

TITAN

Software-Benutzerhandbuch

Index

Allgemeine Hinweise	4
Wichtige Informationen	4
Überarbeitungen	5
SOFTWARE.....	6
1. Einführung.....	6
2. FAQ: Grundlegende Konzepte	7
3. Schritt-für-Schritt-Konfiguration	12
4. Einstellung.....	13
4.1 Mobile	13
4.1.1 Mobile > Status.....	13
4.1.2 Mobile > Basic Settings.....	14
4.1.3 Mobile > Keep Online	16
4.1.4 Mobile > Basic Settings > FailOver.....	17
4.1.5 Mobile > Grundeinstellungen >Bediener	18
4.2 Ethernet	19
4.2.1 Ethernet > Basic Settings.....	19
4.2.2 Ethernet > DHCP-Server.....	21
4.3 WiFi	21
4.3.1 WiFi > Basic Settings.....	22
4.3.2 WiFi > DHCP-Server	24
4.4 Firewall.....	25
4.4.1 Firewall > NAT.....	25
4.4.2 Firewall > Authorized IPs.....	26
4.4.3 Firewall > MAC Filter	28
4.4.4 Firewall > Routen	28
4.5 Serial Settings > Serial portX	29
4.5.1 Serial Settings > Serial portX.....	29
4.5.2 Serial Settings > SSL Certificates	34
4.6 External Devices	36
4.6.1 External Devices > Logger configuration	36
4.6.2 External Devices > Temperature Sensor.....	41
4.6.3 External Devices > Modbus RTU / TCP	43
4.6.4 - External Devices > GPS Receiver	45
4.6.5 - External Devices > Generic Serial Device	46
4.6.6 - External Devices > IEC102 Meter.....	47
4.7 Other	50
4.7.1 Other > AT Command.....	50

4.7.2 Other > DynDns	51
4.7.3 Other > Private DynDns	52
4.7.4 Other > SMS Control	55
4.7.5 Other > Periodic autoreset	56
4.7.6 Other > Time Servers (NTP)	57
4.7.7 Other > Remote console (TCP Server)	58
4.7.8 Other > SNMP	59
4.7.9 Sonstiges >> TACACS+	62
4.7.10 Other > MQTT	62
4.7.11 Other > HTTP / HTTPS	65
4.7.12 Other > User Permissions.	65
4.7.13 Other > Passwords.	67
4.7.14 Other > CA Certificates	67
4.7.15 Other > Email Configuration	68
4.7.16 Other> Modbus Slave	70
4.7.17 Other > TITAN Scripts	74
4.7.18 Sonstiges > Konnektivitätswerkzeuge	107
4.7.19 Sonstiges >> Digitale E/A	109
4.7.20 Sonstiges > Benutzerdefinierter Skin	112
4.7.21 Sonstiges > Benutzerdefinierte LED	113
4.7.22 Other > SYSLOG	114
4.7.23 Sonstiges > Backup / Fabrik	115
4.7.24 Sonstiges > Neustart	116
4.8 VPN	117
4.8.1 VPN > OpenVPN-Server	117
4.8.2 VPN > OpenVPN-Client	118
4.8.3 VPN > IPSec	120
5. AT-Befehle	122
AT-Befehle im Zusammenhang mit der Nachrichtenübermittlung:	124
E/A-bezogene AT-Befehle:	125
AT-Befehle im Zusammenhang mit OpenVPN:	127
AT-Befehle zum Testen der Konnektivität:	128
AT-Befehle im Zusammenhang mit MODBUS:	129
AT-Befehle in Zusammenhang mit der Systemzeit:	130
AT-Befehle in Zusammenhang mit der Konfiguration des Titan-Geräts:	131
External Devices > Modbus RTU / TCP	131
6.Neugigkeiten in den Firmwareversionen	139

Allgemeine Hinweise

Der Empfänger geht davon aus, dass das Produkt akzeptiert wird und ohne Schnittstelle zu den Produkten des Empfängers bereitgestellt wird. Die Dokumentation und/oder das Produkt werden zu Test-, Evaluierungs-, Integrations- und Informationszwecken zur Verfügung gestellt. Die Dokumentation und/oder die Produkte werden in der vorliegenden Form bereitgestellt und können Mängel aufweisen. Die Dokumentation und/oder die Produkte werden ohne jegliche ausdrückliche oder stillschweigende Garantie zur Verfügung gestellt. Soweit gesetzlich zulässig, lehnt die Webdyn darüber hinaus alle Gewährleistungen ab, einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Vermarktbarkeit, Vollständigkeit, Eignung für einen bestimmten Zweck und Nichtverletzung von Rechten Dritter. Alle Risiken, die sich aus der Verwendung oder Leistung des Produkts und der Dokumentation ergeben, verbleiben beim Empfänger. Dieses Produkt ist nicht für den Einsatz in lebenserhaltenden Geräten oder Systemen vorgesehen, bei denen eine Fehlfunktion des Produkts nach vernünftigem Ermessen zu Verletzungen führen könnte. Anwendungen, in denen das beschriebene Produkt verwendet wird, müssen gemäß den technischen Spezifikationen in diesem Leitfaden konzipiert werden. Die Nichteinhaltung eines der vorgeschriebenen Verfahren kann zu Fehlfunktionen oder schwerwiegenden Abweichungen bei den Ergebnissen führen.

Darüber hinaus sind alle Sicherheitshinweise im Zusammenhang mit der Nutzung von mobilen technischen Systemen, einschließlich GSM-Produkten, die auch für Mobiltelefone gelten, zu beachten. Webdyn oder seine Zulieferer haften unabhängig von der Rechtstheorie, auf die sich der Anspruch stützt, nicht für Folgeschäden, beiläufig entstandene, direkte, indirekte, strafende oder sonstige Schäden (einschließlich, aber nicht beschränkt auf Schäden aus entgangenem Gewinn, Betriebsunterbrechung, Verlust von Geschäftsinformationen oder Daten oder sonstigem Vermögensschaden), die sich aus der Nutzung oder der Unmöglichkeit der Nutzung der Dokumentation und/oder des Produkts ergeben, selbst wenn Webdyn auf die Möglichkeit solcher Schäden hingewiesen wurde. Die vorstehenden Haftungsbeschränkungen gelten nicht, soweit zwingend gehaftet wird, z. B. nach dem spanischen Produkthaftungsgesetz, in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit oder wegen der Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit gehaftet wird. Die vorstehende Bestimmung bedeutet keine Umkehr der Beweislast zum Nachteil des Empfängers. Änderungen ohne Vorankündigung vorbehalten. Die Auslegung dieses allgemeinen Vermerks unterliegt spanischem Recht ohne Verweis auf anderes materielles Recht.

Wichtige Informationen

Diese technische Beschreibung enthält wichtige Informationen für die Inbetriebnahme und den Einsatz von TITAN-basierten Geräten. Lesen Sie sie sorgfältig durch, bevor Sie mit ihnen arbeiten. Bei Schäden, die durch Nichtbeachtung dieser Gebrauchsanweisung entstehen, erlischt der Garantieanspruch. Für Folgeschäden können wir keine Haftung übernehmen.

