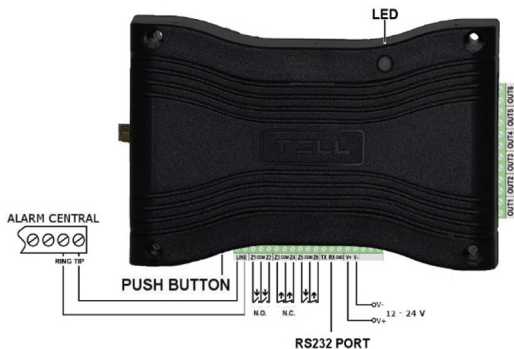


IP Bridge PRO QUICK GUIDE

Dear customer,
Thank you for choosing our product. The full User manual is downloadable from the manufacturer's website:
<https://tell.hu/en/products/qprs-communicators/ip-bridge-pro>



WIRING OF THE MODULE



Connectors from left to right:

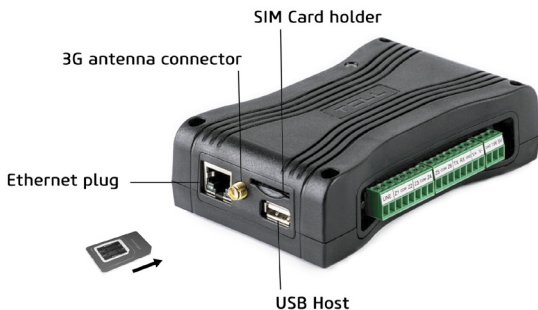
- LINE:** Simulated telephone line for connecting alarm panel
- Z1:** 1. contact input (considered between Z1 and COM)
- COM:** Common terminal between Z1 and Z2 contact inputs
- Z2:** 2. contact input (considered between Z2 and COM)
- Z3:** 3. contact input (considered between Z3 and COM)
- COM:** Common terminal between Z3 and Z4 contact inputs
- Z4:** 4. contact input (considered between Z4 and COM)
- Z5:** 5. contact input (considered between Z5 and COM)

COM:	Common terminal between Z5 and Z6 contact inputs
Z6:	6. contactus input (considered between Z6 and COM)
TX:	RS232 serial port TX
RX:	RS232 serial port RX
GND:	RS232 serial port GND
V+:	Supply voltage 12-24V DC
V-:	Supply voltage negative polarity (GND)

Connect the inputs accordingly to the configured control mode, normally open (N.O.) or normally closed (N.C.).

The device has 6 potential free, normally open (N.O.) relay contacts (OUT1..OUT6 from left to right).

Attention! The maximum loads supported by the outputs is 1A @ 12V DC. In case of higher load or higher voltage please use an external relay!



If the module has a 3G modem, use the 3G antenna connector to wire the **antenna**.

Insert the **SIM card** into the socket until it clicks. To remove, press the card again.

The module's network is configurable through the **USB host**.

Connect the local internet network cable (LAN) coming from the router to the **Ethernet connector** of the IP Bridge.

-> Chapter 3 of the User manual

PUTTING INTO OPERATION

After mounting and connecting the local Internet network, the device can be powered up. Setting up the module can be done from any computer that is connected to the same local network as the device is.

By default the device is delivered with DHCP setting. To detect the IP address assigned by the local router, use the IP Bridge Virtual Client program, which is downloadable from the product page if necessary. If UDP Broadcast service is not allowed on the router, the program is not able to locate the device. In this case you can check the IP address in the router's DHCP list.

If you'd also like to use the device's web interface through the internet, set up on your router the port forwarding of port no. 80 and port no. 443 at the module's IP address.

A text file copied to a USB flash drive can be used to modify the module's network configuration. For details on how to proceed and for the format of the text file see chapter 5.3 of the User Guide.

-> *Chapter 5 of User manual*

WEB INTERFACE

Enter the module's IP address into your browser to open the web interface (e.g: 192.168.1.198) and enter the username and password for login.



In default there are an admin and an additional user in the system. The default login credentials are:

Username / Password: **admin / admin**

Username / Password: **user / user**

Attention! Make sure to change default passwords at your first login. You can do so on the General settings page.















MODULE STATUS

The module displays the module status page after login. In the header you can find the language selector , the view mode selector  and the logout button. In the view mode selector window you can make a backup of your settings or you can also upload a previously saved one.

Attention! The saved configuration file contains sensitive data. Please store it accordingly.

In the header the basic status information is displayed: the module's date/time, current LAN IP address, supply voltage, the module's remote monitoring group ID and device ID and the simulated phone line status. In addition, if the IP Bridge has an extension panel, the mobile internet's IP address, the signal strength in percentage, the IMEI number and the SIM ID are also here.

The input section indicates the current status of the inputs. It is followed by the output section, where the status of the outputs are indicated and the outputs can be also controlled from here. The next section shows the status of connections to the remote monitoring servers. The **Event Log** section lists the last 10 events, which may be events received from the alarm control panel or the internal events of the device. The full event list (maximum 500 events) is available with the **More events** button.

The **Event Log** shows the date and time of the event, CID code, the status of reporting to a monitoring station (1-6), the status of VOIP notifications (1-4), the status of SMS notifications (1-4), the status of saving camera images (), the status of email sending (@), the status of uploading camera images to FTP (), the status of displaying event in TMS (), the status of relay control () and the status of push notification sending (1-4). You can also check the camera images recorded in association with the event  and the details of Settings changed events .

GENERAL SETTINGS

On the *General* tab of *Settings* menu, you can change the settings of communication and operation.

Some of the most important features are:

Users: You can change the username and password of both user levels here. And also the RADIUS server needed to add and manage additional users can be added here.

Account ID and TEX ID: The identifier for reporting to remote monitoring stations can be added here.

Ping servers: To monitor the internal and external network, you can configure 2-2 ping servers. If the module has an extension panel, you can add 2 additional servers to monitor the mobile internet.

Battery: If the supply voltage falls below the alarm threshold for at least 30 seconds, *Battery fault* internal event is generated. If the supply voltage returns above the restore threshold for at least 30 seconds *Battery restore* internal event is generated.

FTP/SFTP: The device can upload the camera images captured at the time of the alarm to the server provided here. To do this, enter the server's IP address. If needed, add the port number separated by a colon (e.g. 192.168.1.1:8181). If necessary, specify the path of the image folder, as well as the username and password.

TMS server: In addition to contact ID messages, the device can also forward the captured camera images and live URLs to the TMS server set up here.

Update server: If the Firmware update server is not set, in default the module downloads the firmware update from the server provided by the manufacturer, but you can add a different server as well.

Firmware update: Notification about the new firmware update will be sent to the email addresses set here. You can set when to check if there is a new update and you can choose how to download and install the update manually or automatically.

Default settings: The device settings will reset to the factory settings, but the current firmware version won't change.

For further details on the settings described above and other options see chapter 6.2 of the **User manual**.

SERVERS

To report events to a monitoring station you need to create server groups. These server groups can be assigned to events you want to report. To do so, first add up to 6 monitoring servers, then create up to 6 groups from the servers.

To add a **Server** enter a name, the IP address or domain name of the server, the port number, select the network and the receiver's type and set the testing details. If the module doesn't have an extension panel the only option is LAN and the network selector is not displayed. In case of a SIA IP receiver the AES key can be set.

To add a server group, give it a name, then create a group from the previously added servers and mark the primary ones. The device attempts to report the events to each primary server at least once. If the event is not reported to at least one primary server within 10 minutes, the device attempts to report it to the backup servers. If reporting to one of the backup servers succeeded, the device won't report the event to the others.

-> Chapter 6.3. of User manual

CAMERAS

By clicking the Cameras menu, IP Bridge automatically finds and lists IP cameras that support the ONVIF recommendation and are connected to the same network.

If the password-free connection to the IP camera is enabled, the device lists the profiles that are set in the camera, which can be checked by clicking the **Profile dependent parameters**. Otherwise you can add the username and password for login, and also the ONVIF port on which the IP Bridge can communicate with the camera.

The profiles can be added to the camera list with the **Add to list** button, but you can also add camera manually by entering its URL. To do this, press the **View/edit** button in the **Added cameras** section. A camera with external address can cause high data traffic.

Attention! Depending on the camera resolution, the SD card may be full after 5-10 thousand events for which camera recording is required. In this case, the device can not store additional camera images until the previously recorded images are deleted. You can do this in the Cameras menu.

-> Chapter 6.4. User manual

MOBILE APPLICATION

The IP Bridge is able to send Push message due to an event, and the status of the inputs can be checked and also controlled through the mobile application. The **TELL Control Center** is available in the App Store and in the Play Store.

First enable this service on the **Mobile application** tab, then set the IP address and port of the server used for Push sending and then select the network type and backup network type. In default the server setting fields are filled with the data of manufacturer's server reserved for this purpose, and the network is the **Default network** set on the **General** tab.

Server IP: 54.75.242.103

Port: 2020



4 mobile devices can be registered for the module. Each slot has a unique identifier that can be displayed by clicking the QR code button at the end of the line. In the mobile application you can register a device into the module by scanning the QR code of the given slot. After the registration the mobile application's ID and the mobile device's name are listed here.

-> *Chapter 6.6 of the User manual*

EVENT SETTINGS

Internal and external events of the module can be configured on the **Events** tab of **Settings** menu item. You can add unique names to the events, that appear in the event log and reports. The names of the inputs are also displayed in the status menu.

External events: Up to 20 external events can be set in the module, which are Contact ID events received on the simulated phone line. This can be done with the **Add more** button at the bottom of the Events page. The event settings are divided into 8 groups, and you can switch between them by the arrows in the header of the table.

Input properties

Input type: according to the wiring NO (normally open) or NC (normally closed)

EOL: This option enables tamper protection on the given input.

Sensitivity (ms): The status change of the given zone input is ignored if it is shorter than the value set here.

Bypass: Bypassed events are not generated.

Notify next: By selecting this checkbox the next event will be generated even if the CID code corresponds to this event.


Event codes

Each internal event can be associated with a Contact ID code, but the CID code, partition and zone can also be modified.

Monitoring station settings

To report an event to a remote monitoring station, you need to **Enable reporting**, and select the **Server group** that you want to report the events Contact ID code to. Reporting to TMS should be enabled separately.

E-mail settings

You can set up email notification about the events here. The recipient list, subject and email body are editable by clicking the  icon. To add multiple addresses separate them by comma.

