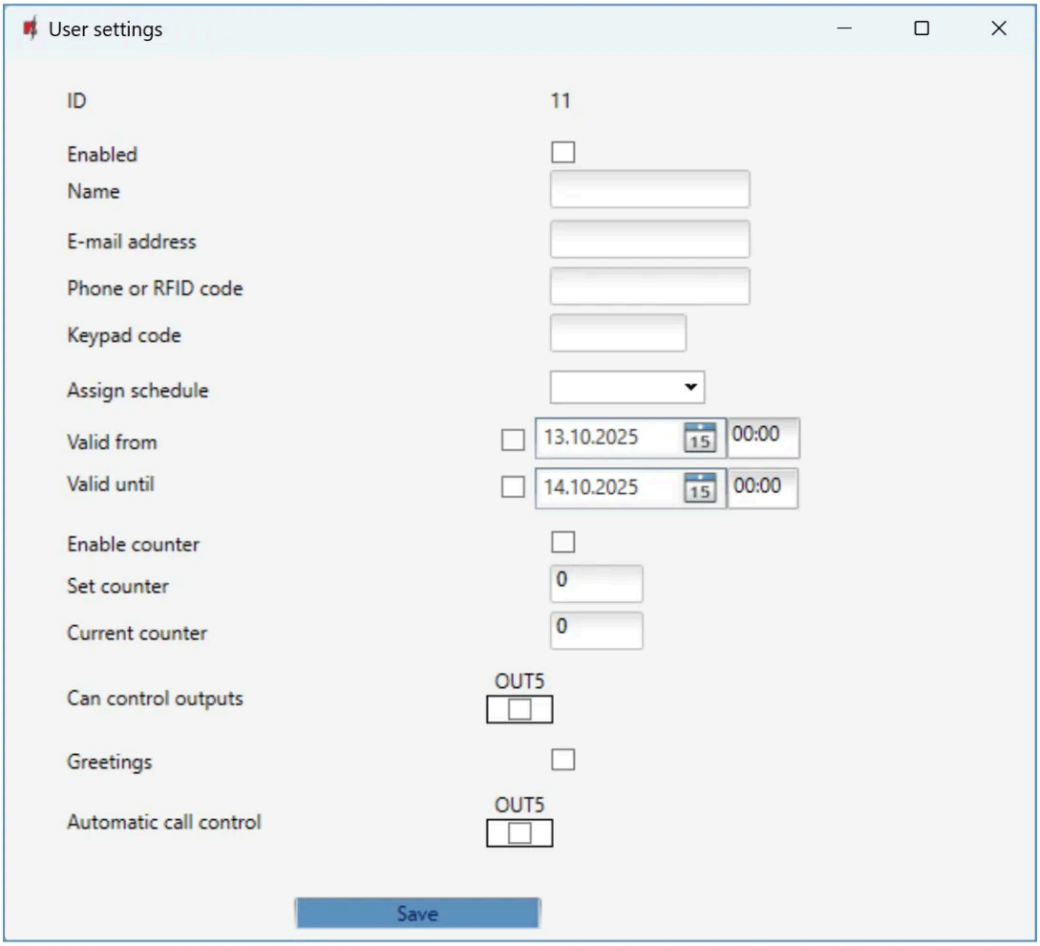


Abbildung 40. TrikdisConfig – **User settings** bei einem Benutzer: **Assign schedule**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs**, **Greetings**, **Automatic call control**.

- **Assign schedule** – der bzw. die Zeitpläne, während derer der Benutzer steuern darf.
- **Valid from**, **Valid until** – Beginn und Ende der Berechtigung (Datum und Uhrzeit) – zum Beispiel für einen Mieter oder Gast.
- **Enable counter** – Einschalten des Zählers; **Set counter** – wie oft der Benutzer innerhalb der angegebenen Zeit steuern darf; **Current counter** – die Anzahl der bisherigen Schaltvorgänge.
- **Can control outputs**, **Greetings**, **Automatic call control** – wie beim Administrator.

5.6.2 Registrieren einer RFID-Karte (eines Schlüsselanhängers)

1. Schließen Sie den RFID-Leser an (Abschnitt 3.6), schalten Sie die Versorgung des GATOR ein, starten Sie TrikdisConfig und verbinden Sie sich per USB-Kabel oder aus der Ferne. Stellen Sie auf der Seite **IN/OUT** die Anzahl der Leser ein (**Wiegand reader mode**).
2. Klicken Sie auf der Seite **User list** auf die Taste **Register RFID**.

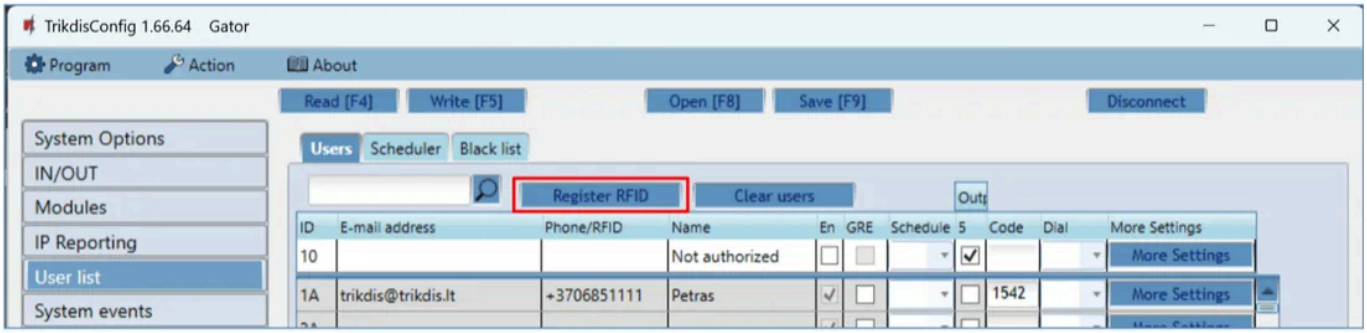


Abbildung 41. TrikdisConfig – User list: die Taste **Register RFID** über der Benutzertabelle.

3. Das Registrierungsfenster (**Add RFID tag/card to reader**) öffnet sich.

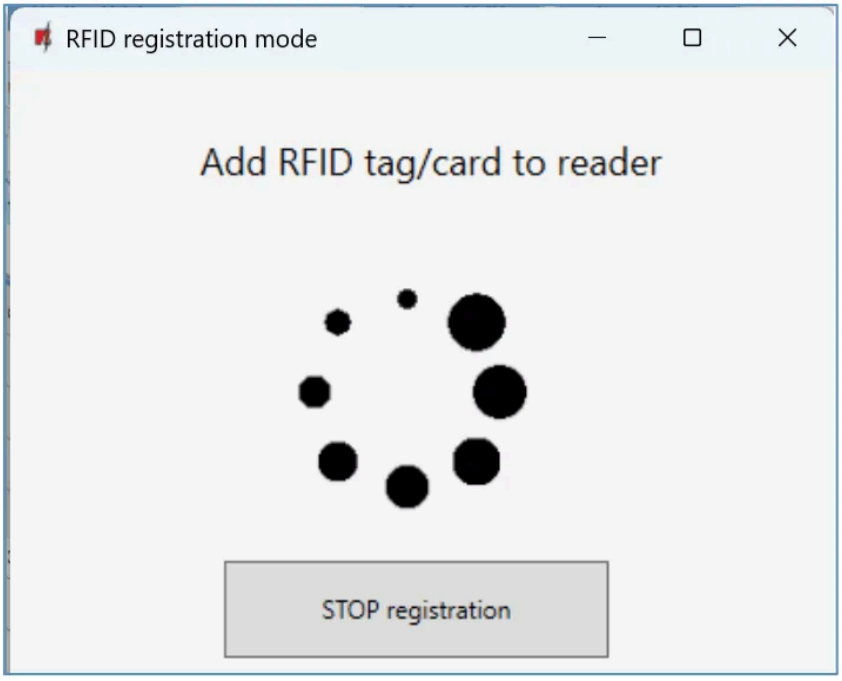


Abbildung 42. Das RFID-Registrierungsfenster: Die Karte muss an den Leser gehalten werden; die Taste **STOP registration** beendet die Registrierung.