Überarbeitungen

ÜBERARBEITUNG	DATUM
6.19	2023/01

SOFTWARE

1. Einführung

Die TITAN-Firmware ermöglicht 2G/3G/4G-Geräte mit erweiterten Gateway-Funktionen.

Zusätzlich zu den klassischen Router-Fähigkeiten, die TITAN-basierte Geräte ermöglichen die Nutzung von 4G/3G/2G - RS232/485-Gateways, die Ausführung von AT-Befehle per SMS (um die Abdeckung zu überprüfen, die Relais zu schalten, digitale Eingänge zu lesen, usw.), die Annahme von GSM-Datenanrufe (CSD), um auf Geräte wie Stromzähler zuzugreifen, die autonome Lektüre von Modbus RTU- oder Modbus TCP-Geräte, die Versendung von Temperatur- und Entfernungsdaten an die Cloud und vieles mehr.

Um die Möglichkeiten dieser Geräte besser zu verstehen, empfiehlt es sich, Kapitel 2 dieses Handbuchs, die FAQ, zu lesen. Nach einer solchen Lektüre werden Sie eine konkretere Vorstellung davon haben, was Sie tatsächlich tun können. Nach der Lektüre der FAQ empfiehlt es sich, einen allgemeinen Blick in die Anwendungshinweise zu werfen (PDF-Dokumente außerhalb dieses Dokuments). Anhand dieser Beispiele können Sie sich ein genaueres Bild von den Möglichkeiten dieses Geräts machen.

Wir unterstützen alle Nutzer unserer Modems und Router im Bedarfsfall mit kostenlosem, schnellem und effizientem technischen Support. Sollten Sie also nach dem Lesen dieses Handbuchs noch Fragen haben, zögern Sie bitte nicht, uns unter der folgenden E-Mail-Adresse zu kontaktieren: contact@webdyn.com. Das Gleiche gilt, wenn Sie eine Funktion benötigen, die nicht in unseren Geräten enthalten ist, oder wenn Sie eine Anpassung benötigen, lassen Sie es uns wissen und wir werden es eingehend prüfen.

2. FAQ: Grundlegende Konzepte

- **Was kann ich mit TITAN-basierten Geräten machen?**

Im Grunde ist es möglich, dasselbe zu tun wie mit einem Standard-4G/3G/2G-Router, aber mit einige zusätzliche erweiterten Gateway-Funktionen. So kann er, zum Beispiel, eine Internetverbindung für Geräte bereitstellen, die an seinen Ethernet-Port angeschlossen sind, sowie NAT für eine Internetverbindung zu Geräten, die an diesem Port hängen.

- **Ist es möglich, WiFi-Geräten eine Internetverbindung zu ermöglichen?**

In der Tat können TITAN-basierte Geräte mit WiFi-Konnektivität als WiFi-Zugangspunkt fungieren und somit WiFi-Client-Geräten, die sich mit ihnen verbinden, eine Internetverbindung bieten. Sie können auch als WiFi Client konfiguriert werden, d.h. die TITAN-basierten Geräte können sich mit einem bestehenden WiFi Access Point in Ihrer Infrastruktur verbinden und diese Verbindung als Internetzugang nutzen.

- **Haben Sie Standard-Gangways?**

Ja, Sie können so viele 4G/3G/2G-Serial-Gateways einsetzen, wie es serielle Anschlüsse an den von Ihnen verwendeten Geräten gibt. Diese Gateways können vom Typ TCP-Client oder TCP-Server sein und können alle gleichzeitig arbeiten.

- **Serielle Gateways RS232 oder RS485?**

Alle Geräte verfügen über mindestens eine oder beide seriellen Schnittstellen RS232 und RS485. Je nach Art des seriellen Anschlusses sind die Pässe vom einen, vom anderen oder von beiden Typen.

- **TITAN-basierte Geräte ermöglichen die Einrichtung von IP-RS232/485-Gateways, aber können sie auch sichere SSL/TLS-Gateways sein?**

Ja, die TITAN-basierten Geräte ermöglichen die Konfiguration von IP-RS232/485-Gateways vom Typ Server und Client mit SSL/TLS-Sicherheit mit gegenseitiger Authentifizierung durch digitale Zertifikate (Client/Server).

- **Erlaubt die TITAN-Firmware auch die Bearbeitung von CSD-Anrufen? Kann ich z. B. ein 4G/3G/2G-Serial-Gateway betreiben, aber auch einen GSM/CSD-Datenanruf zum Ablesen eines Stromzählers annehmen?)**

Ja, aber mit Bedingungen. Wenn die TITAN-basierten Geräte im 2G-Modus betrieben werden, gibt es keine Probleme. Das Gerät nimmt den CSD-Anruf an, wenn der Anruf eingeht (um ein CSD-Seriell-Gateway zu betreiben), und übernimmt am Ende des Anrufs das 2G-Seriell-Gateway. Wenn das Gerät so konfiguriert ist, dass es auch im 3G- oder 4G-Modus funktioniert, hängt die Annahme des CSD/GSM-Anrufs von Ihrem Telefonanbieter ab, da nicht

alle Betreiber dies zulassen. Wenn Sie z. B. Movistar oder Orange nutzen und das Gerät im „Auto 4G/2G“-Modus arbeitet, gibt es keine Probleme mit der Annahme von CSD-Anrufen, unabhängig davon, ob das TITAN-basierte Gerät im 2G- oder 4G-Modus arbeitet (bei 4G wird auf 2G umgeschaltet), aber bei Vodafone ist dies nicht möglich, da es nicht unterstützt wird.

- **Ich möchte einen 4G/3G/2G-Router, aber ich muss in der Lage sein, AT-Befehle direkt an TITAN-basierte Geräte zu senden, um SMS zu versenden, die Netzabdeckung zu überprüfen usw. Ist dies bei TITAN-basierten Geräten möglich?**

Ja, alle Modelle und auf verschiedene Art und Weise. Man kann AT-Befehle ENTFERNT von einer „Telnet-ähnlichen“ Verbindung zu senden, oder über SSH, über Modbus TCP, über SNMP, über HTTP/HTTPS, MQTT/MQTTs, über SMS und sogar eingebettete Befehle in den IP-Serial-Gateways selbst. Es ist auch möglich, AT-Befehle LOKAL über den Ethernet-Port über „Telnet“, SSH, Modbus TCP, SNMP, HTTP/HTTPS und über den seriellen RS232/RS485-Port über eingebettete AT-Befehle oder Modbus RTU zu senden.

- **Unterstützen TITAN-basierte Geräte ein Modbus TCP-zu-Modbus RTU-Gateway?**

Ja, es unterstützt die Konvertierung dieser Protokolle. Wenn Sie also aus der Ferne auf Modbus-RTU-Geräte zugreifen müssen, ermöglicht Ihnen das TITAN-basierte Gerät dies, indem es als Modbus-TCP-zu-Modbus-RTU-Gateway fungiert.