Camera settings


The cameras already added to the module can be assigned with the events here. If an event occurs, the last 5 images recorded by the camera which is assigned to the given event are sent via e-mail, or uploaded to FTP/SFTP server or forwarded to TMS.

VOIP (SIP) settings

V1-V4 columns indicate the phone numbers specified in the **Voice call** section of **VOIP** menu. You can choose which of these you want to be notified when the event occurs. In the **Acknowledgement** column you can select the acknowledgement type (no ack/ with * button/ ack. upon call reject). In each case, the reporting to other phone numbers


can be stopped by pressing the # button. In case of **Ack. upon call reject** option accepting the call also confirms the event automatically and reporting to the further phone numbers can be stopped by pressing the # key on the phone. You can also select the audio file you want to be played during the voice call.

SMS settings

The phone numbers indicated by **SMS1-SMS4** columns can be set in the **SMS** section of **VOIP** menu. The **SMS text** can be edited by pressing the  icon.

Mobile settings

The **MOBIL1-MOBIL4** columns mean the mobile devices listed in the **Mobile application** menu. The message set in the **Push notification text** column will be sent to the selected devices.

With this  icon you can copy all the settings from the first row to all other rows.

For details on events and their settings see chapter 6.7 of the User manual.

REMOTE MODULES

You can add remote IP Bridge modules to your device and use them for transparent serial data transfer or for controlling the remote devices' output. You can add up to 6 remote IP Bridge modules to your device by adding the following data:

Address: The IP address of the device. If the remote module is not on the same network enter the router's IP address and the external port.

Port: The device's https port.

Username and Password: Login credentials to log on to the remote module.

In the **Remote module** field select the remote module you'd like use for serial data transfer. In case of **Remote only** option the device only forwards data received from remote modules to its serial port. This can work with any number of remote modules and they don't even need to be among the associated remote modules.

Connection type: The connection can be continuous or can be configured the way, that the modules connect to each other only for the time of data sending.

Timeout: The module closes the connection if the time specified here has elapsed since sending or receiving the most recent data.

Maximum data delay: The module collects the data received on its serial port. If there's no delay in receiving data, after the amount of time set in this field the module will send the previously collected data to the remote module.

Serial port settings: It need to be set to meet the requirements of the selected connection type.

For further details on remote modules see chapter 6.8 of the User manual. For detailed information on the remote programming of alarm systems, see the Appendix of the User manual.

OUTPUTS

On the **Outputs** tab you can configure the outputs and assign automatic control to them.

Controlling both by internal and external event can be added here. The **Event** can be any of the events listed on the **Events** menu. Select the **Target** and the **Output**. This can be any output of any remote module, that was added on the **Remote modules** tab. The delay of activating the output can be defined in seconds in the **Delay(sec)** field.

The **Output mode** can be selected from the following 4 options:

State change: The event will cause a relay status change.

ON - Timed: The event activates the relay output for the time set in **Time(sec)** field in seconds, then becomes inactive again.

ON - Permanent: The event activates the relay output which remain active until switching off or receiving a status change command.

OFF: The event deactivates the relay output.

Stop: If there are multiple overlapping external events added and the Stop option is checked, the external events that are specified below will not be evaluated.

ROUTER CONTROL

The IP Bridge is capable of monitoring the routers which are on the same network the IP Bridge is connected to. If the module doesn't receive answer from a configured Ping server, it can warm and cold restart the router.

You can select predefined servers from the **Server selector** drop-down

list, in which case the **Pingable server** fields can't be edited. If the Custom option is selected, the pingable servers can be added manually. Please specify servers that can be accessed only through the router you would like to monitor.

Warm restart

Router IP address: If the **Autodetect router IP** option is not selected, you can manually enter the router's IP address.

Connection mode: The module tries to connect to the router via the selected protocol. In addition to the commands you can select from the drop-down menu, you can also specify a unique command, if the selected protocol is SSH.

Router port: This is the router's authentication port.

Username and Password: The username and password for logging into the router.

Number of failed ping attempts for warm restart: How many times to try to ping the router before the module warm restarts the router.

Suspend monitoring after restart: This is the time the module waits before the next ping attempt after the router was restarted, so that the router has enough time to restart.

Cold restart

Remote module: The selected module's selected output will be activated. The **Remote 1-6** options allow you to select from the modules specified in the Remote Modules menu.

Output for router restart: Select the output you want to be activated.

Output activation time: The output status will change for the time given here.

If warm restart is also enabled, you can add the number of unsuccessful warm restarts before cold restarting the router. If only cold restart is enabled, you need to add the number of failed ping attempts before power off and on the router.

Suspend monitoring after restart: This is the time the module waits before the next ping attempt after the router was restarted, so that the router has enough time to restart.

REPORT

The module can send an email about its internal and external events. The frequency and time of sending can be edited in the **Report frequency** field. If the number of events reaches 250, the module sends the event report regardless the frequency.

In the **E-mail addresses** field you can add multiple addresses separated by comma. In the **Events** field you can select which kind of events you want to be listed in the report.

OTHER IMPORTANT INFORMATION

Stopping the module:

To properly switch off the IP Bridge module, keep the microswitch on the module pressed for 2-5 seconds, until the LED turns orange, then release it. When the LED doesn't lit anymore, you can disconnect the power supply.

Restoring factory default settings:

To reset the factory default settings, can be done with the Factory reset button in the General Settings menu or with the button on the module. In the second case, press and hold the button on the module for 8 seconds. The LED is lit orange first then turns red. The module restores the factory default settings then restarts automatically.

Attention! During restore, also the network setting will be reset to the default DHCP.

S.M.A.R.T info:

The SD card's S.M.A.R.T info is displayed on the S.M.A.R.T menu. This works properly only with APACER cards.

LED signals:

Red:	Booting/shutdown in progress
Green:	The system is ready
Orange:	An error occurred/ On/Off is in progress

Technical specification:

<i>Supply voltage:</i>	12-24V DC
<i>Nominal current consumption:</i>	520mA @ 12V DC
<i>Maximum current consumption:</i>	700mA @ 12V DC
<i>Operation temperature:</i>	-20°C - +70°C
<i>Maximum relay output load:</i>	1A @ 12V DC
<i>Dimensions:</i>	130 x 69 x 19 mm
<i>Weight:</i>	200g (packed: 300g)

Generated telephone line specification:

<i>Line voltage:</i>	48 V
<i>Line current:</i>	20 mA
<i>Line impedance:</i>	600 Ohm
<i>Ringng voltage:</i>	±50V (20 Hz)
<i>Dial tone:</i>	425 Hz

**SAFETY INSTRUCTIONS**

***For your safety, please read carefully and follow the instructions below!
Failure to observe safety instructions may be a threat to you and your environment!***

TELL's product (*hereinafter referred to as „device”*) has a built-in mobile communication modem. Depending on the product version, the built-in modem is capable of 2G, 3G or 4G mobile communication.

The 2G modem can use the following frequency bands:

850/900/1800/1900 MHz @GSM/GPRS

The 3G modem can use the following frequency bands: 900/2100 MHz

@UMTS, 900/1800 @GSM/GPRS

The 3GA modem can use the following frequency bands:

800/850/900/1900/2100 MHz @UMTS, 850/900/1800/1900 MHz @GSM

The 4G modem can use the following frequency bands: 900/1800

MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE

The 4GA modem can use the following frequency bands: B2/B4/B5@

WCDMA, B2/B4/B5/B12/B13@LTE

- **DO NOT USE** the device in an environment where radiofrequency radiation can cause a risk and may interfere with other devices, that may cause undesired operation - such as medical devices!
- **DO NOT USE** the device if there's a risk of high humidity, hazardous chemicals or other physical impact!
- **DO NOT USE** the device beyond the specified operating temperature range!
- **DO NOT MOUNT** the device in hazardous environment!
- **DO NOT INSTALL/WIRE** the device under voltage. For easy disconnection, the device's adapter or power supply should be easily accessible!

- **ALWAYS DISCONNECT** the power supply before starting to mount the device!
- **ALWAYS DISCONNECT** the device's power supply before inserting, removing or replacing the SIM card!
- **TO SWITCH OFF** the device disconnect all power sources, including power supply and USB.
- The computer connected to the device must **always be connected to the protective ground!**
- **DO NOT USE** a computer to program the device that is not connected to the protective ground. To avoid ground looping, the power supply of the computer and the device must use the same grounding!

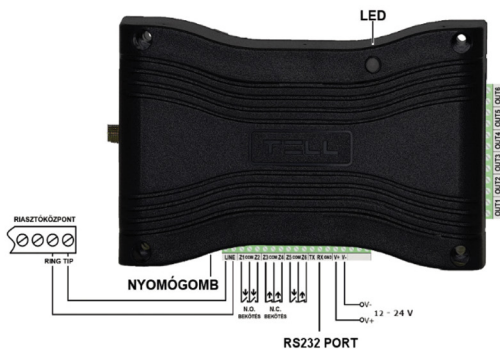
IP Bridge PRO GYORSTELEPÍTÉSI ÚTMUTATÓ

Tisztelt Vásárlónk!

Köszönjük, hogy megvásárolta termékünket! A teljes Használati útmutató letölthető a gyártó weboldaláról:
<https://tell.hu/hu/termek/gprs-kommunikatorok/ip-bridge-pro>



A MODUL BEKÖTÉSE



Csatlakozók sorrendben balról-jobbra:

- LINE:** Szimulált telefonvonal riasztóközpont illesztéshez
- Z1:** 1. kontaktus bemenet (Z1 és COM között értendő)
- COM:** Z1 és Z2 kontaktus bemenetek közös pontja
- Z2:** 2. kontaktus bemenet (Z2 és COM között értendő)
- Z3:** 3. kontaktus bemenet (Z3 és COM között értendő)
- COM:** Z3 és Z4 kontaktus bemenetek közös pontja
- Z4:** 4. kontaktus bemenet (Z4 és COM között értendő)
- Z5:** 5. kontaktus bemenet (Z5 és COM között értendő)
- COM:** Z5 és Z6 kontaktus bemenetek közös pontja

Z6:	6. kontaktus bemenet (Z6 és COM között értendő)
TX:	RS232 soros port TX
RX:	RS232 soros port RX
GND:	RS232 soros port GND
V+:	Tápfeszültség 12-24V DC
V-:	Tápfeszültség negatív pólusa (GND)

A kontaktus bemeneteket a beállításaiknak megfelelően alaphelyzetben nyitott (N.O.) vagy alaphelyzetben zárt (N.C.) formában kösse be. Az eszköz 6 darab potenciálmentes, alaphelyzetben nyitott (N.O.) relé kontaktus kimenettel rendelkezik (balról-jobbra OUT1..OUT6).