4. Halten Sie die Karte an den Leser. Sobald der Leser sie eingelesen hat, öffnet sich ein neues Fenster: Geben Sie den Namen des Benutzers ein (**Enter user name**), markieren Sie den steuerbaren Ausgang (**User can control PGM Output 5**; mit dem Kästchen **Device administrator** wird er Administrator) und klicken Sie auf die Taste **ADD**. Wiederholen Sie das mit den weiteren Karten und drücken Sie dann die Taste **STOP registration**.
5. Schreiben Sie die Kartenliste mit der Taste **Write [F5]** in das Gerät.

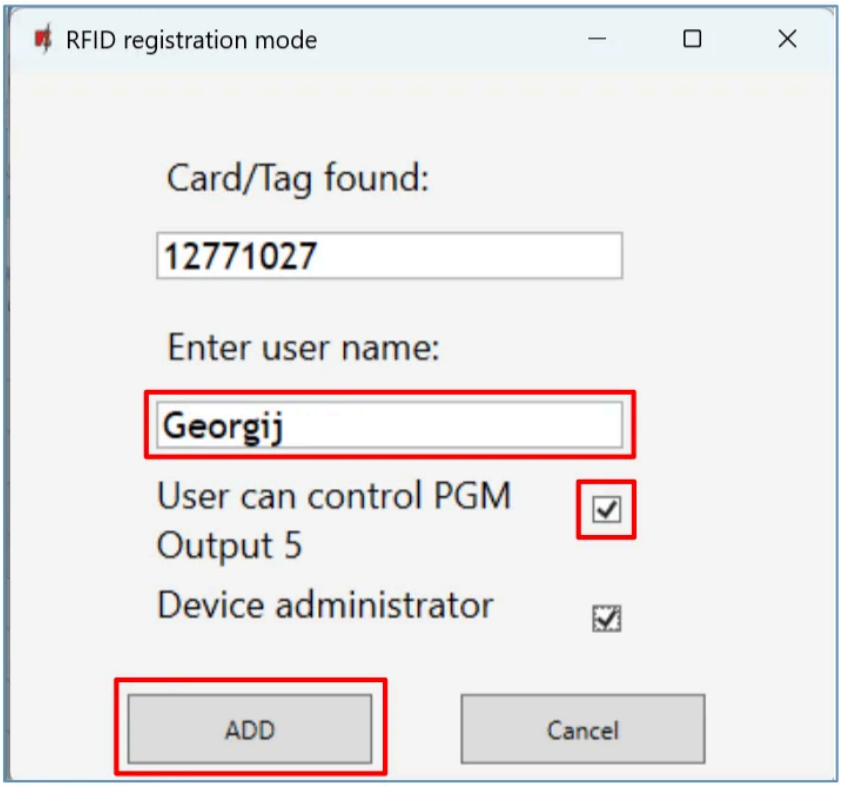


Abbildung 43. Das Fenster der eingelesenen Karte: Name, **User can control PGM Output 5**, **Device administrator**, dann **ADD**.

Anlegen einer Karte anhand ihrer Nummer: Die auf die Karte gedruckte Kennnummer können Sie auch direkt in das Feld **Phone/RFID** eingeben; geben Sie den Namen ein, setzen Sie das Häkchen bei **En** und beim steuerbaren Ausgang, dann **Write [F5]**.

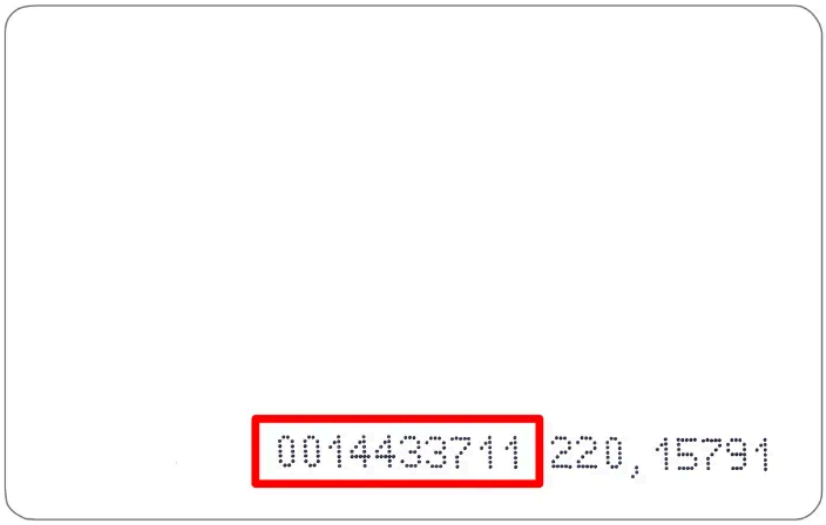


Abbildung 44. Die auf die RFID-Karte gedruckte Kennnummer (am unteren Rand der Karte).

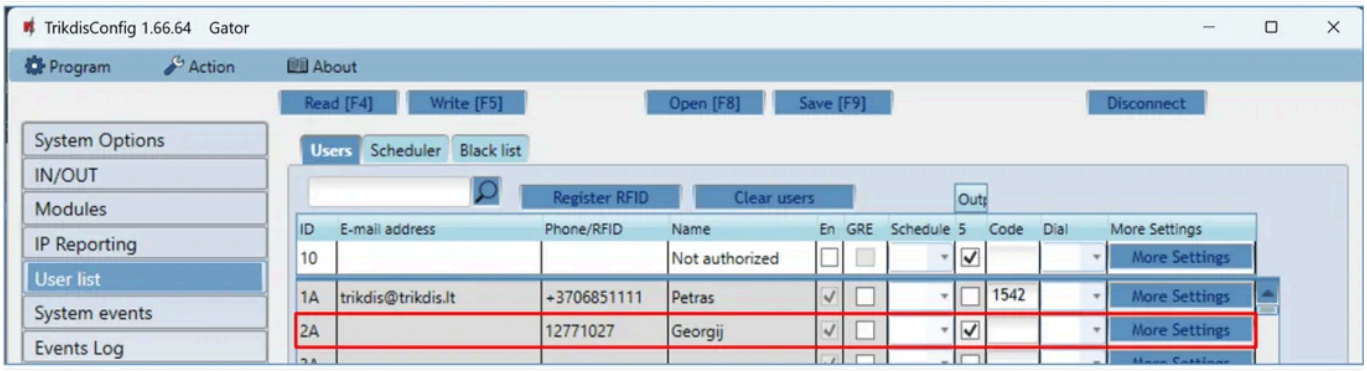


Abbildung 45. TrikdisConfig – User list: die Zeile des neuen Benutzers mit der Kartennummer im Feld **Phone/RFID**, dem Namen, **En** angehakt, der Ausgang 5 markiert.