- **Und können TITAN-basierte Geräte auch autonom arbeiten, indem sie Modbus RTU- oder Modbus TCP-Geräte auslesen und die Messwerte an die Cloud senden?**

Auch. TITAN-basierte Geräte können Modbus RTU- und/oder Modbus TCP-Geräte, auch in Kombination, auslesen, die Messwerte darin speichern und mittels eines JSON-Objekts über HTTP/HTTPS, MQTT/MQTTs oder FTP an WEB-Plattformen senden.

- **Was ist, wenn die TITAN-basierten Geräte Modbus RTU/TCP-Geräte autonom auslesen? Hindert mich das daran, mich sporadisch und aus der Ferne mit den Modbus RTU/TCP-Geräten von meinem Büro aus zu verbinden, um gelegentliche Auslesungen vorzunehmen, Firmware zu ändern usw.?**

Nein. Um auf Modbus-RTU-Geräte in Ihren Räumlichkeiten zuzugreifen können Sie TITAN-basierte Geräte so konfigurieren, dass sie Modbus-Geräte selbstständig lesen und ein sporadisches direktes Gateway einrichten.

- **Verfügen TITAN-basierte Geräte über eine Datenlogger-Funktion und können sie Daten speichern?**

In der Tat. Wie bereits erwähnt, können TITAN-basierte Geräte viele Arten von Daten speichern, die anschließend an Web-, MQTT- und FTP-Plattformen weitergeleitet werden. Dazu gehören zum Beispiel Messwerte von Modbus RTU/TCP-Geräten, aber auch Temperaturmesswerte, allgemeine serielle RS232/RS485-Daten, IEC-102-Zählerstände, digitale Ein- und Ausgänge usw.

- **Wie werden TITAN-basierte Geräte konfiguriert?**

Es gibt mehrere Möglichkeiten, TITAN-basierte Geräte zu konfigurieren, aber im Allgemeinen kann die gesamte Gerätekonfiguration über die Web-Konfiguration erfolgen, d.h. über den internen Webserver der Geräte.

- **Ist es möglich, eine vollständige Konfiguration in das Gerät einzulesen/ zu laden? Dies erleichtert den Produktionsprozess, wenn die Anzahl der zu konfigurierenden Geräte hoch ist.**

Ja, es ist möglich, eine vollständige Konfigurationssicherung / -wiederherstellung durchzuführen (um die Konfiguration eines TITAN-basierten Geräts auf ein anderes TITAN-basiertes Gerät zu kopieren).

- **Ist es möglich, TITAN-basierte Geräte mit einer werksseitig vorinstallierten Konfiguration zu bestellen?**

Ja, das ist möglich. Aber für große Mengen (>500 Einheiten). Für weitere Informationen wenden Sie sich bitte an Ihren Vertriebsmitarbeiter.

- **Unterstützen Sie den DynDNS-Dienst?**

Selbstverständlich und das System ist auch mit NO-IP kompatibel. Außerdem haben Sie die zusätzliche Option „Private DNS“, um Ihre aktuelle IP bei jeder Änderung oder in regelmäßigen Abständen an einen privaten Server zu senden, z. B. an den Server Ihrer Firma. Bei dieser zusätzlichen Option werden neben der aktuellen IP-Adresse auch andere Daten wie Reichweite, Technologie, IMEI, Status der digitalen Ein- und Ausgänge usw. übermittelt.

- **Die TITAN-basierten Geräte ermöglichen also die Verwaltung von digitalen Ein- und Ausgängen?**

Ja. Wenn Ihr TITAN-basiertes Gerätemodell über digitale Ein- oder Ausgänge verfügt, kann es diese verwalten. Der interne Datenlogger kann einfach so konfiguriert werden, dass er jede Änderung eines digitalen Eingangs speichert und an eine Webplattform (über HTTP/HTTPS, MQTT/MQTTS oder FTP) sendet oder einen Zeitraum für das Lesen und Senden des Status der digitalen Eingänge festlegt. Es ist auch möglich, den Status eines digitalen Eingangs

jederzeit per AT-Befehl abzufragen (der über Telnet, SSH, HTTP/S, SMS, MQTT/S, Modbus, SNMP, RS232, RS485... gesendet werden kann). Dasselbe gilt für die digitalen Ausgänge. Darüber hinaus ist es möglich, auf die digitalen Ein-/Ausgänge über den Bereich „TITAN Scripts“ des Geräts zuzugreifen. Von dort aus kann ein kleines Skript (in JavaScript) programmiert werden, damit das Gerät diese digitalen Ein-/Ausgänge nach Belieben verwendet.

- **Verfügen TITAN-basierte Geräte über eine Uhr?**

Ja, sie haben eine interne Uhr. Die Synchronisierung erfolgt über NTP über das Internet.

- **Können TITAN-basierte Geräte per SMS konfiguriert werden?**

Ja, TITAN-basierte Geräte können über AT-Befehle konfiguriert werden. Und die AT-Befehle (zusätzlich zu Telnet, SSH, HTTP/S, MQTT/S, Modbus, SNMP, RS232, RS485) können per SMS an das Gerät gesendet werden. Es können Befehle an das Gerät gesendet werden, um es neu zu starten, seine Konfiguration zu ändern, seine IP-Adresse herauszufinden, die Abdeckung zu überprüfen...

- **Ist es möglich, die Webkonfigurationsumgebung mit Firmenlogos und -bildern individuell zu gestalten?**

Ja. Jeder Benutzer kann die Konfigurations-Webumgebung mit seinen Logos, Fußzeilen, Seitentiteln usw. individuell gestalten. Es ist sogar möglich, auszuwählen, welche Menüs Ihr Endkunde sehen oder ändern kann.

- **Verfügen TITAN-basierte Geräte über eine LED-Anzeige?**

Ja, die Anzahl der LEDs hängt vom jeweiligen Modell ab. Sie können die Funktionalität der LEDs auswählen, um die Abdeckung, IP- und SIM-Probleme des Geräts usw. anzuzeigen. Die LEDs können auch über die TITAN-Skripte verwendet werden, wobei es möglich ist, ein kleines JavaScript-Benutzerskript zu programmieren, um eine LED des Geräts je nach Bedarf ein- oder auszuschalten (z. B. wenn ein digitaler Eingang aktiviert wird).

- **Ist es möglich, ein TITAN-basiertes Gerät als seriellen Datenlogger zu verwenden?**

Ja. Ein TITAN-basiertes Gerät kann so konfiguriert werden, dass es alles, was an der seriellen Schnittstelle ankommt, liest, in seinem internen Datenlogger speichert und über HTTP/S, MQTT/S oder FTP an eine Plattform im Internet sendet.

- **Und, können TITAN-basierte Geräte auch zum Auslesen von IEC 870-5-102-Zählern verwendet werden?**

Ja. Mit TITAN-basierten Geräten können Sie bei der Auslesung von Elektrizitätszählern mit IEC 870-5-102-Protokoll Folgendes tun:

1. Auslesen des Zählers über ein 4G/3G/2G-RS232/485-Gateway
2. Auslesen des Zählers über einen CSD-Datenaufbau
3. Konfigurieren Sie das TITAN-basierte Gerät so, dass es den Zähler in jedem konfigurierten Zeitraum selbstständig ausliest, die Momentanwerte in jedem Zeitraum an eine Webplattform (über HTTP/S, MQTT/S oder FTP) sendet und, falls gewünscht, auch einmal täglich Preisinformationen sendet.
4. Programmieren Sie im Bereich „TITAN-Skripte“ ein kleines JavaScript-Skript, um den Stromzähler nach Belieben auszulesen (z. B. eine bestimmte Variable kontinuierlich zu überwachen, genauere Durchschnittswerte als die Viertelstunden zu erhalten, usw.).