Figyelem! A kimenetek maximális terhelhetősége kimenetenként 1A @ 12V DC. Nagyobb terhelés vagy magasabb feszültség esetén használjon külső relét!



Amennyiben a modul rendelkezik 3G modemmel, csatlakoztathat **antennát**. A **SIM kártyát** kattanásig nyomja be a foglalatba. Eltávolításhoz nyomja meg ismételten a kártyát.

Az **USB hoston** keresztül módosíthatja a modul hálózati konfigurációját. A routertől érkező helyi internet hálózati kábelt (LAN) csatlakoztassa az **Ethernet csatlakozóhoz**.

-> Felhasználói útmutató 3. fejezet

A MODUL BEÜZEMELÉSE

A bekötés és a helyi internet hálózat csatlakoztatását követően a modul tápfeszültség alá helyezhető. A beállítást a modullal azonos hálózaton lévő számítógép segítségével végezheti el.

A modul alapértelmezetten DHCP beállítással kerül szállításra. A helyi router által kiosztott IP cím felderítéséhez szükség esetén használja a termék oldaláról letölthető IP Bridge Virtual Client programot. Amennyiben a routerben nem engedélyezett az UDP Broadcast szolgáltatás, a program nem tudja felderíteni a modult, és ebben az esetben a router DHCP listájában található meg az IP címet.

Amennyiben interneten keresztül is szeretné elérni a modult, állítsa be a routerén a 80-as és 443-as portra a port átirányítást a modul IP címére.

Egy pendrive-ra másolt szövegfájl segítségével módosítható a modul hálózati konfigurációja. Ennek menete és a szövegfájl formátumának részletei megtalálható a felhasználói útmutató 5.3-as pontjában.

-> *Felhasználói útmutató 5. fejezet*

WEBES FELÜLET

A webes felület megnyitásához írja be a modul IP címét (pl: 192.168.1.198) egy böngészőbe, majd adja meg a felhasználónevet és jelszót.



Alapértelmezetten egy adminisztrátor és egy további felhasználó van a rendszerben. A belépési adatok a következők:

Felhasználónév / Jelszó: **admin / admin**

Felhasználónév / Jelszó: **user / user**

Figyelem! Az első bejelentkezéskor az alapértelmezett jelszavakat feltétlenül változtassa meg. Ezt az Általános beállítások oldalon teheti meg.

MODUL ÁLLAPOT

A modul a belépést követően az állapot oldalt jeleníti meg. A legfelső sávban a nyelvválasztó , a felületnézet választó  és a kijelentkezés

kapott helyet. A felületnézet ablakban van lehetőség biztonsági mentést készíteni a beállításokról, illetve korábban kimentett beállításokat visszatölteni.

Figyelem! A kimentett konfigurációs állomány érzékeny adatokat tartalmaz. Kérjük, ennek megfelelően tárolja!

A fejlécben kerülnek megjelenítésre az alapvető állapotinformációk: a modul dátum/idő, aktuális LAN IP cím, a tápfeszültség értéke, a modul távfelügyeleti csoportkódja és eszközzazonosítója, valamint a szimulált telefonvonal állapota. Ezen kívül, ha rendelkezik kiegészítő panellel, a mobilinternet IP címét, a mobilinternet térerő értékét százalékos értékben, az IMEI számot és a SIM azonosítót kijelzi.

A zónabemenetek aktuális állapotát mutató **Bemenetek** szekciót a kimenetek állapotát jelző **Kimenetek** szekció követi, ahonnan vezérelhetők is a kimenetek. Ezt követi a vevőegységekkel való kapcsolat állapotát mutató **Szerverek** szekció. Végül pedig az **Eseménynapló** következik, amely a riasztóközponttól átvett és a modul saját eseményeit tartalmazó napló utolsó 10 bejegyzését listázza. A **További események...** gomb segítségével a teljes napló (max. 500 esemény) elérhető.

Az **eseménynapló** mutatja az esemény keletkezésének időpontját és dátumát, CID kódot, a távfelügyeleti szerverre való bejelzés állapotát (☐1–☐6), VOIP értesítések állapotát (☎1–☎4), SMS értesítések állapotát (☎1–☎4), kameraképek mentésének állapotát (📷), emailküldés állapotát (@), kameraképek FTP-re töltésének állapotát (📁), TMS rendszerben való megjelenítés állapotát (📺), relévezérlés állapotát (↔) valamint a push kiértesítések állapotát (☐1–☐4). Lehetőség van továbbá megnézni az eseményhez tartozó kameraképeket 📷 illetve a Beállítások módosítása típusú események további részleteit (?)

-> Felhasználói útmutató 6.1. fejezet

ÁLTALÁNOS BEÁLLÍTÁSOK

A **Beállítások** menüpont **Általános** fülén a kommunikációhoz és az üzemeltetéshez szükséges beállításokat módosíthatjuk.

Néhány fontosabb beállítás a teljesség igénye nélkül:

Felhasználók: A két alapértelmezett felhasználói szint felhasználónevét

és jelszavát itt lehet módosítani, valamint a további felhasználók hozzáadásához és kezeléséhez szükséges RADIUS szerver elérését is itt lehet megadni.

Ügyfélazonosító és TEX azonosító: A távfelügyeleti átjelzéshez szükséges azonosítókat itt adhatja meg.

Ping szerverek: A külső és belső hálózat ellenőrzéséhez 2-2 ping szervert állíthatunk be. Ha az eszköz rendelkezik kiegészítő panellel, akkor a mobilinternet ellenőrzéséhez további kettőt.

Tápfeszültség figyelés: Ha a tápfeszültség az alsó küszöb alá csökken minimum 30 mp-re, **Akkumulátor hiba** belső esemény generálódik, ha a tápfeszültség értéke meghaladja a visszaállási értéket minimum 30 mp-ig, akkor **Akkumulátor hiba visszaállítás** belső esemény generálódik.

FTP/SFTP: A riasztáskor rögzített kameraképeket tudja az itt megadott szerverre felszinkronizálni. Ehhez adja meg a szerver IP címét. A portot kettősponttal elválasztva írja mögé (pl: 192.168.1.1:8181). Amennyiben szükséges, a könyvtárszerkezet útvonalát, valamint felhasználónevet és jelszót is megadhat itt.

TMS szerver: Az eszköz képes a Contact ID üzeneteken túl a riasztáskor rögzített kameraképek és az élő URL továbbítására is az itt beállított TMS szerver felé.

Frissítési szerver: Alapértelmezetten a gyártó szerveréről tölti le a frissítéseket, de itt beállítható ettől eltérő szerver is.

Firmware frissítés: Az itt megadott e-mail címekre érkezik értesítés, ha új frissítés érhető el. Beállítható, hogy mikor ellenőrizze, hogy van-e új, illetve szabályozható, hogy manuálisan vagy automatikusan szeretnének letölteni és telepíteni a frissítést.

Alapértelmezett beállítások: Az eszköz beállításai visszaállnak a gyári beállításokra, de a firmware aktuális verziója megmarad

A fenti beállításokról és további lehetőségekről részletesebben olvashat a **Használati útmutató 6.2-es** fejezetében.

SZERVEREK

Az események távfelügyeletre történő bejelzéséhez szervercsoportot kell létrehoznia. A későbbiekben ezeket a szervercsoportokat tudja a bejelezni kívánt eseményhez rendelni. Ehhez először vigye fel a távfelügyeleti szervereket (max 6 db), majd hozzon létre csoportokat (max 6 db) a szerverekből.

Szerver hozzáadásához adjon meg egy tetszőleges nevet, a szerver IP címét vagy domain nevét, a portot, válassza ki a kommunikációs csatornát és a vevő típusát, valamint állítsa be az életjelküldést. Ha nincs kiegészítő panel a modulhoz, akkor a LAN az egyetlen lehetőség és nem jelenik meg a hálózattválasztó. SIA IP típusú vevő esetében megadható AES kulcs.

Szervercsoport hozzáadásához adjon meg egy tetszőleges nevet, majd a felvitt szerverekből állítsa össze a csoportot és jelölje meg az elsődlegeseket. Minden elsődleges szerverre legalább egyszer megpróbálja majd bejelezni az eseményt. Ha 10 perc próbálkozás után nem sikerült egy elsődlegesre sem bejelezni, csak akkor próbálkozik a tartalék szerverekkel. Ha már egy tartalékra sikerült az átjelzés a többire nem küldi el.

-> *Felhasználói útmutató 6.3. fejezet*

KAMERÁK

Az IP Bridge automatikusan megkeresi a vele azonos hálózaton lévő ONVIF ajánlást támogató kamerákat és kilistázza a Kamerák menüpontban.

Ha a kamerában engedélyezett a jelszó nélküli csatlakozás, kilistázza a kamerában beállított profilokat. Ezeket a **Profilfüggő paraméterek** gomb megnyomásával tekintheti meg. Ellenkező esetben szintén itt lehet megadni a belépéshez szükséges felhasználónevet és jelszót, valamint az ONVIF portot, amin keresztül az IP Bridge kommunikálni tud a kamerával.

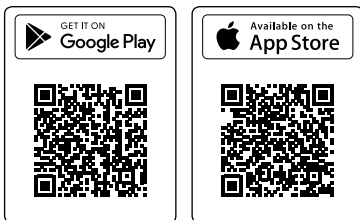
A kilistázott profilokat hozzáadhatja a kameralistához a **Listához ad** gomb megnyomásával. A listához manuálisan is hozzáadhat kamerát az URL-je megadásával. Ehhez nyomja meg a **Hozzáadott kamerák listája** táblázatban található **Megjelenítés/szerkesztés** gombot. Külső címről meghívatkozott kamera esetében azonban számolni kell nagy adatforgalommal.

Figyelem! A kamera felbontásától függően 5-10 ezer kamerakép rögzítést igénylő esemény után az SD kártya betelhet. Ebben az esetben az eszköz nem tud további kameraképeket tárolni, amíg a korábban rögzített képek nem kerülnek törlésre. Ezt a Kamerák menüpontban tudja megtenni.