Anlegen einer Karte aus Protegus 2: Wählen Sie in der Benutzerliste das Hinzufügen eines neuen Benutzers, geben Sie die E-Mail-Adresse, den Namen, die Kennnummer der Karte (in das Feld der Telefonnummer), bei einem Leser mit Codetastatur den 4-stelligen Code ein, markieren Sie den Ausgang und speichern Sie (Abschnitt 4.5).

5.6.3 Reiter Scheduler – Zeitpläne der Benutzer

Der Benutzer darf nur während des zugeordneten Zeitplans steuern (zum Beispiel die Reinigungskraft werktags zwischen 6 und 8 Uhr). Den Zeitplan ordnen Sie in der Spalte **Schedule** des Benutzers oder im Feld **More settings** → **Assign schedule** zu.

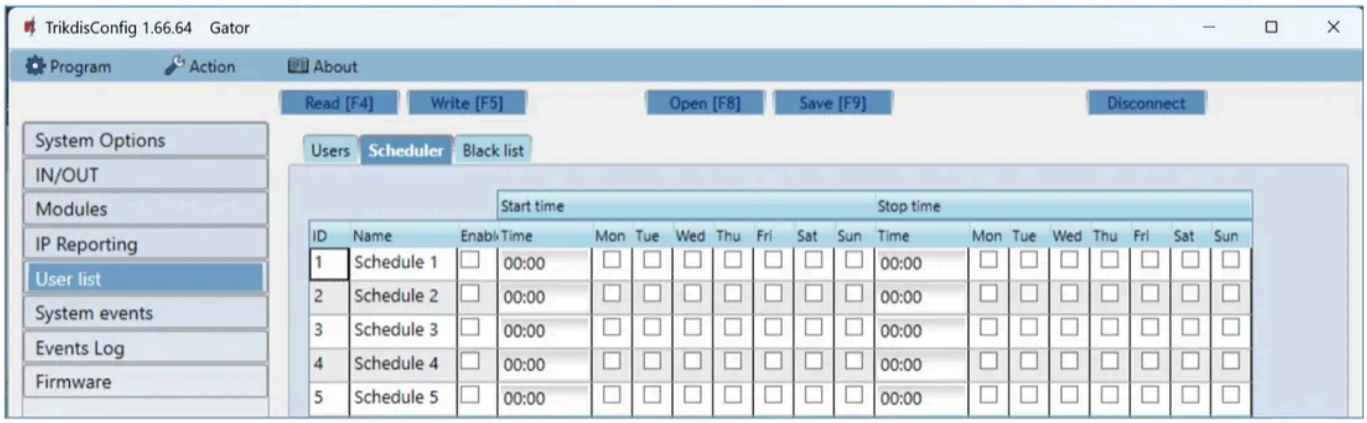


Abbildung 46. TrikdisConfig – User list, Reiter **Scheduler**: fünf Zeitpläne, jeder mit **Enable**, Start- und Endzeit mit den Wochentagen.

- **Name** – der Name des Zeitplans.
- **Enable** – Freigabe des Zeitplans.
- **Start time** – die Wochentage und die Uhrzeit, ab der der Benutzer steuern darf.
- **Stop time** – die Wochentage und die Uhrzeit, bis zu der er steuern darf.

5.6.4 Reiter Black list – Sperrliste

Wer hier eingetragen ist, kann das Gerät auf keine Weise steuern.

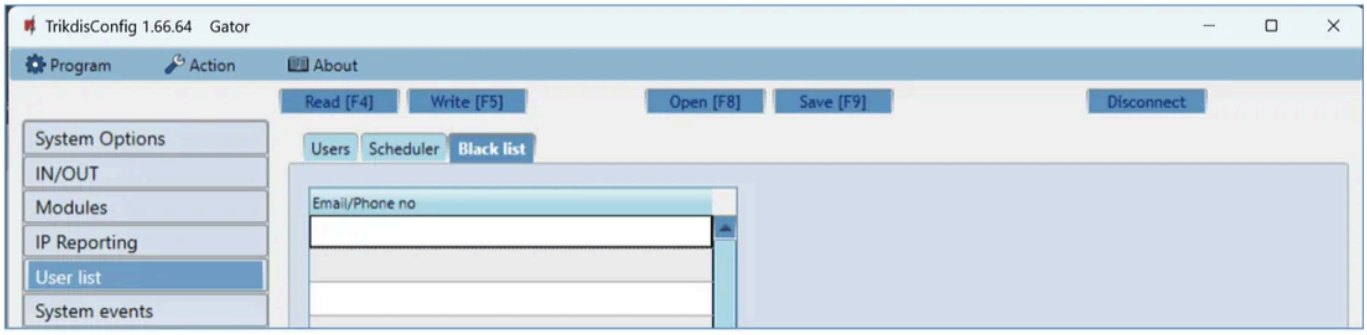


Abbildung 47. TrikdisConfig – User list, Reiter **Black list**: die Tabelle der gesperrten E-Mail-Adressen, Telefonnummern und Kartennummern.

Auf der Sperrliste stehen die E-Mail-Adressen, Telefonnummern und RFID-Kartennummern, denen die Steuerung des GATOR verboten ist. Einträge können Sie auch direkt aus dem Ereignisprotokoll aufnehmen: Klicken Sie mit der rechten Maustaste auf die Telefonnummer, die E-Mail-Adresse oder die Kartennummer und wählen Sie den Menüpunkt **Add to black list**. Per SMS verwalten die Befehle `SETB` und `DELB` die Liste (Abschnitt 4.7).

5.7 Seite „System events“

Hier legen Sie fest, welche der eigenen Systemereignisse des GATOR an die Leitstelle und an die App Protegus 2 gehen.

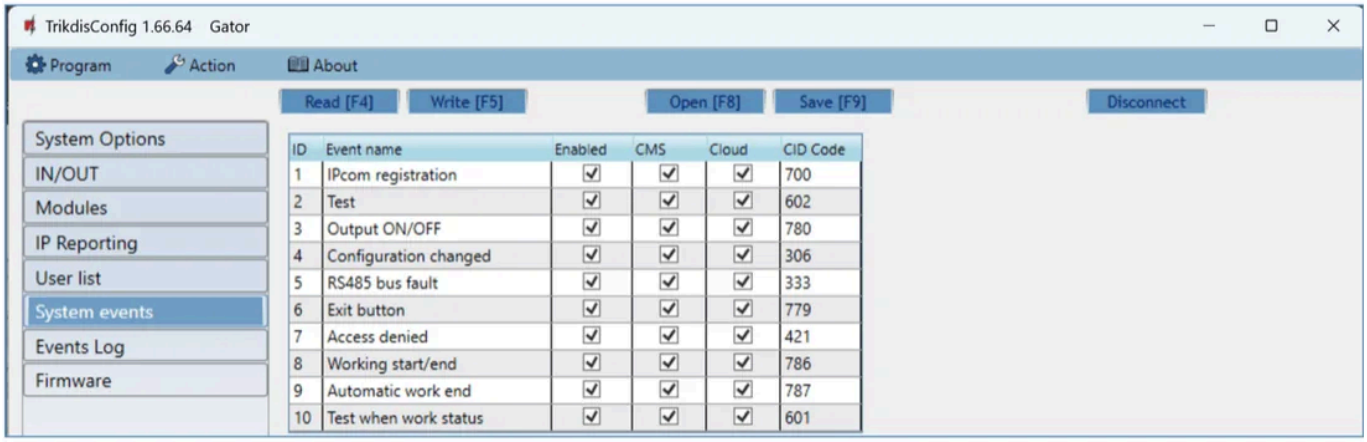


Abbildung 48. TrikdisConfig – **System events**: die Liste der Ereignisse mit dem Contact-ID-Code (zum Beispiel IPcom registration 700, Test 602, Output ON/OFF 780, Configuration changed 306, RS485 bus fault 333, Exit button 779, Access denied 421, Working start/end 786, Automatic work end 787), jedes mit den Kästchen **Enabled**, **CMS** und **Cloud**.