- **Ist es möglich, ein VPN mit TITAN-basierten Geräten einzurichten?**

Ja. TITAN-basierte Geräte ermöglichen die Konfiguration eines IPSEC- oder OpenVPN-VPNs.

- **Welche anderen wichtigen Merkmale haben TITAN-basierte Geräte?**

In diesem Handbuch finden Sie Einzelheiten zu den verschiedenen Funktionen, aber zusätzlich zu dem, was bereits in den vorangegangenen Abschnitten erwähnt wurde, ermöglicht die TITAN-basierte Ausrüstung:

- Konfiguration des Autoresets (periodisches Autoreset, zu einem bestimmten Zeitpunkt, Autoreset bei IP-Konnektivitätsproblemen usw.)
- Authentifizierungsdienst durch Tacacs+ für HTTP, Telnet und SSH
- Sichere Konfiguration über HTTPS
- Konfiguration der Benutzerberechtigungen für den Zugriff auf die verschiedenen Funktionen der TITAN-basierten Geräte entsprechend den Rollen „admin“, „user“, „guest“.
- Konfiguration des SMTP-Dienstes für den Versand von E-Mails
- Konfiguration als SLAVE MODBUS. Damit können TITAN-basierte Geräte über Modbus konfiguriert und/oder ausgelesen werden. So kann er beispielsweise über Modbus den Status seiner digitalen Eingänge auslesen, die Uhrzeit des Geräts abfragen, einen digitalen Ausgang ändern usw., und das alles von einem Modbus-Master-Gerät wie einer SPS aus.
- TITAN-Skripte. In diesem Abschnitt können Sie ein kleines Benutzerskript in JavaScript schreiben, um zum Beispiel: serielle Geräte zu lesen oder benutzerdefinierte Daten an sie zu senden, Modbus-Geräte zu lesen, einen digitalen Ausgang zu lesen oder zu ändern, SMS, EMAILs, SNMP-Traps zu senden, einen IEC 870-5-102-Zähler zu lesen, MQTT-Nachrichten zu senden, PINGs auszuführen, den Status der Geräte-LEDs zu ändern, Dateien zu schreiben und zu lesen, Dateien über FTP zu senden oder zu empfangen usw. usf.

3. Schritt-für-Schritt-Konfiguration

Wie in den vorangegangenen Abschnitten erwähnt, erfolgt die Konfiguration von TITAN-basierten Geräten hauptsächlich über die Webumgebung.

Was wird benötigt?

- Ein PC mit Webbrowser (Chrome, Brave, Firefox, ...) und Ethernet-Anschluss
- Ein Ethernet-Kabel, um den PC mit dem Gerät zu verbinden

Schritte für den Zugriff auf die Konfigurationsumgebung

- Schließen Sie ein Ethernet-Kabel zwischen dem PC und dem Gerät an.
- Der PC muss eine feste IP-Adresse im Bereich 192.168.1.X als IP-Adresse für 192.168.1.2 haben
- Öffnen Sie einen Browser, mit der Adresse <http://192.168.1.2>. Es sollte ein Fenster wie das folgende erscheinen:



- Verwenden Sie den Standard-Benutzernamen und das Standard-Passwort: admin und admin

4. Einstellung

4.1 Mobile

Der Bereich Mobile deckt alles ab, was mit den 4G/3G/2G-Einstellungen des Geräts zu tun hat, vom Verbindungsstatus über die Netzkonfigurationsparameter bis zur Verbindungsüberwachung.

4.1.1 Mobile > Status

Dieser Bildschirm zeigt den allgemeinen Status des Geräts an.

- Firmware-Version: FW-Version des Geräts
- WAN Mobile IP: WAN-IP-Adresse (IP-Adresse, die der 4G/3G/2G-Verbindung zugewiesen ist), falls verfügbar
- GSM-Modul: gibt den Hersteller und das Modell des internen GSM-Moduls des Geräts an.
- Network (2g/3g/4g): Zeigt an, ob die aktuelle WAN-Verbindung das 2G- (GPRS), 3G- oder 4G-Netzwerk verwendet
- Signalstärke: Zeigt die Stärke des Signals an. 0=null, 31=maximal
- Zusätzliche Signalinformationen: für 3G- und 4G-Verbindungen, zeigt RSCP/ECNO und RSRP/RSRQ an
- Interne Temperatur: zeigt die interne Temperatur des Prozessors an



4.1.2 Mobile > Basic Settings

In diesem Abschnitt können Sie die Parameter der 4G/3G/2G-WAN-Verbindung konfigurieren. Sie benötigen einige Informationen über Ihre SIM-Karte, z. B. APN, Login und Passwort. Ihr Lieferant muss sie Ihnen zur Verfügung stellen.

- Mobile WAN: Wenn Sie IP-Konnektivität (4G/3G/2G) benötigen, setzen Sie diese Option auf „Aktiviert“. Wenn Sie keine SIM-Karte verwenden wollen, setzen Sie sie auf „Deaktiviert“.
- Sim-Mode: Je nach Gerätemodell stehen 1 SIM-Steckplatz oder 2 SIM-Steckplätze zur Verfügung. Wenn Sie 2 SIM-Steckplätze haben: „SIM1“ wird der Router SIM1 verwenden. „SIM2“ wird der Router „SIM2“ verwenden. „SIM1 + SIM2 (Backup)“: Der Router verwendet SIM1 und im Falle von Problemen wird SIM2 verwendet.
- SIM1 APN: APN des Netzbetreibers von SIM1. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM1 Username: Benutzername des SIM1-Betreibers. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM1 Password: SIM-1 Betreiberpasswort. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM1 Pin: Wenn Ihre SIM1-Karte eine PIN hat, müssen Sie diese hier angeben.
- SIM2 APN: APN des SIM2-Betreibers. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM2 Username: Benutzername des SIM2-Betreibers. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM2-Password: SIM2-Betreiberpasswort. Sie sollten sich bei Ihrem GSM-Anbieter erkundigen
- SIM2 Pin: Wenn Ihre SIM2-Karte eine PIN hat, müssen Sie diese hier angeben.
- Authentication: Sie müssen die Authentifizierungsmethode „PAP“ oder „CHAP“ angeben. Es wird empfohlen, den Standardwert auf „AUTO“ zu setzen.
- Auswahl des Netzes:
 - Auto (4G/3G/2G): Das Gerät verwendet 4G, wenn eine Netzabdeckung vorhanden ist, und andernfalls 3G oder 2G.
 - Auto (4G/2G): Das Gerät verwendet 4G, wenn es Netzabdeckung gibt, und andernfalls 2G.
 - 4G: Die Geräte müssen in jedem Fall das 4G-Netz nutzen. Wenn es keine 4G-Abdeckung gibt, schaltet das Gerät nicht auf 2G oder 3G um
 - 3G: Das Gerät nutzt in jedem Fall das 3G-Netz. Wenn es keine 3G-Abdeckung gibt, schaltet das Gerät nicht auf 2G um.
 - 2G: Das Gerät nutzt in jedem Fall das 2G-Netz.
- DNS selection:
 - mit der Option „Get DNS from Operator“ werden die vom Gerät verwendeten DNS von der Telefongesellschaft zugewiesen.
 - „Selected DNS servers“ bedeutet, dass die DNS-Server verwendet werden, die in den unten beschriebenen Parametern DNS1 und DNS2 angegeben sind.