-> *Felhasználói útmutató 6.4. fejezet*

MOBILALKALMAZÁS

Az IP Bridge képes események hatására push üzenetet küldeni, illetve a hozzá fejlesztett mobilalkalmazásból ellenőrizhető a bemenetek állapota és vezérelhetőek a kimenetei. A **TELL Control Center** alkalmazás elérhető az App Storeban és a Play áruházban is.



Első lépésben a **Mobilalkalmazás** oldalon engedélyezni kell ezt a szolgáltatást és be kell állítani a Push küldéshez szükséges szerver IP címét, portját valamint ki kell választani, hogy az eszköz milyen kommunikációs csatornán csatlakozzon hozzá és legyen-e tartalék hálózat. Alapesetben ezek a beállítások a gyártó erre a célra fenntartott szerverének adatait tartalmazzák. A hálózat pedig az **Általános** oldalon beállított **Alapértelmezett hálózat**.

Szerver IP: 54.75.242.103

Port: 2020

Az IP Bridgehez 4db mobilkészíték regisztrálható. Minden slotnak külön azonosítója van, amit a sor végén található QR kód gomb megnyomásával jeleníthetünk meg. A mobilalkalmazásban eszköz hozzáadásakor az adott slot QR kódját beolvasva lehet az eszközt beregisztálni a modulba. Ilyenkor megjelenik a mobilalkalmazás azonosítója, illetve a mobilkészíték neve.

-> *Felhasználói útmutató 6.6 fejezet*

ESEMÉNYEK BEÁLLÍTÁSAI

Az Események menüpontban a modul belső és külső eseményei egyaránt konfigurálhatóak. Az eseményeknek egyedi név adható, ami megjelenik az eseménynaplóban és a riportokban. Illetve a bemenetek nevei az állapot menüpontban is megjelennek.

Külső esemény: A modulba a belső eseményeken túl maximum 20 db külső esemény is beállítható, ami a szimulált vonalról érkező Contact ID eseményeket jelenti. Ezt a táblázat alján található **Hozzáadás** gombbal teheti meg.

Az események beállításai 8 csoportra vannak osztva, ezek közt a táblázat fejlécében található nyilakkal lehet váltani.

Bemenet beállítások

Bemenet típusa: a bekötésnek megfelelően NO (alaphelyzetben nyitott) vagy NC (alaphelyzetben zárt)

EOL: Ezzel a beállítással engedélyezhető a szabotázsvédelem az adott bemeneten.

Érzékenység (ms): Az itt beállított időnél rövidebb állapotváltozásokat az adott zónabemeneten nem veszi figyelembe.

Kiiktat: A kiiktatott események nem generálódnak le.

Következő értesítése: Ezzel engedélyezhető, hogy akkor is értékelje ki a következő külső eseményt is, ha erre is illeszkedik a CID kód.


Eseménykódok

Minden belső eseményhez alapbeállításként tartozik egy Contact ID kód, de a CID kód, Partíció és Zóna mezők értéke is átírható.

Távfelügyelet beállítások

Esemény távfelügyeletre történő bejelzéséhez engedélyezni kell a bejelzést és a **Szerverek** oldalon létrehozott szervercsoportokból ki kell választani, hova szeretnénk bejelezni az esemény Contact ID kódját.

E-mail beállítások

Esemény bekövetkeztéről itt lehet beállítani e-mail értesítőt. A szerkesztés  ikont megnyomva szerkeszthető a címzettek listája, az üzenet tárgya és szövege. Az e-mail címeket vesszővel elválasztva kell megadni.

Kamera beállítások


A kamera beállítások menüben a modulban beállított kamerákat lehet eseményekhez rendelni. Ha az esemény bekövetkezik, akkor a modul a hozzárendelt kamera utolsó 5 képét küldi a megfelelő e-mail címre, vagy tölti fel egy FTP/SFTP szerverre, vagy továbbítja a TMS szerver felé.

VOIP (SIP) beállítások

A **V1-V4** oszlopok a **VOIP** menüpont **Hanghívás** részében megadott telefonszámokat jelzik, ezek közül lehet választani, hogy az adott esemény bekövetkeztekor melyik számokat értesítse a modul. A **Nyugtázás** osz-


lopban választható a nyugtázás módja (nem kell / * gombbal / híváselutasítással). További műveleteket leállítani minden esetben a # gomb megnyomásával lehet. **Híváselutasítás nyugtáz** opciónál a hívás fogadása is nyugtáz, de ebben az esetben szintén le lehet állítani a további értesítéseket a # gomb segítségével. Kiválasztható a kiértéskor lejátszandó hangüzenet is.

SMS beállítások

Az SMS1-SMS4 oszlopokhoz tartozó telefonszámokat a VOIP menüpont SMS szekciójában lehet beállítani. A küldendő SMS szövege pedig a  ikonnal szerkeszthető.

Mobil beállítások

A MOBIL1-MOBIL4 oszlopok a Mobilalkalmazás menüpontban listázott mobilkészüléket jelentik. A kiválasztott eszközökre megy ki a Push üzenet szöveg oszlopban beállított értesítés.

Az  ikon segítségével az első sorban megadott értékeket átmásolhatja az összes további eseményre is.

Az eseményekről és beállításairól részletesebben olvashat a Használati útmutató 6.5 fejezetében olvashat.

TÁVOLI MODULOK

Az eszközhöz távoli IP Bridge modulok rendelhetők, aminek segítségével transzparens soros adatátvitel valósítható meg vagy a távoli modulok kimenetei vezérelhetők automatikusan. A modulhoz 6 darab távoli IP Bridge rendelhető az alábbi adatok megadásával.

Távoli eszköz címe: Az eszköz IP címe. Ha nem azonos hálózaton van a két eszköz, a router IP címét kell beírni és a külső portot.

Port: Az adott eszköz https portja.

Felhasználónév és Jelszó: A távoli eszközre való bejelentkezéshez szükséges adatok.

A hozzáadott IP Bridge modulokból választható ki a **Távoli modul** mezőben, hogy melyikkel jöjjön létre a soros adatátvitel. A **csak fogadás** opció esetén az IP Bridge csak fogadja a távoli moduloktól az adatokat és továbbítja a soros portjára. Ebben az esetben tetszőleges számú modultól tud adatot fogadni és azokat hozzá se kell adni a fenti listához.

Kapcsolat típusa: Lehet folyamatos, illetve úgy is beállítható, hogy csak a küldés idejére kapcsolódjanak egymáshoz a modulok.

Időtűllépés: A modul bontja a kapcsolatot, ha az itt megadott idő eltelt a legutóbbi adat küldése vagy fogadása óta.

Maximális adatkésleltetés: A modul folyamatosan gyűjti a soros portján érkező adatokat. Ha nincs az adatfogadásban szünet, az itt megadott idő letelte után mindenképp elküldi az addig fogadott adatokat a hozzárendelt távoli modulnak.

Soros port beállítások: A kapcsolat típusának megfelelően kell beállítani. A távoli modulokkal kapcsolatosan további információkat talál a Használati útmutató 6.8 fejezetében. A riasztórendszerek távprogramozásával kapcsolatos részletes információkat pedig a Használati útmutató Mellékletében találja.

KIMENETEK

A **Kimenetek** menüben lehet a kimeneteket konfigurálni, illetve automatikus vezérléseket hozzájuk rendelni.

Belső és külső esemény általi vezérlést is itt adhatunk hozzá. A **Vezérlő esemény** tetszőleges esemény lehet, ami szerepel az **Események beállítása** menüpontban. Válassza ki a **Vezérlendő modult** és **Kimenetet**. Ez lehet az adott modul bármelyik kimenete, vagy a **Távoli modulok** menüben hozzáadottak bármelyike. A kimenet aktiválása késleltethető a **Késleltetés** mezőben megadott másodperccel.

A **Kimenetvezérlés módja** négyféle lehet:

Állapotváltás: Az esemény hatására az adott relé állapotot vált.

BE-Időzített: Esemény hatására az Időzítés oszlopban megadott időtartamra aktívvá válik, majd inaktívra vált.

BE-Tartós: A kimenet aktívra vált és az is marad, a következő kikapcsolás vagy állapotváltás eseményig.

Ki: Az adott kimenet inaktívra vált.

Megáll: Ha több egymást fedő külső eseményt vittünk fel és ezt a mezőt bejelöli, a következőnek megadott külső esemény nem értékelődik ki.

ROUTER FELÜGYELET

Az IP Bridge képes a vele egy hálózaton lévő routerek felügyeletét ellátni. Amennyiben nem kap választ a beállított Ping szerverektől, szoftveresen és/vagy hardveresen újra tudja indítani a routert.

A **Szerver választó** listából lehet az előre definiált szerverpárok közül választani, ilyenkor a pingelendő szervereket nem lehet szerkeszteni. Az egyedi opció kiválasztásakor manuálisan adható meg a két

pingelendő szerver. Olyan szervereket kell megadni, amelyeket csak a felügyelendő routeren keresztül képes elérni.

Szoftveres újraindítás

Router IP cím: Választhatunk automatikus felismerést, vagy beírhatjuk manuálisan.

Kapcsolódás módja: A modul a kiválasztott protokollon próbálja elérni a routert. A legördülő menüből kiválasztható parancsokon kívül egyedi parancs is megadható, amennyiben SSH a kiválasztott protokoll.

Router port: A router autentikációs portja.

Felhasználónév és Jelszó: A routerbe való belépéshez szükséges felhasználónév és jelszó.

Router újraindításához szükséges sikertelen pingek száma: Hányszor próbálkozzon pinggel, mielőtt újraindítja a routert.

Ellenőrzés felfüggesztése újraindítás után: Újraindítás után a megadott ideig nem indít ping kérést a szerver felé, hogy a routernek legyen elegendő ideje újraindulni.

Hardveres újraindítás

Távoli modul: A kiválasztott modul kiválasztott kimenete aktiválódik. A Távoli 1-6 opciók a Távoli modulok menüben hozzáadott modulokat jelölik.

Kimenet a router újraindításához: Kiválasztható, hogy a modulnak melyik kimenete aktiválódjon.

Kimenet aktiválás időtartama: Az itt megadott időre vált állapotot.