- **ID** – die Nummer des Ereignisses.
- **Event name** – der Name des Ereignisses.
- **Enabled** – Überwachung des Ereignisses.
- **CMS** – das Ereignis geht an die Leitstelle.
- **Cloud** – das Ereignis geht an die App Protegus 2.
- **CID Code** – der Contact-ID-Code des Ereignisses.

5.8 Seite „Events Log“

Das eigene Ereignisprotokoll des Geräts – für die Fehlersuche und zum Nachverfolgen der Zutritte.

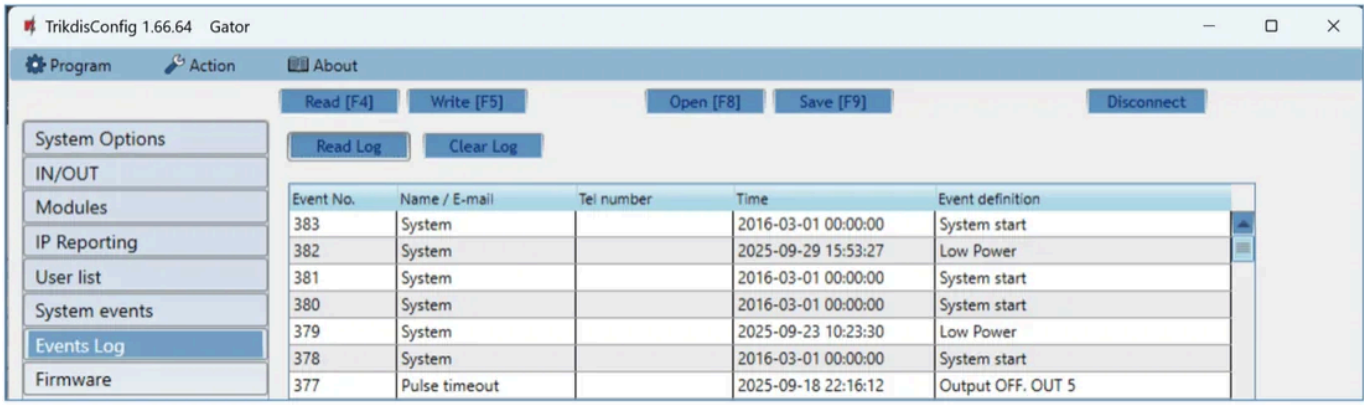


Abbildung 49. TrikdisConfig – **Events Log**: die Tasten **Read Log** und **Clear Log**; bei den Ereignissen die Nummer, der Name oder die E-Mail-Adresse des Benutzers, die Telefonnummer, die Uhrzeit und die Beschreibung des Ereignisses.

Klicken Sie auf die Taste **Read Log**: Die Software liest die Ereignisse aus dem Speicher des Geräts aus (bis zu 5000). Das Protokoll zeigt alle Vorgänge und internen Ereignisse des GATOR mit ausführlichen Daten: wer wann womit (Anruf, SMS, App, Karte) das Tor geöffnet hat und welche Eingänge sich geändert haben. Die Taste **Clear Log** löscht das Protokoll.

5.9 Zurücksetzen auf Werkseinstellungen

Um die Werkseinstellungen wiederherzustellen, klicken Sie unten links im Programmierfenster in der Gruppe **Default settings** auf die Taste **Restore**. Das Zurücksetzen löscht alle Einstellungen – auch die Benutzerliste und die Passwörter –, deshalb empfiehlt es sich, die Einstellungen vorher in einer Datei zu speichern (**Save [F9]**).

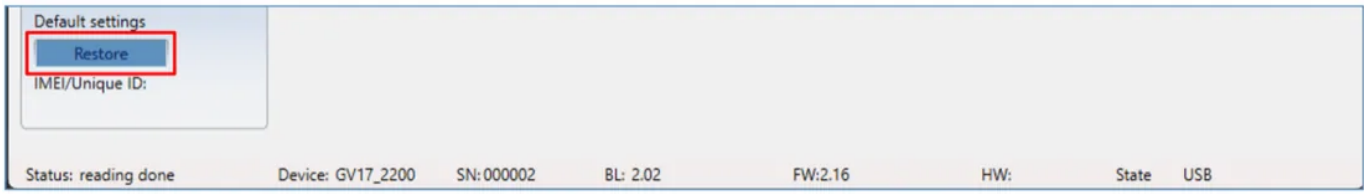


Abbildung 50. TrikdisConfig – die Taste **Restore** der Gruppe **Default settings** über der Statusleiste.

5.10 Anzeige des Torzustands

Die App Protegus 2 und das Widget können den tatsächlichen Zustand des Tors (offen oder geschlossen) anzeigen. Dazu muss der Eingang **1 IN** des GATOR an den Zustandsausgang des Torantriebs oder an den Endschalter des Tors angeschlossen werden (Abschnitt 3.5), und in der Software muss der Eingang dem Ausgang zugeordnet werden, der das Tor schaltet:

1. Auf der Seite **IN/OUT** muss **1 IN** die Funktion **Input** haben, mit dem zum Kontakt passenden Typ (im Beispiel NO). Wählen Sie in der Zeile von **5 OUT** in der Spalte **Assign IN** den Eingang **1 IN**.
2. Wenn Sie auch eine SMS über das Öffnen und Schließen des Tors möchten, geben Sie für 1 IN die Texte **SMS event text** und **SMS restore text** ein (zum Beispiel „Tor offen“ / „Tor geschlossen“).