- DNS1 und DNS2: DNS-Server für die Auflösung von Domännennamen. Wir empfehlen die Verwendung von Googles 8.8.8.8 und 8.8.4.4 oder die von Ihrem Provider angegebenen Werte. Diese DNS werden verwendet, wenn die FailOver-Funktion ausgewählt wird, wenn die Datenausgabe über die 4G/3G/2G-WAN-Schnittstelle erfolgt
- Remote-Webserver management: Wenn Sie das Kontrollkästchen aktivieren, können Sie aus der Ferne auf die Webkonfiguration des Geräts zugreifen, und zwar über seine öffentliche IP-Adresse (die in Mobile > Status angegeben ist). Sie können den Port über das Menü Other >Http / Https ändern4

The screenshot displays the webdyn configuration interface, powered by TITAN and flexitron group. The left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Firewall (Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, Modem Settings). The main content area is titled 'Mobile > Basic Settings' and contains the following configuration options:

Configuration Item	Value	Description
Mobile WAN	Enabled (IP active)	Enable Wireless WAN interface
Sim Mode	SIM1 + SIM2 (backup)	Sim selection
SIM1 APN:	movistar.es	APN of SIM card 1
SIM1 Username:	MOVISTAR	Username of SIM card 1
SIM1 Password:	*****	Password of SIM card 1
SIM1 Pin:		PIN of SIM card 1
SIM2 APN:	movistar.es	APN of SIM card 2
SIM2 Username:	MOVISTAR	Username of SIM card 2

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.1.3 Mobile > Keep Online

Auf diesem Bildschirm können Sie einen PING konfigurieren, um die Konnektivität des Geräts sicherzustellen. Im Falle eines PING-Fehlers zu den konfigurierten Zeiten wird die 4G/3G/2G-Verbindung neu gestartet. Es ist ratsam, diese Funktion zu nutzen.

- Enabled: Aktivieren Sie das Kontrollkästchen, damit das TITAN-basierte Gerät in regelmäßigen Abständen einen PING senden kann, um die Verbindung zu überprüfen
- Ping Server: gibt die IP- oder DNS-Adresse des Servers an, gegen den gepingt werden soll
- Period: gibt an, wie viele Minuten lang ein PING-Check durchgeführt werden soll
- Timeout: gibt die Anzahl der Sekunden an, die das Gerät auf die PING-Antwort warten muss, bevor es den PING als fehlgeschlagen betrachtet
- Retries: gibt die Anzahl der PING-Wiederholungen an, die durchgeführt werden sollen, bevor Verbindungsprobleme berücksichtigt und die 4G/3G/2G-Sitzung neu gestartet wird
- Retry period: gibt die Anzahl der Minuten zwischen den Wiederholungsversuchen an

The screenshot displays the 'webdyn' interface, powered by TITAN and part of the flexitron group. The left sidebar lists configuration categories: Mobile, Ethernet, Firewall, External Devices, and VPN. The 'Mobile' section is expanded, showing 'Status', 'Basic Settings', and 'Keep Online'. The 'Keep Online' configuration page is active, showing the following settings:

- Enabled:** ☒ Enable PING method for keep online Wan Session
- Ping Server:** IP or DNS address
- Period:** Minutes between pings (1 ... 1440)
- Timeout:** Timeout in seconds (5 ... 20)
- Retries:** Number of retries (0 ... 9)
- Retry period:** Minutes between retries (1 ... 1440)

A 'SAVE CONFIG' button is located at the bottom of the configuration area.

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

4.1.4 Mobile > Basic Settings > FailOver

Dieser Konfigurationsbildschirm ist über die Schaltfläche am unteren Rand des Abschnitts Mobile > Basic Settings zugänglich.

Ermöglicht die Konfiguration der Failover-Funktion des Geräts. Zum Beispiel, um die Datenausgabe von TITAN-basierten Geräten über ihre WiFi- oder Ethernet-Schnittstelle zu konfigurieren und im Falle eines Ausfalls der Ethernet- oder WiFi-Schnittstelle die 4G/3G/2G-Schnittstelle zu aktivieren, so dass die Datenausgabe über diese Schnittstelle erfolgt, bis die WiFi- oder Ethernet-Schnittstelle die Verbindung wiederherstellt.

- Enabled: Aktivieren Sie das Kontrollkästchen, um die Failover-Funktion zu aktivieren
- IP1: um die Konnektivität der verwendeten Failover-Schnittstelle (Ethernet oder WiFi) zu überprüfen, führt das TITAN-basierte Gerät regelmäßig einen PING auf diese IP durch. Im Falle eines Fehlschlags wird der Ping auf IP2 erneut versucht
- IP2: zur Überprüfung der Konnektivität der verwendeten Failover-Schnittstelle (Ethernet oder WiFi) führt das TITAN-basierte Gerät einen PING auf dieser IP2 durch, wenn IP1 ausfällt. Im Falle eines Ausfalls wird die WAN-Schnittstelle (4G/3G/2G) aktiviert, um für die Dauer des Ausfalls der Verbindung genutzt zu werden
- Schnittstelle: Kommunikationsschnittstelle (Ethernet oder WiFi), die als primäre Datenausgangsschnittstelle verwendet wird
- 4G/3G/2G-interface: Verhalten der 4G/3G/2G-Backup-Schnittstelle. Es kann zwischen den Modi „On when failover“ und „Always on“ gewählt werden. Im „On when failover“-Modus ist die 4G/3G/2G-WAN-Schnittstelle ausgeschaltet und wird erst bei Ausfall der primären Schnittstelle (WiFi- oder Ethernet-Schnittstelle) aktiviert und dann verwendet. Im „Always on“-Modus ist die 4G/3G/2G-WAN-Schnittstelle immer aktiv, und wenn die primäre Schnittstelle (WiFi oder Ethernet) ausfällt, wird sie verwendet. Da die 4G/3G/2G-WAN-Schnittstelle bereits aktiv ist, erfolgt die Umschaltung schneller

The screenshot shows the webdyn configuration interface. At the top, the webdyn logo is displayed with the text 'powered by TITAN' and 'flexitron group'. Below the logo, a sidebar on the left contains a menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), External Devices (Logger configuration, ModBus Devices), and VPN. The main content area is titled 'Mobile > Basic Settings > WAN Failover'. It contains the following settings:

- Enabled:** A checkbox that is currently unchecked. To its right, the text 'Enable failover.' is displayed.
- IP1:** A text input field containing '8.8.8.8'. To its right, the text 'IP address for check Ethernet/Wifi connection. **Mandatory.** Example: 8.8.8.8' is displayed.
- IP2 (backup):** A text input field containing '8.8.4.4'. To its right, the text 'IP or DNS address for check Ethernet/Wifi connection. Example: 8.8.4.4' is displayed.
- Interface:** A dropdown menu showing 'Ethernet (eth0)'. To its right, the text 'Interface for failover' is displayed.
- Period:** A dropdown menu showing '5 seconds'. To its right, the text 'Connectivity checking period' is displayed.
- 4G/3G/2G interface:** A dropdown menu showing 'On when failover (slow mode)'. To its right, the text 'Behaviour of 4G/3G/2G interface' is displayed.