Amennyiben a szoftveres újraindítás is engedélyezett, megadható, hogy hány sikertelen szoftveres újraindítás után indítsa újra hardveresen a routert. Ha csak hardveres újraindítás engedélyezett, akkor a sikertelen pingek számát kell megadni az újraindítás feltételeként.

Az Ellenőrzés felfüggesztése újraindítás után mezőben megadott ideig nem indít ping kérést a szerver felé, hogy a routernek legyen elegendő ideje újraindulni.

RIPORT

A modul e-mailben ki tudja küldeni a saját belső és külső eseményekről készült riportot. Ennek gyakorisága és pontos ideje a **Jelentés gyakoriság** mezőben szerkeszthető. Ha az események száma eléri a 250-et a beállításoktól függetlenül is elküldi a riportot.

Az E-mail címek mezőben több e-mail cím megadására is lehetőség van, ezeket vesszővel elválasztva adja meg. A riportba bekerülő események szűrhetőek a **Jelentendő eseménycsoportok** beállítással.

EGYÉB FONTOS INFORMÁCIÓK

Modul leállítása:

Szabályos leállításhoz tartsa nyomva a modulon található mikrokapcsolót 2-5 másodpercig, amíg a LED nem vált narancssárgára, majd engedje el. Amint a LED kialszik, lekapcsolhatja a tápfeszültséget.

Gyári beállítások visszaállítása:

A gyári beállítások az általános beállítások menüpontban található gomb, vagy a modulon található nyomógomb segítségével állíthatók vissza. Az utóbbi esetben tartsa nyomva 8 másodpercig a modulon található gombot. A LED narancssárgára vált, majd pirosra. A modul elvégzi a visszaállítást és automatikusan újraindul.

Figyelem! A visszaállítás során a hálózati beállítás is visszaáll az alapértelmezett DHCP-re.

S.M.A.R.T info:

Az SD kártya S.M.A.R.T adatait a S.M.A.R.T menüpontban lehet megtekinteni. Ez a funkció APACER márkájú kártyákkal működik megfelelően.

LED jelzések:

Piros:	Rendszerindítás/rendszerleállítás folyamatban
Zöld:	A rendszer üzemkés
Narancs:	Hiba lépett fel/Be-ki kapcsolás folyamatban van

Technikai specifikáció:

Tápfeszültség:	12-24V DC
Névleges áramfelvétel:	520mA @ 12V DC
Maximális áramfelvétel:	700mA @ 12V DC
Működési hőmérséklet:	-20°C - +70°C
Kimenetek terhelhetősége:	1A @ 12V DC
Méret:	130 x 69 x 19 mm
Súly:	200g (csomagolva: 300g)

Generált telefonvonal specifikáció

Vonali feszültség:	48 V
Vonali áram:	20 mA
Vonali impedancia:	600 Ohm
Csengető feszültség:	±50V (20 Hz)
Tárcsahang:	425 Hz



BIZTONSÁGI UTASÍTÁSOK

Biztonsága érdekében kérjük figyelmesen olvassa végig és kövesse az alábbi utasításokat! A biztonsági utasítások esetleges be nem tartása veszélyt jelenthet Önre és a környezetére is!

A TELL terméke (továbbiakban „eszköz”) beépített mobilkommunikációs modemmel rendelkezik. Termékváltozattól függően, a beépített modem 2G, 3G vagy 4G mobilkommunikációra képes.

A 2G modem az alábbi frekvenciasávokat használhatja:
850/900/1800/1900 MHz @GSM/GPRS

A 3G modem az alábbi frekvenciasávokat használhatja: 900/2100 MHz
@UMTS, 900/1800 @GSM/GPRS

A 3GA modem az alábbi frekvenciasávokat használhatja:
800/850/900/1900/2100 MHz @UMTS, 850/900/1800/1900 MHz @GSM

A 4G modem az alábbi frekvenciasávokat használhatja: 900/1800
MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE

A 4GA modem az alábbi frekvenciasávokat használhatja: B2/B4/B5@WCDMA, B2/B4/B5/B12/B13@LTE

- **NE HASZNÁLJA** az eszközt olyan környezetben, ahol a rádiófrekvenciás sugárzás veszélyt okozhat és egyéb eszközökkel interferencia alakulhat ki, amely megzavarhatja azok működését - például egészségügyi eszközök!
- **NE HASZNÁLJA** az eszközt magas páratartalom vagy veszélyes kemikáliák, vagy egyéb fizikai behatások fennállása esetén!
- **NE HASZNÁLJA** az eszközt a megadott működési hőmérséklettartományon kívül!
- **NE TELEPÍTSE** az eszközt veszélyes környezetben!
- **TILOS** az eszközt feszültség alatt felszerelni / bekötni. A könnyű áramtalaníthatóság érdekében az eszköz hálózati adaptere, vagy tápegysége legyen könnyen elérhető helyen!
- **MINDIG VÁLASSZA LE** az eszközt a tápfeszültségről a felszerelés megkezdése előtt!
- **MINDIG VÁLASSZA LE** az eszközt a tápfeszültségről a SIM kártya behelyezése, eltávolítása vagy cseréje előtt!
- **AZ ESZKÖZ KIKAPCSOLÁSÁHOZ** válassza le az eszközről az összes áramforrást, beleértve a tápfeszültséget és az USB csatlakozást is!
- **AZ ESZKÖZHÖZ CSATLAKOZTATOTT** számítógép minden esetben legyen csatlakoztatva a védőföldhöz!
- **NE HASZNÁLJON** olyan számítógépet az eszköz programozására, amely nincs csatlakoztatva a védőföldhöz. A földhurok elkerülése érdekében a számítógép és az eszköz tápegysége ugyanazon földelést kell, hogy használja!
- **NE PRÓBÁLJA MEGJAVÍTANI** az eszközt. Az eszköz javítását csak szakképzett személy végezheti!
- **BIZTOSÍTSON MEGFELELŐ ÁRAMFORRÁST** az eszköznek! Az eszköz csak olyan tápegység használata esetén működik biztonságosan és megfelelően, amely az eszköz kézikönyvében megadott követelmények maximális értékeit is képes teljesíteni. A pontos adatokat az eszköz kézikönyvében és a <http://tell.hu> weboldalon is megtalálja.

- **NE HASZNÁLJA** az eszközt olyan tápegységgel, amely nem felel meg az MSZ EN 60950-1 szabványnak!
- **NE CSERÉLJE FEL** a tápfeszültség polaritását! A tápfeszültséget minden esetben az eszközön jelölt polaritásnak megfelelően kösse be!
- **NE CSATLAKOZTASSA** a GSM antenna csatlakozóját a védőföldhöz. A GSM antenna csatlakozójának fémes részeit és a modul termináljait se közvetlenül, se közvetve **NE** csatlakoztassa a védőföldhöz, mert ez a modul meghibásodását okozhatja!
- **FIGYELEM!** A termék automatikus tápfeszültség-leválasztás (Under Voltage Lock Out) funkcióval rendelkezik. Terméktípustól függően, amennyiben a tápfeszültség 8,4...8,2V alá csökken, a modul automatikusan kikapcsol. A modul ismét csak 11,2...11,4V-os tápfeszültség-szintnél kapcsol be.

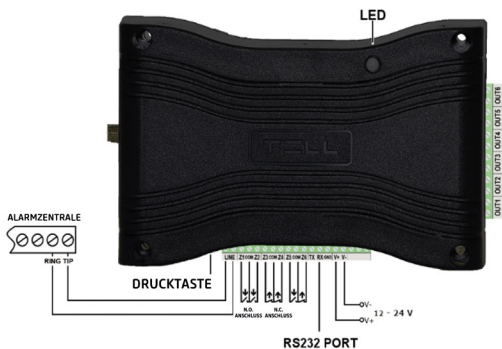
IP Bridge PRO SCHNELLINSTALLIERUNGSANWEISUNG

Sehr geehrter Kunde,

Wir bedanken uns für den Kauf unseres Produktes! Die vollständige **Gebrauchsanweisung** kann von der Webseite des Herstellers heruntergeladen werden: <https://tell.hu/de/produkte/gprs-communicators/ip-bridge-pro>



ANSCHLUSS DES MODULS



Reihenfolge der Anschlüsse von links nach rechts:

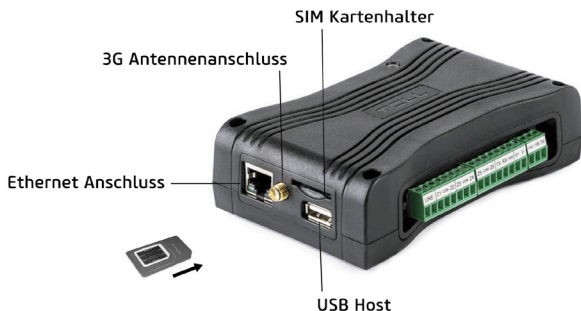
- LINE:** Simulierte Telefonleitung zur Anpassung der Alarmzentrale
- Z1:** Eingang des 1. Kontakts (gilt zwischen Z1 und COM)
- COM:** Gemeinsamer Punkt zwischen den Kontakten Z1 und Z2
- Z2:** Eingang des 2. Kontakts (gilt zwischen Z2 und COM)
- Z3:** Eingang des 3. Kontakts (gilt zwischen Z3 und COM)
- COM:** Gemeinsamer Punkt zwischen den Kontakten Z3 und Z4
- Z4:** Eingang des 4. Kontakts (gilt zwischen Z4 und COM)
- Z5:** Eingang des 5. Kontakts (gilt zwischen Z5 und COM)

COM:	Gemeinsamer Punkt zwischen den Kontakten Z5 und Z6
Z6:	Eingang des 6. Kontakts (gilt zwischen Z6 und COM)
TX:	Serielle Schnittstelle TX RS232
RX:	Serielle Schnittstelle RX RS232
GND:	Serielle Schnittstelle GND RS232
V+:	Speisespannung 12-24V DC
V-:	Speisespannung Negativpol (GND)

Die Kontakteingänge schließen Sie anhand ihrer Einstellungen im geöffneten Zustand in der Grundstellung (NO) oder im geschlossenen Zustand in der Grundstellung (NC) an.

Das Gerät verfügt über 6 Stück potentialfreien, in der Grundstellung geöffneten Ausgänge (NO) für die Relaiskontakte (von links nach rechts OUT1...OUT6).

Achtung! Maximale Belastbarkeit der Ausgänge pro Ausgang: 1A @ 12V DC. Bei größerer Belastung oder höherer Spannung benutzen Sie ein externes Relais!