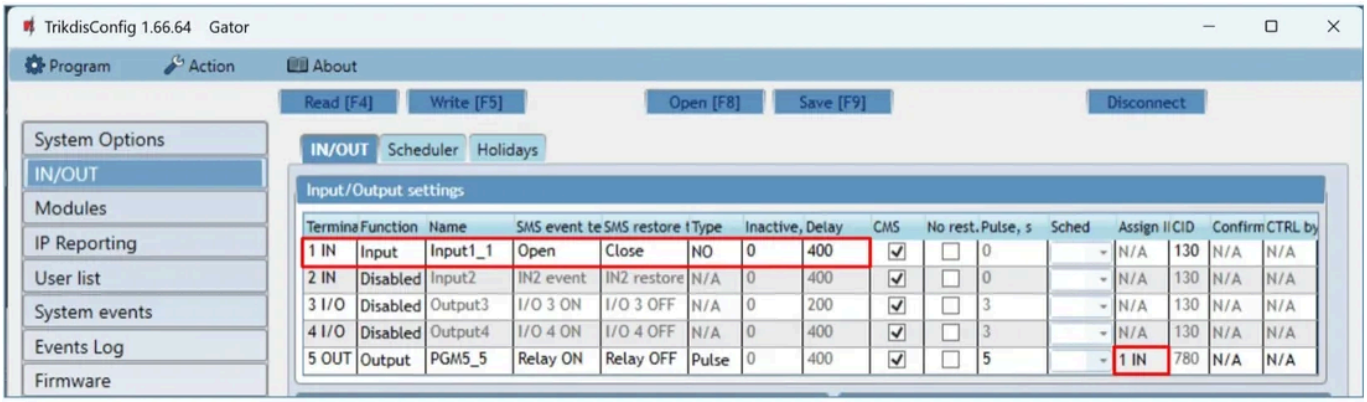


Abbildung 51. TrikdisConfig – IN/OUT: der Eingang **1 IN** (NO, mit den SMS-Texten **Open** / **Close**), in der Zeile von **5 OUT** in der Spalte **Assign IN** der Eingang **1 IN**.

3. Klicken Sie auf der Seite **User list** in der Zeile des Benutzers auf die Taste **More settings** und setzen Sie in der Gruppe **SMS notification for** das Häkchen bei **IN1**, damit der Benutzer eine SMS über den Zustand des Tors erhält. Klicken Sie auf die Taste **Save** und schreiben Sie dann die Einstellungen (**Write [F5]**).



Abbildung 52. TrikdisConfig – User list: die Taste **More settings** in der Zeile des Benutzers.

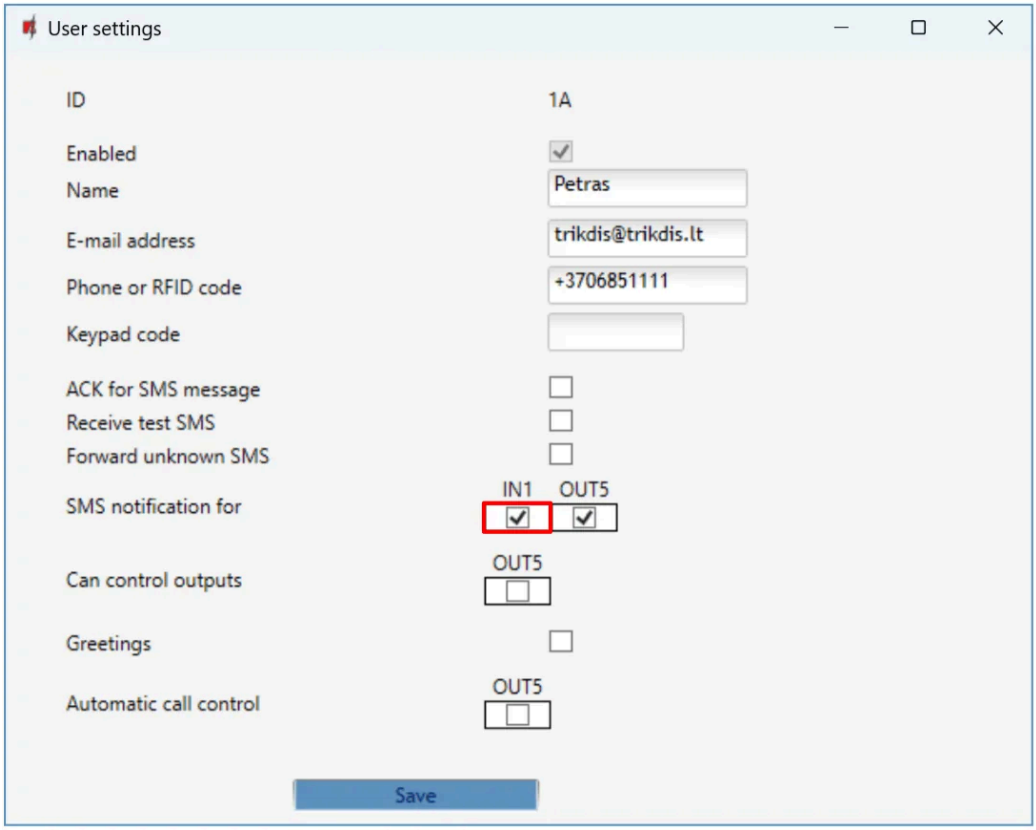


Abbildung 53. TrikdisConfig – User settings: in der Gruppe **SMS notification for IN1** (und **OUT5**) angehakt, unten die Taste **Save**.

6. Fernprogrammierung

Die Einstellungen des GATOR können Sie über die Protegus-Cloud auch aus der Ferne auslesen und ändern – Sie müssen nicht zum Standort fahren.

Voraussetzungen für die Fernprogrammierung

In TrikdisConfig muss auf der Seite **IP Reporting** das Kästchen **Enable cloud service** angehakt sein (Abschnitt 5.5; per SMS: `CONNECT 123456 PROTEGUS=ON`), die Versorgung muss in Ordnung sein (die LED **POWER** blinkt grün), und das Gerät muss im Netz sein (die LED **NETWORK** leuchtet grün und blinkt gelb). Sind diese Bedingungen nicht erfüllt, ist das Gerät aus der Ferne nicht erreichbar.

1. Laden Sie die neueste Version von TrikdisConfig von der Website von Trikdis herunter (https://www.trikdis.com) und installieren Sie sie, falls sie noch nicht auf Ihrem Computer ist.
2. Vergewissern Sie sich, dass der GATOR mit dem Internet verbunden und die Protegus-Cloud eingeschaltet ist.
3. Starten Sie TrikdisConfig. Geben Sie im Bereich **Remote access** des Startbildschirms in das Feld **Unique ID** die **IMEI**-Nummer des GATOR ein (sie steht auf dem Aufkleber an der Unterseite des Geräts und auf dem Karton; bei USB-Verbindung sehen Sie sie auch in der Statusleiste).
4. Geben Sie in das Feld **System Name** einen beliebigen Namen ein (zum Beispiel den Namen des Objekts) und klicken Sie auf die Taste **Configure**.

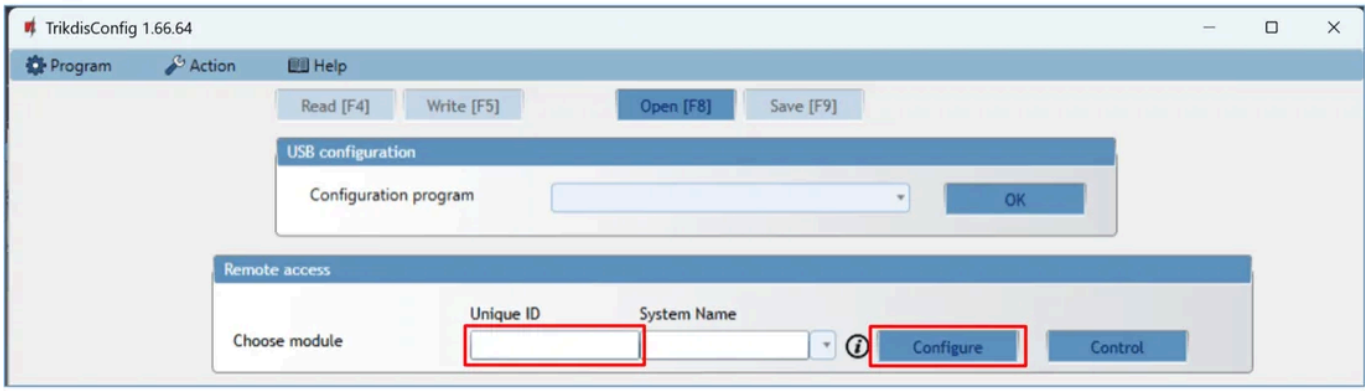


Abbildung 54. TrikdisConfig – der Bereich **Remote access**: das Feld **Unique ID**, das Feld **System Name** und die Taste **Configure**.