At the bottom of the main content area, there is a 'SAVE CONFIG' button.

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

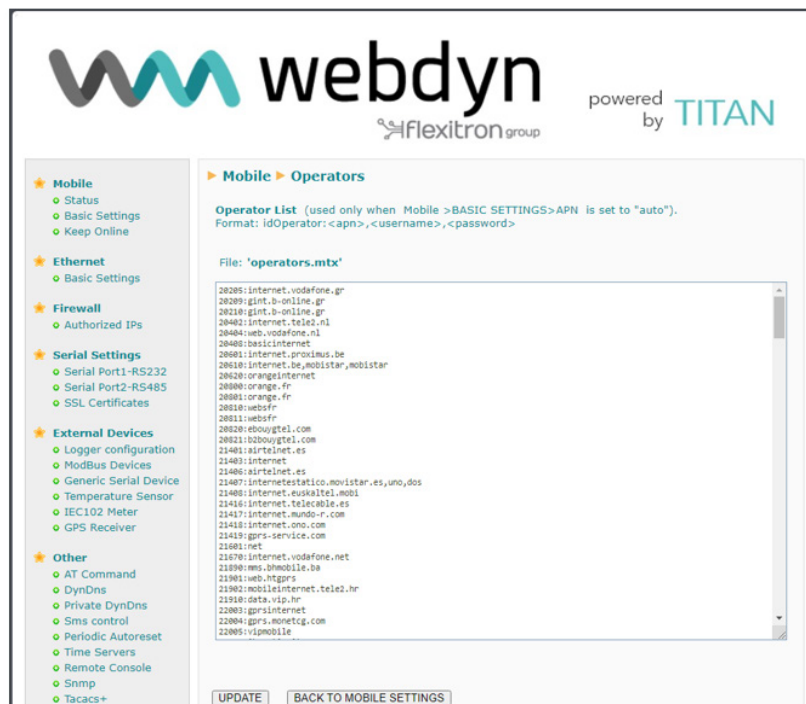
4.1.5 Mobile > Grundeinstellungen > Bediener

Dieser Konfigurationsbildschirm ist über die Schaltfläche am unteren Rand des Abschnitts Mobile> Basic Settings zugänglich.

Hier können Sie den APN, den Benutzer und das Passwort konfigurieren, die im Falle eines automatischen APN verwendet werden sollen. Sie können den APN im automatischen Modus verwenden, indem Sie den Text „auto“ (ohne Anführungszeichen) in den APN-Feldern im Abschnitt Mobile > Grundeinstellungen angeben.

Die Datei „operators.mtx“ muss das folgende Format haben:

<ID_Operator>:<apn>,<username>,<password> (wobei <username>,<password> optional sind)



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.2 Ethernet

Der Konfigurationsabschnitt „Ethernet“ bezieht sich auf den Konfigurationsteil der Ethernet-Ports der TITAN-basierten Geräte.

4.2.1 Ethernet > Basic Settings

In diesem Abschnitt können Sie die grundlegenden Netzwerkparameter der Ethernet-Verbindung konfigurieren. Dieses Menü unterscheidet sich geringfügig, je nachdem, ob das TITAN-basierte Gerät über einen oder mehrere Ethernet-Anschlüsse verfügt.

TITAN-basierte Geräte mit 1 Ethernet-Anschluss

The screenshot shows the webdyn TITAN configuration interface. At the top, there is a logo for 'webdyn flexitron group' and the 'TITAN' logo with the tagline 'Makes your APPLICATION happen'. On the left, a sidebar menu lists various settings: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), and Serial Settings. The main content area is titled 'Ethernet > Basic Settings > LAN Port'. It contains several input fields for configuration: IP Address (192.168.1.2), IP Subnet Mask (255.255.255.0), IP Gateway (empty), DNS 1 (empty), and DNS 2 (empty). To the right of these fields are labels: 'Local IP LAN', 'Local Mask', 'IP Gateway (Leave blank if not used)', 'DNS Server 1', and 'DNS Server 2'. At the bottom of the main area are two buttons: 'SAVE CONFIG' and 'REFRESH'.

- IP-Adresse: statische lokale IP-Adresse der Ethernet-Schnittstelle (Standard 192.168.1.2)
- IP-Subnet Mask: Subnetzmaske (Standard 255.255.255.0)
- IP-Gateway: IP-Adresse des ausgehenden Gateways (nur wenn der WAN-Port im WAN-Modus konfiguriert ist)
- DNS1: Primärer DNS-Server
- DNS2: sekundärer DNS-Server

TITAN-basierte Geräte mit mehreren Ethernet-Anschlüssen

The screenshot shows the webdyn TITAN configuration interface. The top header includes the webdyn logo and the TITAN logo with the tagline "Makes your APPLICATION happen". The left sidebar contains a navigation menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs, MAC Filter, Routes), Serial Settings (Serial Port1-RS232, Serial Port2-RS232, Serial Port3-RS485, Serial Port4-TTL, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor). The main content area is divided into two sections: "Ethernet Basic Settings WAN Port" and "Ethernet Basic Settings LAN Ports". The WAN Port section includes fields for IP mode (static), IP Address (192.168.10.2), IP Subnet Mask (255.255.255.0), IP Gateway, DNS 1, DNS 2, and a checkbox for Remote webserver management. The LAN Ports section includes fields for IP Address (192.168.1.2) and IP Subnet Mask (255.255.255.0). At the bottom of the LAN Ports section are buttons for "SAVE CONFIG" and "REFRESH".

Bei Geräten mit mehr als einem Ethernet-Anschluss gibt es immer 1 WAN-Anschluss und die übrigen LAN-Anschlüsse.

Konfiguration des WAN-Anschlusses

- IP-Modus: ermöglicht die Verwendung einer statischen oder dynamischen (DHCP) IP-Konfiguration für den WAN-Port
- IP-Adresse: statische lokale IP-Adresse der Ethernet-WAN-Schnittstelle (Standard 192.168.1.2)
- IP-Subnet Mask: Subnetzmaske der Ethernet-WAN-Schnittstelle (Standard 255.255.255.0)
- DNS1: Primärer DNS-Server
- DNS2: sekundärer DNS-Server
- IP-Gateway: IP-Adresse des ausgehenden Gateways

Konfiguration der LAN-Anschlüsse

- IP-Adresse: statische lokale IP-Adresse der Ethernet-LAN-Schnittstelle (Standard 192.168.10.2)
- IP-Subnet Mask: Subnetzmaske der Ethernet-LAN-Schnittstelle (Standard 255.255.255.0)

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

4.2.2 Ethernet > DHCP-Server

In diesem Abschnitt können Sie den DHCP-Server aktivieren und konfigurieren, der an der Ethernet-Schnittstelle des TITAN-basierten Geräts zugewiesen ist.