Falls das Modul über ein 3G Modem verfügt, können Sie **Antenne** anschließen.

Legen Sie die **SIM-Karte** in den Kartenhalter so ein, dass sie einrastet. Zur Abnahme drücken Sie die Karte nochmal an.

Die Netzkonfiguration des Moduls kann über den **USB** Host geändert werden.

Schließen Sie das lokale Netzkabel (LAN) zum Internet aus dem Router an den **Ethernet Anschluss** an.

-> *Anwendungsanweisung, Abschnitt 3*

INBETRIEBSETZUNG DES MODULS

Nach Beschaltung und Anschluss des lokalen Netzwerks kann man das Modul einspeisen. Die Einstellungen können mit Hilfe eines Computers auf dem gleichen Netz wie das Modul eingestellt werden.

Das Modul wird standardmäßig mit der Einstellung DHCP geliefert. Zur Identifizierung der vom lokalen Router ausgeteilten IP-Adresse benutzen Sie nach Bedarf das Programm IP Bridge Virtual Client, das Sie aus der Internetseite des Produkts herunterladen können. Falls die Dienstleistung UDP Broadcast im Router nicht freigegeben ist, kann das Programm das Modul nicht identifizieren. In diesem Fall können Sie die IP-Adresse in der DHCP-Liste des Routers finden.

Falls Sie zum Modul auch über Internet zugreifen möchten, stellen Sie an Ihrem Router auf den Schnittstellen Nr. 80 und 443 die Port-Umlenkung auf die IP-Adresse des Moduls ein.

Die Netzkonfiguration des Moduls kann mit Hilfe einer auf einem Pen-drive kopierten Textdatei geändert werden. Die Vorgehensweise und die Details über das Format der Textdatei finden Sie unter dem Punkt 5.3 der Anwendungsanweisung.

-> *Anwendungsanweisung, Abschnitt 5*

WEBOBERFLÄCHE

Zum Öffnen der Weboberfläche schreiben Sie die IP-Adresse des Moduls (z.B. 192.168.1.198) in einem Browser ein, dann geben Sie den Benutzernamen und das Passwort an.



Standardmäßig sind ein Systemadministrator und ein weiterer Anwender im System. Die Anmeldedaten sind wie folgt:

Benutzername / Passwort: **admin / admin**

Benutzername / Passwort: **user / user**

Achtung! Bei der ersten Anmeldung verändern Sie unbedingt die standardmäßig angegebenen Passworte. Das können Sie auf der Seite Allgemeine Einstellungen vornehmen.















MODULZUSTAND

Das Modul zeigt nach der Anmeldung die Seite Zustand. In der obersten Leiste sind die Funktionen Sprachauswahl , das Aufsichtsbild  und die Abmeldung platziert. Im Fenster Aufsichtsbild kann man Sicherheitsspeicherung über die Einstellungen machen bzw. früher entladen und gespeicherten Einstellungen zurückladen.

Achtung!Der ausgelesene und gespeicherte Datensatz enthält sensible Daten. Bitte, die Daten dementsprechend speichern!

In der Kopfzeile sind die grundsätzlichen allgemeinen Informationen dargestellt: Datum/Uhrzeit des Moduls, aktuelle LAN IP-Adresse, Speisespannung, Gruppencode und Gerät-ID der Fernüberwachung des Moduls sowie der Zustand der simulierten Telefonleitung. Außerdem werden – falls ein zusätzliches Panel vorhanden ist – die IP-Adresse des mobilen Internets, die Höhe der Feldstärke des mobilen Internets in Prozent, die IMEI-Nummer und die SIM-ID-Nummer angezeigt.

Nach der Sektion **Eingänge** über den aktuellen Zustand der Zoneneingänge kommt die Sektion **Ausgänge**, die den Zustand der Ausgänge anzeigt und von der die Ausgänge auch gesteuert werden können. Dann kommt die Sektion **Server** über den Zustand der Kontakte mit den Empfangseinheiten. Anschließend kommt das **Ereignisprotokoll**, das eine Liste über die letzten 10 Einträge des von der Alarmzentrale übernommenen Protokolls über die eigenen Ereignisse des Moduls erfasst. Mit Hilfe der Taste **Weitere Ereignisse...** ist das komplette Ereignisprotokoll (max. 500 Ereignisse) erreichbar.

Das Ereignisprotokoll enthält die Uhrzeit und das Datum der Entstehung des Ereignisses, den CID-Code, den Zustand der Anmeldung auf den Server der Fernüberwachung (1–6), den Zustand der VOIP-Benachrichtigungen (1–4), den Zustand der SMS-Nachrichten (1–4) den Speicherungsstatus der Kamerabilder () , den Zustand der E-Mail-Sendung @, den Zustand der Ladung der Kamerabilder auf den FTP () , den Zustand der Darstellung im TSM System () , den Zustand der Relaissteuerung () sowie den Zustand der Push-Auswertungen (1–4). Außerdem kann man die Kamerabilder zum Ereignis () und die Details der Ereignisse Typ Änderungen der Einstellungen () ansehen.

-> *Anwendungsanweisung, Abschnitt 6.1*

ALLGEMEINE EINSTELLUNGEN

Die Einstellungen bezüglich der Kommunikation und des Betriebes können auf dem Tab **Allgemein** des Menüpunkts **Einstellungen** geändert werden.

Einige wichtigsten Einstellungen ohne Anspruch auf Vollständigkeit:

Benutzer: Die Benutzernamen und Passworte der zwei Standardebenen können auch geändert werden sowie hier kann man die Erreichbarkeit des Servers RADIUS zum Hinzufügen und zur Verwaltung weiterer Benutzer angeben.

Kunden-ID und TEX-ID: Hier können Sie die Identifikationsdaten zur Signallübergabe der Fernüberwachung angeben.

Ping Server: Zur Kontrolle des externen und internen Netzes sind je 2 Ping Server eingestellt. Wenn das Gerät über zusätzliches Panel verfügt, dann sind noch zwei für die Kontrolle des mobilen Internets eingestellt.

Überwachung der Speisespannung: Wenn die Speisespannung mindestens 30 Sekunden lang die untere Toleranzgrenze unterschreitet, wird ein internes Ereignis *Störung Batterie* generiert, wenn der Wert der Speisespannung mindestens 30 Sekunden lang den Rückstellungswert überschreitet, wird ein internes Ereignis ***Rückstellungsstörung Batterie*** generiert.

FTP/SFTP: Sie können die beim Alarm erfassten Kamerabilder an den hier angegebenen Server synchronisieren. Geben Sie dazu die IP-Adresse des Servers an. Schreiben Sie die Schnittstelle abgetrennt mit Doppelpunkt dahinter (z.B.: 192.168.1.1:8181). Bei Bedarf können Sie hier den Faden der Verzeichnisstruktur sowie den Benutzernamen und das Passwort hier angeben.

TSM Server: Das Gerät kann die beim Alarm erfassten Kamerabilder und Live URL außer den Contact ID-Nachrichten an den hier eingestellten Server weiterleiten.

Server zum Update: Standardmäßig werden die Updates aus dem Server des Herstellers geladen, aber ein anderer Server kann hier auch eingestellt werden.

Firmware Update: Aus den hier angegebenen E-Mail-Adressen kommen die Nachrichten über die vorhandenen neuen Updates. Es kann eingestellt werden, wann es kontrolliert werden soll, ob es neue Updates vorhanden sind bzw. ob die Updates manuell oder automatisch abgeladen und installiert werden soll.

Standardeinstellungen: Die Einstellungen des Geräts werden auf die Werkseinstellungen zurückgestellt, aber die aktuelle Version von Firmware wird erhalten

Über die obigen Einstellungen und die weiteren Möglichkeiten können Sie mehr im Abschnitt 6.2 der **Gebrauchsanweisung** lesen.

SERVER

Zur Signalübergabe der Ereignisse an die Fernüberwachung müssen Servergruppen erstellt werden. Später können Sie diese Servergruppen dem zu signalisierenden Ereignis zuordnen. Dazu müssen Sie zuerst die Server der Fernüberwachung (max. 6 Stk.) erfassen, dann Gruppen (max. 6 Stk.) aus dem Server erstellen.

Zum **Hinzufügen** eines Servers geben Sie einen beliebigen Namen, die IP-Adresse oder den Domain-Namen des Servers, die Schnittstelle an, wählen Sie den Kommunikationskanal und den Kundentyp an sowie stellen Sie die Lebenszeichensendung ein. Wenn kein zusätzliches Panel zum Modul vorhanden ist, ist LAN die einzige Möglichkeit, und erscheint keine Netzwahlmöglichkeit. Bei einem Empfänger Typ SIA IP kann ein AES-Schlüssel angegeben werden.

Zum Hinzufügen einer Servergruppe geben Sie einen beliebigen Namen an, dann stellen Sie die Gruppe aus den erfassten Servern zusammen, und geben Sie die primären Server an. Das Gerät macht mindestens einen Signalübergabe-Versuch über das Ereignis zu jedem primären Server. Wenn keine Signalübergabe-Versuche nach 10 Minuten auf einen primären Server erfolgreich sind, macht es Versuche mit den zusätzlichen Servern. Wenn die Signalübergabe auf einen zusätzlichen Server erfolgreich war, wird keine Signalübergabe an die anderen Server erfolgen.

-> *Anwendungsanweisung, Abschnitt 6.3*

KAMERAS

Das IP Bridge sucht automatisch die Kamera am gleichen Netz, die die ONVIF-Empfehlung unterstützen, und erstellt eine Liste darüber im Menüpunkt Kameras.

Wenn die Verbindung ohne Passwort für die Kamera freigegeben ist, werden die in der Kamera eingestellten Profils aufgelistet. Diese sind

durch Drücken der Taste **Profilabhängige Parameter** ersichtlich. Andernfalls kann man der Benutzernamen und das Passwort zur Anmeldung sowie die ONVIF-Schnittstelle zur Kommunikation mit dem IP Bridge auch hier angeben.

Die aufgelisteten Profile können Sie durch Drücken der Taste **Zur Liste hinzufügen** hinzugefügt werden. Zur Liste können Sie durch Angabe von URL auch manuell Kameras hinzufügen. Dazu müssen Sie die Taste **Anzeigen/Editieren** in der Tabelle **Liste der hinzugefügten Kameras** drücken. Wenn die Kamera aus einer externen Adresse angerufen ist, ist es mit großem Datenverkehr zu rechnen.