5. Das Programmierfenster des GATOR öffnet sich. Klicken Sie auf die Taste **Read [F4]**: Die Software liest die aktuellen Einstellungen des Geräts aus. Fragt die Software nach dem Zugangscode, geben Sie den 6-stelligen **Administratorcode** ein. Wenn Sie das Häkchen bei **Remember password** setzen und auf die Taste **Write [F5]** klicken, merkt sich die Software den Code.
6. Nehmen Sie die Einstellungen vor und schreiben Sie sie mit der Taste **Write [F5]**. Trennen Sie zum Schluss mit der Taste **Disconnect** die Verbindung und schließen Sie die Software.

Für die Fernprogrammierung ist keine Hilfe vor Ort nötig: Der Kunde prüft nur Versorgung und Netz anhand der LEDs. Für Änderungen an der Benutzerliste braucht es nicht einmal TrikdisConfig – der Administrator verwaltet sie auch aus Protegus 2 (Abschnitt 4.5) oder per SMS (Abschnitt 4.7).

7. Funktionsprüfung

Testen Sie am Ende der Installation und der Einrichtung das gesamte System – vor Ort, noch bevor Sie es übergeben:

1. **Versorgung**: Die LED **POWER** blinkt grün. Blinkt sie gelb, ist die Versorgungsspannung nicht in Ordnung – messen Sie sie an den Versorgungsklemmen (9–32 V DC oder 12–24 V AC).
2. **Netz**: Die LED **NETWORK** leuchtet grün und blinkt entsprechend der Signalstärke gelb (3 Blinkimpulse reichen bereits aus). Blinkt die LED **TROUBLE**, zeigt die Anzahl der Blinkimpulse den Fehler an (Abschnitt 1.5).
3. **Eingänge**: Lösen Sie nacheinander die angeschlossenen Eingänge aus (Torzustandskontakt, Ausgangstaster) und prüfen Sie, ob die Empfänger die richtigen Nachrichten per SMS, in Protegus 2 und in der Leitstelle erhalten.
4. **Ausgänge**: Schalten Sie die Ausgänge aus der Ferne ein – per Anruf, aus der App, per SMS und auch mit der Karte, wenn ein Leser vorhanden ist – und prüfen Sie, ob sich das Tor öffnet, die Empfänger die Nachrichten erhalten und der Torzustand auch in der App der Wirklichkeit folgt (Abschnitt 5.10).

Die DATA-LED ist die einfachste Internetprüfung. Die DATA-LED leuchtet, wenn sich im Speicher des Geräts eine Meldung befindet, die auf das Senden wartet. Das Grün der NETWORK-LED sagt nur, dass die Netzwerkverbindung aufgebaut ist – bei einem Mobilfunkgerät hat es sich im Netz des Anbieters angemeldet, bei einem Ethernet-Gerät steht die Verbindung bis zum Router –, nicht aber, dass das Gerät auch das Internet erreicht. Ist die NETWORK-LED grün, leuchtet die DATA-LED aber auch nach einem Ereignis oder Testbericht dauerhaft, funktioniert die Internetverbindung nicht: Die Meldung kann nicht gesendet werden. Im

Mobilfunknetz liegt der Fehler meist am APN oder am Datendienst der SIM-Karte, bei Ethernet am Router, an der Firewall oder am DNS. Erlischt die DATA-LED, wurde die Meldung gesendet, und die Datenverbindung ist in Ordnung.

Den Zustand des Geräts können Sie auch per SMS vom Administratortelefon abfragen: Auf den Befehl `INFO 123456` sendet der GATOR seinen Typ, die Signalstärke, die Versorgungsspannung, die Firmware-Version, Datum und Uhrzeit zurück (Abschnitt 4.7). Kommt keine Antwort-SMS an, prüfen Sie, ob beim Administrator **ACK for SMS message** eingeschaltet ist (Abschnitt 5.6).

8. Firmware-Aktualisierung

Ist der GATOR mit TrikdisConfig verbunden und gibt es eine neuere Firmware, bietet die Software die Aktualisierung von selbst an – dafür muss der Computer mit dem Internet verbunden sein. Läuft auf dem Computer ein Virenschutzprogramm, kann es die automatische Aktualisierung blockieren; geben Sie TrikdisConfig in diesem Fall im Virenschutzprogramm frei.

Sie können die Firmware auch selbst aktualisieren – auf eine neuere und bei Bedarf auch auf eine ältere Version. Nach der Aktualisierung bleiben alle Einstellungen des Geräts unverändert.

1. Starten Sie die Software TrikdisConfig und verbinden Sie das Gerät per USB-Kabel, oder öffnen Sie seine Programmierung aus der Ferne.
2. Wenn es eine neuere Firmware gibt, bietet das Programm deren Download an – nehmen Sie ihn an.
3. Wählen Sie die Seite **Firmware** und klicken Sie auf die Schaltfläche **Open firmware**. Wählen Sie die Firmware-Datei aus.
4. Drücken Sie die Schaltfläche **Update [F12]**, warten Sie das Ende der Aktualisierung ab, und klicken Sie dann im Popup-Fenster auf **OK**. Ziehen Sie währenddessen nicht das Kabel ab und unterbrechen Sie die Verbindung nicht.

Die Firmware-Dateien befinden sich im Installationsordner von TrikdisConfig, im Unterordner **Firmwares**, in dem mit dem Gerätenamen bezeichneten Ordner. Gibt es diesen Ordner nicht, dann gibt es entweder keine Aktualisierung dafür, oder die Software TrikdisConfig selbst muss aktualisiert werden. Die neuesten Dateien können Sie als registrierter Benutzer auch von der Website des Herstellers, auf der Seite des Geräts, herunterladen.