- Enabled: Wenn Sie das Kontrollkästchen aktivieren, wird der DHCP-Server auf der Ethernet-Schnittstelle aktiviert
- Starting IP Address: gibt die erste IP-Adresse an, die vom DHCP-Server zugewiesen wird
- Ending IP Address: gibt die letzte IP-Adresse an, die vom DHCP-Server zugewiesen wurde
- MAC-Adresse / IP-Adresse: Mit diesen beiden Parametern kann der DHCP-Server einer bestimmten MAC-Adresse immer dieselbe IP-Adresse zuweisen

webdyn powered by **TITAN**
flexitron group

★ **Mobile**

- Status
- Basic Settings
- Keep Online

★ **Ethernet**

- Basic Settings
- DHCP Server

★ **Firewall**

- NAT
- Authorized IPs

★ **External Devices**

- Logger configuration
- ModBus Devices

★ **VPN**

- IPsec
- OpenVPN Client
- OpenVPN Server

▶ **Ethernet > DHCP Server**

Enabled: ☒ DHCP Server enabled / disabled

Starting IP Address: First IP address for DHCP (ex 192.168.1.100)

Ending IP Address: Last IP address for DHCP (ex 192.168.1.110)

SAVE CONFIG

MAC Address	IP Address	
00:06:01:09:24:2C	192.168.1.100	Delete

MAC Address: Set a MAC address (ex 54:42:49:0A:E9:2C)

IP Address: Set assigned IP address (ex 192.168.1.120).
Important note: This IP must be outside the previous range of automatic assignment

SAVE RULE

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Drücken Sie die Taste „SAVE RULE“ für jedes MAC/IP-Paar, das Sie erstellen möchten. Sie können bis zu 10 Paare erstellen.
- Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

4.3 WiFi

Der Konfigurationsbereich „WiFi“ bezieht sich auf den Konfigurationsteil des WiFi-Interface. Mit einer WiFi-Konfiguration im „Access Point“-Modus können Sie z. B. WiFi-Client-Geräten einen Internetzugang ermöglichen oder Ihre eigenen TITAN-basierten Geräte konfigurieren. Durch eine Konfiguration im „WiFi Client“-Modus können Sie das TITAN-basierte Gerät dazu bringen, einen anderen WiFi-Zugangspunkt in

Ihren Räumlichkeiten als Zugang zum Internet zu nutzen.

4.3.1 WiFi > Basic Settings

In diesem Abschnitt können Sie die grundlegenden Netzwerkparameter des WiFi-Schnittstellen konfigurieren.

- **Enabled:** Wenn Sie das Kontrollkästchen aktivieren, wird die WiFi-Schnittstelle des TITAN-basierten Geräts aktiviert
- **WiFi mode:** Hier können Sie zwischen den Betriebsarten „WiFi Access Point“ und „WiFi Client“ wählen. Verwenden Sie den Modus „WiFi Access Point“, wenn Sie das TITAN-basierte Gerät verwenden möchten, um WiFi-Geräten über die 4G/3G/2G-Schnittstelle einen Internetzugang zu ermöglichen. Verwenden Sie „WiFi Client“, wenn Sie eine vorhandene WiFi-Infrastruktur (z. B. den Glasfaser-Router eines Unternehmens) als Internetanschluss nutzen möchten.
- **WiFi SSID:** Öffentliche SSID (im Modus „WiFi Access Point“ wird die SSID angegeben, die vom TITAN-basierten Gerät erstellt werden soll, im Modus „WiFi Client“ wird die SSID angegeben, mit der sich das TITAN-basierte Gerät verbinden wird)
- **Security:** Hier können Sie den WiFi-Sicherheitsmodus festlegen. WPA2 empfohlen
- **KEY:** gibt das WiFi-Passwort an, das für den WPA2-Modus erforderlich ist
- **IP Mode:** Geben Sie im Modus „WiFi-Client“ an, ob eine statische IP-Adresse als lokale WiFi-IP-Adresse verwendet werden soll oder ob die IP über DHCP bezogen werden soll
- **IP-Adresse:** IP-Adresse des WiFi-Schnittstellen. Standard 192.168.2.1
- **Subnet Mask:** Subnetzmaske der WiFi-Schnittstelle
- **DNS1:** Primärer DNS-Server
- **DNS2:** sekundärer DNS-Server
- **IP Gateway:** Im Modus „WiFi Client“ können Sie das Gateway angeben, wenn die lokale IP statisch ist
- **Internet Access:** Aktivieren Sie die Möglichkeit, über ein WiFi-Gerät auf das Internet zuzugreifen
- **LAN Access:** Aktivieren Sie diese Option, um von einem WiFi-Gerät aus auf Geräte zuzugreifen, die an den Ethernet-Port des Computers angeschlossen sind


webdyn
 powered by TITAN


- ★ **Mobile**
 - Status
 - Basic Settings
 - Keep Online
- ★ **Ethernet**
 - Basic Settings
- ★ **Wifi**
 - Basic Settings
 - DHCP Server
- ★ **Firewall**
 - NAT
 - Authorized IPs
- ★ **Serial Settings**
 - Serial Port1-RS232
 - Serial Port2-RS485
 - SSL Certificates
- ★ **External Devices**
 - Logger configuration
 - ModBus Devices
 - Generic Serial Device
 - Temperature Sensor
 - IEC102 Meter
 - W-MBus
 - GPS Receiver
- ★ **Other**
 - AT Command

► Wifi ► Basic Settings

Enabled:	Disabled ▼	Enable Wifi
Wifi mode:	Wifi Access Point ▼	Select between Wifi Access Point or Wifi Client
Wifi SSID:		Select the public name for the Wifi Network
Security:	OPEN ▼	Select security mode
KEY:		Password for WPA2-Personal security mode
Channel:	1 ▼	Wifi Channel

IP Address:	192.168.2.1	Local IP LAN
IP Subnet Mask:	255.255.255.0	Local Mask
DNS 1:	8.8.8.8	DNS Server 1
DNS 2:	8.8.4.4	DNS Server 2
IP Gateway:		Left blank if not used or using another WAN interface

Internet access:	☐	Check if wifi devices can access to Internet
LAN access:	☐	Check if wifi devices can connect with LAN devices

SAVE CONFIG

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

4.3.2 WiFi > DHCP-Server

In diesem Abschnitt können Sie den DHCP-Server aktivieren und konfigurieren, der dem WiFi-Schnittstelle des TITAN-basierten Geräts zugewiesen wurde.