Achtung! Nach einem Ereignis mit der Erfassung von 5-10 Tausenden Kamerabildern – abhängig von der Auflösung der Kamera – kann die SD-Karte voll sein. In diesem Fall kann das Gerät nur dann weitere Kamerabilder speichern, wenn die früher gespeicherten Bilder vorab gelöscht werden. Das können Sie im Menüpunkt Kameras vornehmen.

-> *Anwendungsanweisung, Abschnitt 6.4*

MOBILANWENDUNG

Das IP Bridge ist auf Grund von Ereignissen zur Sendung von Push-Nachrichten fähig, bzw. der Zustand der Eingänge kann aus der dazu entwickelten Mobilanwendung kontrolliert werden, die Ausgänge können außerdem gesteuert werden. Die Anwendung **TELL Control Center** ist im App Store und im Play Store verfügbar.



Als erster Schritt müssen Sie diese Dienstleistung auf der Seite **Mobilanwendung** freigeben und die IP-Adresse, die Schnittstelle zur Push-Sendung einstellen sowie auswählen, über welchen Kommunikationskanal

das Gerät die Verbindung herstellen muss und ob ein zusätzliches Netz nötig ist. Standardmäßig enthalten diese Einstellungen die Daten des vom Hersteller zu diesem Zweck vorgesehenen Servers. Und das Netz ist das auf der Seite **Allgemein** eingestellte **Standardnetz**.

Server IP: 54.75.242.103

Schnittstelle: 2020

Zum IP Bridge können 4 Stk. Mobilgeräte registriert werden. Jeder Slot hat eigene Identifizierungsdaten, die durch Drücken der Taste QR-Code am Ende der Reihe hervorgerufen werden können. In der Mobilanwendung kann man das Gerät ins Modul registrieren, indem man den QR-Code des betroffenen Slots einliest. In diesem Fall werden die Identifikationsdaten der Mobilanwendung bzw. der Name des Mobilgeräts angezeigt.

-> *Anwendungsanweisung, Abschnitt 6.6*

EINSTELLUNGEN DER EREIGNISSE

Im Menüpunkt Ereignisse können sowohl die internen als auch die externen Ereignisse des Moduls konfiguriert werden. Zu den Ereignissen kann man einen individuellen Namen angeben, der im Ereignisprotokoll und in den Berichten angezeigt wird. Die Namen der Eingänge erscheinen außerdem im Menüpunkt Zustand auch.

Externes Ereignis: Im Modul können maximal 20 Stk. externe Ereignisse für Ereignisse Contact ID aus der simulierten Leitung außer den internen Ereignissen eingestellt werden. Mit Hilfe der Taste Hinzufügen in der Tabelle unten kann man diese Einstellung vornehmen.

Die Einstellungen der Ereignisse sind in 8 Gruppen eingestellt. Mit Hilfe der Pfeile in der Kopfzeile der Tabelle kann man diese wechseln.

Einstellungen der Eingänge

Typ der Eingänge: entsprechend des Anschlusses NO (in der Grundstellung geöffnet) oder NC (in der Grundstellung geschlossen)

EOL: Mit Hilfe dieser Einstellung kann der Sabotageschutz auf dem betroffenen Eingang freigegeben werden.

Sensibilität (ms): Das Gerät berücksichtigt auf dem betroffenen Zonen- eingang keine Zustandsänderungen, die für kürzere Zeit als die hier eingestellte Zeit erfolgen.

Abschalten: Die abgeschalteten Ereignisse werden nicht generiert.

Nächste Benachrichtigung: Hier kann man die Auswertung des nächsten externen Ereignisses freigeben, auch wenn ein CID-Code hier angepasst ist.


Ereigniscodes

Standardmäßig gehört zu jedem internen Ereignis ein Contact ID Code, aber die Werte des CID-Codes, der Partition und der Zone können auch umgeschrieben werden.

Einstellungen der Fernüberwachung

Im Falle der Signalübertragung eines Ereignisses an die Fernüberwachung muss man die Signalübergabe freigeben und aus der auf der Seite Server erfassten Servergruppe angeben, wohin der Contact ID Code des Ereignisses übertragen werden muss. Die Signalübergabe des Ereignisses auf TMS muss man extra freigeben.

E-Mail Einstellungen

Hier kann man die E-Mail-Benachrichtigung über das Eintreten bestimmter Ereignisse einstellen. Durch Drücken das Piktogramm Editieren  können die Liste der Empfänger, der Betreff und der Text der Nachricht editiert werden. Die E-Mail-Adressen muss man mit einem Komma abgetrennt angeben.

Einstellungen der Kamera


Im Menü Einstellungen der Kamera kann man die Kameras im Modul den Ereignissen zuordnen. Wenn ein Ereignis erfolgt, schickt das Modul die letzten 5 Bilder der zugeordneten Kamera an die angegebene E-Mail-Adresse zu oder die Bilder werden auf einen FTP/SFTP Server hochgeladen oder dem TMS Server weitergeleitet.

VOIP (SIP) Einstellungen

Die Spalten **V1-V4** zeigen die im Teil **Anruf** des Menüpunktes **VOIP** angegebenen Telefonnummern an. aus diesen Nummern kann man auswählen, welche beim Eintreten eines Ereignisses vom Modul benachrichtigt werden soll. In der Spalte **Bestätigen** kann man die Art der Bestätigung angeben (entfällt / mit der Taste * / durch Abweisen des Anrufs). Das Stoppen der weiteren Operationen ist jederzeit mit der Taste # möglich. Bei der Option **Bestätigung des Abweisens des Anrufs** wird der Empfang des Anrufs auch bestätigt, aber die weiteren Benach-


richtigungen können auch in diesem Fall durch Drücken der Taste # gestoppt werden. Die bei der Auswertung abzuspielende Tonnachricht kann auch ausgewählt werden.

SMS-Einstellungen

Die Telefonnummern zu den Spalten **SMS1-SMS4** können in der Sektion **SMS** des Menüpunktes **VOIP** eingestellt werden. Der **SMS-Text** von zu versendenden SMS kann mit dem  editiert werden.

Mobileinstellungen

Die Spalten **MOBIL1-MOBIL4** stellen die im Menüpunkt **Mobilanwendung** aufgelisteten Mobilgeräte dar. An die ausgewählten Geräte wird die in der Spalte Text der Push-Nachricht eingestellte Benachrichtigung versandt.

 Mit Hilfe des Piktogramms können Sie die in der ersten Zeile angegebenen Werte auch zu den allen weiteren Ereignissen kopieren.

Über die Ereignisse und Einstellungen können Sie im Abschnitt 6.7 der Gebrauchsanweisung mehr lesen.

FERNMODULE

Den Geräten können IP Bridge Fernmodule zugeordnet werden. Dadurch kann eine transparente serielle Übertragung erfolgen oder können die Ausgänge der Fernmodule automatisch gesteuert. Dem Modul können 6 Stk. IP Bridge Fernmodule mit der Angabe folgenden Daten zugeordnet werden.

Adresse des Ferngeräts: IP-Adresse des Geräts. Wenn die zwei Geräte sich nicht am gleichen Netz befinden, muss man die IP-Adresse des Routers und die externe Schnittstelle angeben.

Schnittstelle: Https-Schnittstelle des betroffenen Geräts.

Benutzername und Passwort: Die zur Anmeldung am Ferngerät erforderlichen Daten.

Im Feld **Fernmodule** kann man aus den zugeordneten IP Bridge Fernmodule ausgewählt werden, mit welchem die serielle Datenübertragung erfolgen soll. Bei der Option **Nur Empfang** empfängt das IP Bridge die Daten aus den Fernmodule und weiterleitet diese an die serielle Schnittstelle. In diesem Fall ist der Datenempfang von Fernmodulen in beliebiger Anzahl möglich, diese müssen nicht der obigen Liste hinzugefügt werden.

Art der Verbindung: Die Verbindung kann dauernd sein, oder sie kann auch so eingestellt werden, dass die Module nur während der Datenübertragung miteinander verbunden werden.

Zeitüberschreitung: Das Modul trennt bei der Überschreitung der hier angegebenen Zeit ab dem letzten Datenversand oder -empfang die Verbindung.

Maximale Verzögerung der Datenübertragung: Das Modul sammelt dauernd die über die serielle Schnittstelle empfangenen Daten. Wenn es keine Pausen während des Datenempfangs entstehen, schickt es die bereits empfangenen Daten dem zugeordneten Fernmodul nach dem Ablauf der hier angegebenen Zeit zu.

Einstellungen der seriellen Schnittstelle: Sie muss anhand des Typs der Verbindung eingestellt werden.

Bezüglich der Fernmodule können Sie mehr im Abschnitt 6.8 der Gebrauchsanweisung lesen. Und die detaillierten Informationen über die Fernprogrammierung der Alarmsysteme finden Sie in der Anlage der Gebrauchsanweisung.

AUSGÄNGE

Im Menü **Ausgänge** kann man die Ausgänge konfigurieren bzw. automatische Steuerungen zuordnen.

Hier können Steuerungen durch ein internes oder externes Ereignis zugefügt werden. Das **steuernde Ereignis** kann ein beliebiges Ereignis sein, das unter dem Menüpunkt **Ereignisse einstellen** vorhanden ist. Wählen Sie das **Zu steuernde Modul** und den **Ausgang** aus. Ein beliebiger Ausgang des betroffenen Moduls oder ein der im Menü **Fernmodule** hinzugefügten Ausgänge kann ausgewählt werden. Die Aktivierung des Ausgangs kann man um die im Feld **Verzögerung** angegebenen Sekunden verzögert werden.

Es gibt vier verschiedenen **Steuerungsarten zu den Ausgängen:**

Zustandsänderung: Durch das Ereignis ändert sich der Zustand des betroffenen Relais.

EIN – zeitgesteuert: Durch das Ereignis wird er für die in der Spalte Timing angegebene Dauer aktiv, dann wieder inaktiv.

EIN – dauernd: Der Ausgang wird aktiv und bleibt bis zum Ereignis des nächsten Ausschaltens oder der Zustandsänderung auch aktiv.

Aus: Der betroffene Ausgang wird inaktiv.

Stopp: Wenn mehrere sich überschneidende externe Ereignisse erfasst sind und dieses Feld markiert ist, wird das nächste angegebene Ereignis nicht ausgewertet.