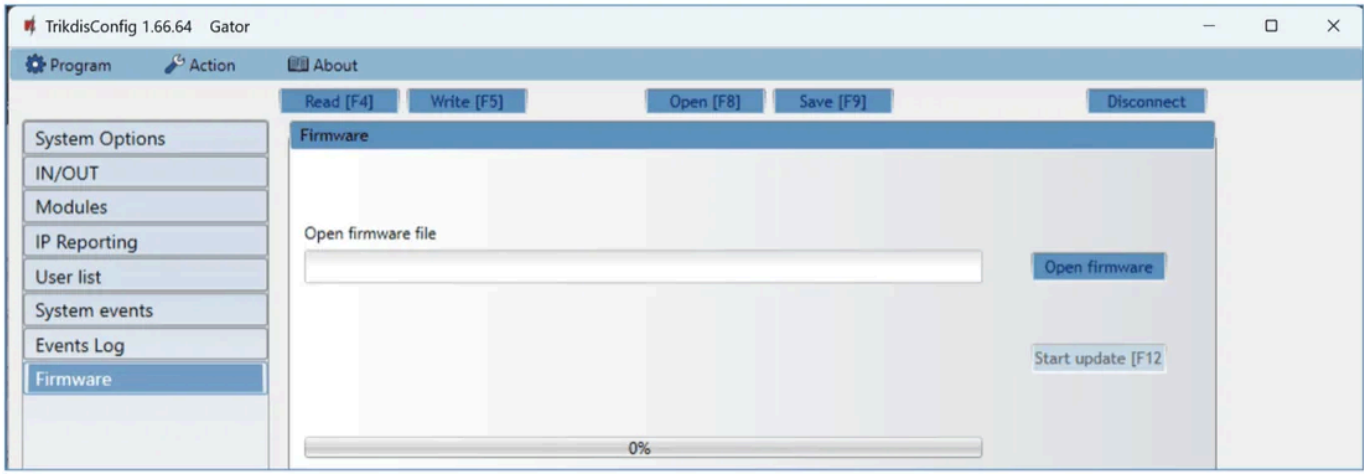


Abbildung 55. TrikdisConfig – GATOR, Seite **Firmware**: die Taste **Open firmware**, das Feld der gewählten Datei, die Taste **Start update [F12]** und die Fortschrittsanzeige.

Beim GATOR heißt die Taste, die die Aktualisierung startet, **Start update [F12]**. Für die Module RF-LORA und iO-LORA ist mindestens Firmware **2.13** erforderlich, für die Module W485 und E485 mindestens **1.06**; die aktuelle Version sehen Sie im Feld **FW** der Statusleiste (Abschnitt 5.1).

9. Fehlersuche und häufige Fragen

Wenn das Gerät nicht tut, was Sie erwarten, sehen Sie sich zuerst die LEDs an (Abschnitt 1.5), danach die folgenden Punkte.

Die LED TROUBLE blinkt – was bedeutet die Anzahl der Blinkimpulse?

Die Anzahl der Blinkimpulse nennt die Fehlerursache: **1** – keine SIM-Karte (oder sie hat keinen Kontakt: nehmen Sie sie heraus und legen Sie sie wieder ein); **2** – der PIN-Code der SIM-Karte ist falsch (schalten Sie die PIN-Abfrage in einem Telefon aus oder geben Sie die richtige PIN im Feld **System Options → SIM card PIN** ein); **3** – keine Verbindung zum Mobilfunknetz möglich (Signalstärke, Antenne, ist die SIM-Karte aktiv, 2G-Karte in einem 4G-Gerät); **4** – keine Verbindung zur Protegus-Cloud oder zum primären IP-Empfänger möglich (mobile Daten auf der SIM, APN, Adresse und Port des Empfängers); **5** – keine Verbindung zum Ersatz-IP-Empfänger möglich; **6** – die interne Uhr ist nicht gestellt (Zeitsynchronisierung, Befehl `TIME`); **7** – die Versorgungsspannung ist nicht in Ordnung.

Ich rufe an, aber der GATOR reagiert nicht

- Leuchtet die LED **NETWORK** nicht grün, ist das Gerät nicht im Netz: Prüfen Sie die SIM-Karte (aktiv, PIN ausgeschaltet, für den Empfang von Anrufen geeignet), die Antenne und die Signalstärke (die Anzahl der gelben Blinkimpulse).
- Wenn Sie bereits Benutzer angelegt haben oder das Kästchen **En** der Zeile **Not authorized** (Nr. 10) leer ist, nimmt das Gerät nur Anrufe von Nummern auf der Liste an – die Nummer des Anrufers muss in der Liste stehen, im internationalen Format (+43…), freigegeben (**En**), mit gültigem Zeitplan und gültiger Gültigkeitsdauer (Abschnitt 5.6).
- Am Telefon des Anrufers darf die Rufnummer nicht unterdrückt sein, sonst kann das Gerät ihn nicht erkennen.
- Prüfen Sie, ob die Nummer nicht auf der Sperrliste steht (Abschnitt 5.6.4).

Auf Anruf öffnet er nicht, aus der App aber schon

Wenn ein W485 oder E485 Modul am Gerät angeschlossen ist, prüfen Sie im Reiter **Modules → Parameters** in der Gruppe **SIM parameters** das Kästchen **Use dial and SMS when working over internet module**: Ist es leer, verwendet das Gerät während der Internetverbindung keine Anrufe und SMS (Abschnitt 5.4). Setzen Sie das Häkchen, wenn auch die Steuerung per Anruf nötig ist.

Während des Anrufs kann ich nicht mit der Telefontastatur steuern

Für die Steuerung per Tastatur (DTMF) muss der Wert **System Options → Hang-up after** größer als 0 sein, sonst weist das Gerät den Anruf sofort ab (Abschnitt 4.2). Bei Geräten mit dem Typcode **GV17_2E70** und **GV17_2S70** funktioniert die DTMF-Steuerung nicht – den Typ zeigt das Feld **Device** der Statusleiste.

Protegus 2 findet das Gerät nicht, oder es wird nicht Online

- Auf der Seite **IP Reporting** muss **Enable cloud service** angehakt sein (per SMS: `CONNECT 123456 PROTEGUS=ON`), und die LED **TROUBLE** darf nicht 4-mal blinken.

- Die SIM-Karte braucht einen mobilen Datendienst, und der APN muss stimmen: Beim Feld **System Options → APN** wählt das Kästchen **Auto** aus der eingebauten Liste; kommt die Verbindung nicht zustande, geben Sie den APN des Anbieters ein (Liste).
- In der App muss die IMEI genau stimmen, und wenn der **Cloud Access Code** nicht der werkseitige `123456` ist, geben Sie den richtigen ein.
- Ist alles in Ordnung, warten Sie nach dem Hinzufügen höchstens 1 Minute (Abschnitt 4.3).

Das Widget funktioniert nicht, oder ich finde es nicht

Das Widget gibt es nur auf **Android**-Telefonen (Abschnitt 4.4); auf dem iPhone öffnen Sie vom Startbildschirm der App aus. Unter Android muss der GATOR zu den Systemen hinzugefügt sein, und Sie müssen angemeldet sein; bleibt das Widget grau, öffnen Sie die App einmal und prüfen Sie die Internetverbindung.

Der RFID-Leser liest die Karte nicht, oder der GATOR reagiert nicht darauf

- Prüfen Sie den Anschluss gemäß der Zeichnung in Abschnitt 3.6 (bei einem Leser **D0 → 1 IN**, **D1 → 2 IN**; beim zweiten Leser **D0 → 3 I/O**, **D1 → 4 I/O**; gemeinsamer Minuspunkt) und die Versorgung des Lesers: Bei einem 12-V-Leser muss der GATOR mit **DC-Versorgung** laufen, bei einem Leser mit 5-V-Signalpegel setzen Sie das Häkchen bei **Low voltage reader**.
- Auf der Seite **IN/OUT** muss **Wiegand reader mode** der Anzahl der Leser entsprechen (**Single** / **Dual**), und **3 I/O**, **4 I/O** dürfen nicht auf eine andere Funktion eingestellt sein.
- Erkennt das Gerät die Signale des Lesers nicht, probieren Sie das Kästchen **Disable reader filter**.
- Die Karte muss in der Tabelle **User list** stehen (registriert oder mit ihrer Nummer eingetragen), freigegeben, mit dem Ausgang des Lesers (Abschnitt 5.6.2). Das Ereignisprotokoll (Abschnitt 5.8) zeigt, ob das Lesen stattgefunden hat und warum es abgelehnt wurde (**Access denied**).

In der App ist der tatsächliche Zustand des Tors nicht zu sehen

Für die Torzustandsanzeige muss der Zustandsausgang des Torantriebs oder der Endschalter des Tors an den Eingang **1 IN** angeschlossen werden (Abschnitt 3.5), auf der Seite **IN/OUT** muss der Typ des Eingangs dem Kontakt entsprechend eingestellt und in der Zeile von **5 OUT** in der Spalte **Assign IN** der Eingang **1 IN** gewählt werden (Abschnitt 5.10). In der App zeigt das Symbol des Ausgangs danach den Zustand des Eingangs.

Das Gerät antwortet nicht auf SMS-Befehle

- SMS-Befehle nimmt es nur von den **Administrator**-Nummern (1A–7A) an; wer als Erster anruft oder eine SMS sendet, wird Administrator. Wenn Sie nicht wissen, wer das ist, lesen Sie die Tabelle **User list** in TrikdisConfig aus.
- Im Befehl muss das Passwort nach dem Befehlswort stehen, mit Leerzeichen (`INFO 123456`); das neue Passwort hat 6 Zeichen.
- Die Antwort-SMS kommt nur, wenn beim Administrator **ACK for SMS message** angehakt ist (Abschnitt 5.6).
- Läuft das Gerät mit einem Internetmodul (W485 / E485) und ist **Use dial and SMS when working over internet module** leer, verarbeitet es SMS während der Internetverbindung nicht (Abschnitt 5.4).

Ich habe das Administratorpasswort vergessen

Das Passwort lässt sich nicht abfragen. Verbinden Sie sich per USB-Kabel mit dem Gerät und stellen Sie die Werkseinstellungen mit der Taste **Restore** unten links im Programmierfenster wieder her (Abschnitt 5.9) – dabei werden die Benutzerliste und alle Einstellungen gelöscht, daher muss das Gerät danach neu eingerichtet

werden. Wenn Sie die Einstellungen früher in einer Datei gespeichert haben (**Save [F9]**), können Sie sie nach dem Zurücksetzen mit der Taste **Open [F8]** laden und müssen nur das Passwort neu eingeben.

Brauche ich eine SIM-Karte, wenn ich ein W485 oder E485 Modul verwende?

Nein: Der GATOR funktioniert mit dem WLAN-Modul W485 oder dem Ethernet-Modul E485 auch ohne SIM-Karte, die Steuerung erfolgt dann aus der App (und mit RFID-Karte), ohne Anruf und SMS. Setzen Sie im Reiter **Modules** → **Parameters** das Häkchen bei **Disable indication of the absence of a SIM card**, damit das Gerät die fehlende Karte nicht als Fehler meldet (Abschnitt 5.4). Wenn Sie auch den Ersatzweg über das Mobilfunknetz möchten, legen Sie eine SIM-Karte ein und lassen Sie das Kästchen **Disable the use of SIM card mobile data** leer.

Ich möchte mehrere Tore von einem Gerät aus steuern

Das eigene Relais des GATOR schaltet ein Tor; die Klemmen **3 I/O** und **4 I/O** können als Open-Collector-Ausgang (50 mA) ein externes Relais ansteuern. Für weit voneinander entfernte Tore lassen sich mit dem Sende-Empfänger **RF-LORA** bis zu 8 drahtlose **iO-LORA** Erweiterungen anschließen, jede mit eigenem Relais, Eingang und RFID-Leser (Abschnitt 3.9); für mehr kabelgebundene Ein- und Ausgänge eine Erweiterung **iO8** oder **iO8-LORA** (Abschnitt 3.10). Bei den Benutzern markieren Sie im Feld **Can control output**, welchen Ausgang sie schalten dürfen.

10. Sicherheitshinweise

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.

- Der GATOR darf nur von Fachpersonal installiert und gewartet werden.
- Lesen Sie vor der Installation diese Anleitung, um Fehler zu vermeiden, die zu Fehlfunktionen oder zu Schäden an den Geräten führen können.
- **Trennen Sie vor jedem elektrischen Anschließen die Versorgungsspannung** – die des GATOR und auch die des Torantriebs.
- Vom Hersteller nicht genehmigte Änderungen, Umbauten oder Reparaturen führen zum Verlust der Garantie.
- Beachten Sie die örtlichen Vorschriften zur Abfallentsorgung: Entsorgen Sie das Gerät und seine Teile nicht mit dem Hausmüll – geben Sie das Altgerät als Elektronikschrott ab.

Siehe auch

- Das Torautomatisierungsgerät GV17 kann mit Protegus 2 verwendet werden – der GATOR und die App zusammen.

- GV17 als Zutrittskontroll- und/oder Arbeitszeiterfassungssystem – RFID-Leser, Ein- und Ausgang, Arbeitszeit in Protegus 2.
- Dual-Path-Kommunikation jetzt auch für den Torantrieb-Controller GV17 GATOR – W485 / E485 Modul für den GATOR.
- Flexible drahtlose Zutrittskontrolle mit dem GATOR RF-LoRa-System – Module RF-LORA und iO-LORA, mehrere Tore in einem System.
- APN-Einstellungen – Liste der europäischen Mobilfunkanbieter – wenn die mobile Datenverbindung nicht zustande kommt.
- Protegus: Android-, iPhone- und Web-App – über die App.
- Englischsprachige Dokumentation: docs.trikdis.com – Cellular gate controller GATOR.

Die Anleitungen auf docs.trikdis.com sind in englischer Sprache.

Passende Produkte

Trikdis GV17 - GATOR smarter 4G GSM / IP Torcontroller

Trikdis GV17 – GATOR Smart 2G GSM / IP Torsteuerung **Trikdis W485 WiFi -Modul (RS485)**

Trikdis E485 Ethernet -Modul (RS485) **Trikdis RF-Lora Wireless Expander-Modul**

Trikdis io-lora Wireless Expander-Modul **Trikdis IO8 Wired Expander Modul**

Trikdis io8-lora Wireless Expander-Modul

Trikdis Ant04 GSM Stick-On-Antenne mit 2,5 m Draht

Trikdis ME301M Magnetantenne mit 2,5 m Draht

Urheberrecht

Diese Anleitung wurde von trikdis.hu und mobilamb.eu erstellt. Text, Aufbau, eigene Abbildungen und Ergänzungen sind unser geistiges Eigentum und urheberrechtlich geschützt. Ohne unsere Erlaubnis darf sie weder ganz noch teilweise kopiert, verbreitet oder auf einer anderen Website veröffentlicht werden. Für die Installation und Nutzung des Produkts darfst du sie frei herunterladen und ausdrucken.

Die Namen und Logos Trikdis und Protegus sind Marken der UAB Trikdis.

Immer aktuelle Version dieser Anleitung: https://trikdis.at/gv17-anleitung