ROUTER ÜBERWACHUNG

Das IP Bridge kann die Router im gleichen Netz überwachen. Wenn es keine Antwort von den eingestellten Ping Servern bekommt, kann es den Router mit Hilfe von Softwares und/oder Hardwares neustarten.

Aus der Liste zur **Auswahl des Servers** kann man die vorab definierten Serverpaare auswählen, in diesem Fall können die anzupingelnden Server nicht editiert werden. Bei der Auswahl der individuellen Option können beide anzupingelnden Server manuell ausgewählt werden. Solche Server sind anzugeben, die ausschließlich über den zu überwachenden Router erreichbar sind.

Neustart mit Software

IP-Adresse des Routers: Wir können die automatische Identifizierung auswählen oder die Adresse manuell einschreiben.

Art der Verbindung: Das Modul wird versuchen, den Router über das ausgewählte Protokoll zu erreichen. Außer den aus dem Dropdown-Menü auswählbaren Befehlen können individuelle Befehle auch angegeben werden, falls das SSH das ausgewählte Protokoll ist.

Router Schnittstelle: Schnittstelle des Routers zur Authentication.

Benutzername und Passwort: Zur Anmeldung in den Router sind Benutzername und Passwort erforderlich.

Anzahl der erfolglosen Pings zum Neustart des Routers: Die Anzahl der Ping-Versuche vor dem Neustart des Routers.

Aussetzung der Kontrolle nach dem Neustart: Für die nach dem Neustart angegebene Dauer wird keine Ping-Anforderung an den Server gestartet, damit der Router genügend Zeit zum Neustart hat.

Neustart mit Hardware

Fernmodul: Der ausgewählte Ausgang des ausgewählten Moduls wird aktiviert. Die Optionen Fernmodule 1-6 stellen die im Menü Fernmodule hinzugefügten Module dar.

Ausgang zum Neustart des Routers: Es kann ausgewählt werden, welcher Ausgang des Moduls aktiviert werden soll.

Dauer der Ausgangsaktivierung: Die hier angegebene Dauer wird zum Wechsel des Zustands benötigt.

Falls der Neustart mit Software auch freigegeben ist, kann es ange-

geben werden, nach wie vielen erfolglosem Neustart mit Software der Router mit Hardware neugestartet werden soll. Wenn ausschließlich der Neustart mit Hardware freigegeben ist, muss die Anzahl der erfolglosen Pings als Bedingung für den Neustart angegeben werden.

Für die im Feld **Aussetzung der Kontrolle nach dem Neustart** angegebene Dauer wird keine PING-Anforderung an den Server gestartet, damit der Router genügend Zeit zum Neustart hat.

BERICHT

Das Modul kann die Berichte über die eigenen internen und externen Ereignisse per E-Mail versenden. Die Versandhäufigkeit und die genaue Uhrzeit des Versands können im Feld **Häufigkeit des Berichts** editiert werden. Wenn die Anzahl der Ereignisse 250 erreicht, wird der Bericht unabhängig von den Einstellungen versandt.

Im Feld **E-Mail-Adressen** können Sie mehrere E-Mail-Adressen, abgetrennt mit Komma, angeben. Zu den im Bericht erfassten Ereignissen kann ein Filter durch die Einstellung **Zu meldenden Ereignisgruppen** eingestellt werden.

SONSTIGE WICHTIGE INFORMATIONEN

Stoppen des Moduls:

Zum ordnungsmäßigen Stoppen drücken Sie den Mikroschalter auf dem Modul 2-5 Sekunden lang, bis die LED orangefarbig wird. Dann lassen Sie den Mikroschalter los. Sobald die LED erlischt, können Sie die Speisespannung ausschalten.

Werkseitige Einstellungen zurücksetzen:

Die werkseitigen Einstellungen können mit Hilfe der Taste im Menüpunkt Allgemeine Einstellungen oder der Drucktaste am Modul zurückgesetzt werden. Die Drucktaste am Modul muss man 8 Sekunden lang drücken. Die LED wird zuerst orangefarbig, dann rot. Das Modul führt das Zurücksetzen und einen automatischen Neustart durch.

Achtung! Während des Zurücksetzens wird auch die Netzeinstellung auf das standardmäßige DHCP zurückgestellt.

S.M.A.R.T Info:

Die S.M.A.R.T-Daten der SD-Karte werden im Menüpunkt S.M.A.R.T angezeigt. Diese Funktion funktioniert mit den Karten Typ APACER einwandfrei.

LED Signale:

<i>Rot:</i>	Systemstart / Systemstopp läuft
<i>Grün:</i>	Das System ist betriebsbereit
<i>Orange:</i>	Störung vorhanden / Ein-/Aus-schalten läuft

Technische Spezifikationen:

<i>Speisespannung:</i>	12-24V DC
<i>Nominale Stromaufnahme:</i>	520mA @ 12V DC
<i>Maximale Stromaufnahme:</i>	700mA @ 12V DC
<i>Betriebstemperatur:</i>	-20°C - +70°C
<i>Belastbarkeit der Ausgänge:</i>	1A @ 12V DC
<i>Dimensionen:</i>	130 x 69 x 19 mm
<i>Gewicht:</i>	200g (csomagolva: 300g)

Spezifikationen der generierten Telefonleitung:

<i>Spannung der Leitung:</i>	48 V
<i>Leitungsstrom:</i>	20 mA
<i>Impedanz der Leitung:</i>	600 Ohm
<i>Spannung des Klingelns:</i>	±50V (20 Hz)
<i>Wählton:</i>	425 Hz



SICHERHEITSANSWEISUNGEN

Für Ihre Sicherheit bitten wir Sie, folgende Anweisungen aufmerksam zu lesen und befolgen! Die Nichteinhaltung der Sicherheitsanweisungen können eine Gefahr für Sie und Ihre Umwelt bedeuten!

Das Produkt von TELL (im Folgenden „Gerät“) hat ein eingebautes Kommunikationsmodem. Abhängig von der Version des Produktes kann das eingebaute Modul im System 2G, 3G oder 4G kommunizieren.

Das **2G-Modem** kann folgende Frequenzbänder benutzen: 850/900/1800/1900 MHz @GSM/GPRS

Das **3G-Modem** kann folgende Frequenzbänder benutzen: 900/2100 MHz @UMTS, 900/1800 @GSM/GPRS

Das **3GA-Modem** kann folgende Frequenzbänder benutzen: 800/850/900/1900/2100 MHz @UMTS, 850/900/1800/1900 MHz @GSM

Das **4G-Modem** kann folgende Frequenzbänder benutzen: 900/1800 MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE

Das **4GA-Modem** kann folgende Frequenzbänder benutzen: B2/B4/B5@ WCDMA, B2/B4/B5/B12/B13@LTE

- **VERWENDEN SIE** das Gerät in **KEINER** Umgebung, wo die Radiofrequenz Strahlungsgefahr hervorrufen kann und mit anderen Geräten Interferenz entstehen kann, die zur Störung der Funktion von diesen Geräten führen kann - z. B. Sanitätsgeräte!
- **VERWENDEN SIE** das Gerät **NICHT** bei hoher Luftfeuchtigkeit oder Vorhandensein von gefährlichen Chemikalien oder bei sonstigen mechanischen Einwirkungen!
- **VERWENDEN** Sie das Gerät **KEINER** außerhalb des spezifizierten Betriebstemperaturbereichs!
- **INSTALLIEREN SIE** das Gerät **NICHT** in einer gefährlichen Umgebung.
- Es ist **VERBOTEN**, das Gerät unter Spannung zu montieren / anzuschließen. Damit das Gerät einfach von der Spannung abgetrennt werden kann, soll das Netzteil oder die Stromversorgungseinheit des Gerätes auf einem leicht zugänglichen Ort platziert werden!

- **TRENNEN SIE** das Gerät **IMMER** von der Speisespannung, bevor Sie mit der Montage beginnen!
- **TRENNEN SIE** das Gerät **IMMER** von der Speisespannung, bevor Sie die SIM-Karte einlegen, entfernen oder austauschen!
- Zum **AUSSCHALTEN DES GERÄTES** trennen Sie alle Stromquellen vom Gerät, einschließlich der Speisespannung und des USB-Anschlusses!
- Der **ZUM GERÄT ANGESCHLOSSENE** Computer soll immer an die Schutzterdung angeschlossen sein!
- **VERWENDEN SIE** für die Programmierung des Gerätes **KEINEN** Computer, der an die Schutzterdung nicht angeschlossen ist. Zur Vermeidung der Entstehung einer Erdschleife müssen die Speiseeinheiten des Computers und des Gerätes die selbe Erdung benutzen!
- **VERSUCHEN SIE NICHT** das Gerät zu **REPARIEREN**. Die Reparatur des Gerätes darf nur von dafür ausgebildeten Fachkräften vorgenommen werden!
- **STELLEN SIE GEEIGNETE STROMQUELLE** für das Gerät zur Verfügung! Das Gerät arbeitet sicher und zuverlässig nur bei Verwendung von Speiseeinheiten, die fähig sind auch die maximalen Werte der Anforderungen im Handbuch des Gerätes zu erfüllen. Die genauen Daten können Sie im Handbuch des Gerätes und auch auf der Webseite unter <http://tell.hu> finden.
- **VERWENDEN SIE** das Gerät mit **KEINER** Speiseeinheit, die den Vorschriften der ungarischen Norm MSZ EN 60950-1 nicht entspricht!
- **VERTAUSCHEN SIE** die Polarität der Speisespannung **NICHT!** Die Speisespannung ist in jedem Fall entsprechend der am Gerät angegebenen Polarität anzuschließen!
- **SCHLIESSEN SIE** den Anschluss der GSM-Antenne **NICHT** an die Schutzterdung. Schließen Sie die metallischen Teile der GSM-Antenne **WEDER** direkt **NOCH** indirekt an eine Schutzterdung, da es zum Defekt des Moduls führen kann!
- **ACHTUNG!** Das Gerät verfügt über die Funktion automatische Speisespannung-Abtrennung (Under Voltage Lock Out). Abhängig von der Produktart, schaltet sich das Modul automatisch aus, wenn die Speisespannung unter 8,4...8,2V fällt. Das Modul schaltet sich wieder ein, wenn die Speisespannung 11,2...11,4V erreicht.