- Enabled: Wenn Sie das Kontrollkästchen aktivieren, wird der DHCP-Server der WiFi-Schnittstelle aktiviert.
- Starting IP Address: gibt die erste IP-Adresse an, die vom DHCP-Server zugewiesen wird
- Ending IP Address: gibt die letzte IP-Adresse an, die vom DHCP-Server zugewiesen wurde
- MAC-Adresse / IP-Adresse: Mit diesen beiden Parametern kann der DHCP-Server einer bestimmten MAC-Adresse immer dieselbe IP-Adresse zuweisen

The screenshot displays the webdyn DHCP Server configuration page. The header includes the webdyn logo and 'powered by TITAN'. The left sidebar lists various configuration categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration). The main content area is titled 'Wifi > DHCP Server' and contains the following fields and controls:

- Enabled:** A checkbox to toggle the DHCP server on or off. Text: 'DHCP Server enabled / disabled'.
- Starting IP Address:** A text input field. Text: 'First IP address for DHCP (ex 192.168.2.100)'.
- Ending IP Address:** A text input field. Text: 'Last IP address for DHCP (ex 192.168.2.110)'.
- SAVE CONFIG:** A button to save the DHCP server configuration.
- MAC Address:** A text input field. Text: 'Set a MAC address (ex 54:42:49:0A:E9:2C)'.
- IP Address:** A text input field. Text: 'Set assigned IP address (ex 192.168.2.120)'. Below this field is an important note: 'Important note: This IP must be outside the previous range of automatic assignment'.
- SAVE RULE:** A button to save a specific MAC/IP rule.

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Drücken Sie die Taste „SAVE RULE“ für jedes MAC/IP-Paar, das Sie erstellen möchten. Sie können bis zu 10 erstellen. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden

4.4 Firewall

Abschnitt zur Konfiguration der Sicherheitsaspekte des Geräts.

4.4.1 Firewall > NAT

Abschnitt, von dem aus Anschlüsse für den externen Zugriff auf interne Geräte, die mit dem Gerät verbunden sind, zugeordnet werden können. Wenn Sie beispielsweise eine IP-Kamera an den Ethernet-Anschluss des TITAN-basierten Geräts angeschlossen haben und von einem entfernten Computer darauf zugreifen möchten, muss dieser Abschnitt entsprechend konfiguriert werden. Sie können insgesamt bis zu 10 Regeln erstellen.

- Service name: Beschreibender Name für eine Zuordnungsregel
- Protocol: gibt das Protokoll der Anschlusszuordnung an. TCP, UDP oder beides
- Input port: gibt den Eingangsport zum TITAN-basierten Gerät über die WAN-Schnittstelle an
- Output port: gibt den Anschluss für die Weiterleitung an das interne Gerät an, das an das TITAN-basierte Gerät angeschlossen ist
- Server-IP-Adresse: IP-Adresse des extern zu steuernden Geräts (z. B. IP-Adresse einer Kamera)
-

Service name	Protocol	Input Port	Output Port	Server IP Address
	TCP+UDP			

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden
- Denken Sie auch daran, dass für eine korrekte Durchführung eines NAT:

- Die LAN-IP-Adresse des zu steuernden Geräts muss innerhalb des Netzwerkbereichs der LAN-IP-Adresse des TITAN-basierten Geräts liegen
- Die Gateway-IP-Adresse des zu steuernden Geräts muss die LAN-IP-Adresse des TITAN-basierten Geräts sein. Siehe die Beispiele im Anhang für weitere Informationen
- Die Schnittstelle für NAT kann angegeben werden. Wenn Sie das Dienstprogramm nicht kennen, verwenden Sie die Option „auto“. Die Verwendung dieser Option kann z. B. für OpenVPN nützlich sein, wenn Sie über NAT auf Geräte zugreifen wollen, die am Ethernet-Port hängen (und somit die gleiche Konfiguration für den Fernzugriff auf verschiedene Punkte haben)

4.4.2 Firewall > Authorized IPs

Auf diesem Bildschirm können Sie bis zu 3 IP-Adressen festlegen, die berechtigt sind, Verbindungen über die WAN-Schnittstelle für die verschiedenen Dienste des Geräts zu akzeptieren. Wenn Sie eine autorisierte IP-Adresse 90.166.108.200 (z. B. Ihre Büro-IP-Adresse) angeben, sind bestimmte Dienste der TITAN-basierten Geräte nur von dieser IP-Adresse aus zugänglich.

- Authorized IP1: Autorisierte IP-Adresse Nummer 1
- Authorized IP2: Autorisierte IP-Adresse Nummer 2
- Authorized IP3: Autorisierte IP-Adresse Nummer 3
- Router configuration: Legt fest, ob Fernverbindungen zur Web-Konfigurationsumgebung des Geräts von jeder IP-Adresse oder nur von autorisierten IP-Adressen akzeptiert werden sollen.
- Serielle Gateways: gibt an, ob Fernverbindungen zu 4G/3G/2G-RS232/485-Gateway-Diensten von jeder IP oder nur von autorisierten IP-Adressen akzeptiert werden.
- Remote console: gibt an, ob Fernverbindungen zum Remote-Konsolendienst (Telnet oder SSH) von jeder IP-Adresse oder nur von autorisierten IP-Adressen akzeptiert werden sollen.
- NAT: gibt an, ob Fernverbindungen zu den zugeordneten Ports des Geräts von jeder IP-Adresse oder nur von autorisierten IP-Adressen akzeptiert werden sollen.
- ModBus TCP Slave: gibt an, ob Fernverbindungen zum Modbus-TCP-Slave-Dienst des TITAN-basierten Geräts von jeder IP oder nur von autorisierten IP-Adressen akzeptiert werden.
- SNMP: gibt an, ob Fernverbindungen zum SNMP-Dienst des TITAN-basierten Geräts von jeder IP-Adresse oder nur von autorisierten IP-Adressen akzeptiert werden sollen.
- OpenVPN: gibt an, ob Fernverbindungen zum Dienst „OpenVPN Server“ des TITAN-basierten Geräts von jeder IP-Adresse oder nur von autorisierten IP-Adressen akzeptiert werden sollen.
- PING: antwortet nur auf PING-Anfragen, die von autorisierten IPs gestellt werden
- Outgoing Connections: Hier können Sie festlegen, ob das TITAN-basierte Gerät den Internetzugang für alle IP-Adressen oder nur für autorisierte IP-Adressen bereitstellen kann. Stellen Sie sich zum Beispiel vor, dass Sie wollen, dass nur Ethernet- oder WiFi-Geräte, die mit dem TITAN verbunden sind, Daten an Ihren Server senden können, um zu verhindern, dass das Gerät für andere Aktionen (Internet-Browsing usw.) missbraucht wird

The screenshot shows the webdyn configuration interface. At the top, the webdyn logo is displayed with the tagline 'powered by TITAN' and 'flexitron group'. On the left, a sidebar menu lists various configuration categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter). The main content area is titled 'Firewall > Authorized IPs (for WAN interfaces)'. It contains three input fields for 'Authorized IP1:', 'Authorized IP2:', and 'Authorized IP3:', each followed by the text 'Remote connections from this IP are allowed'. Below these are several dropdown menus for security settings: 'Router configuration:' (ALLOW ANY IP), 'Serial gateways:' (ONLY AUTHORIZED IP), 'Remote console:' (ALLOW ANY IP), 'ModBus TCP Slave:' (ALLOW ANY IP), 'SNMP:' (ALLOW ANY IP), 'TCP & UDP exceptions:' (ALLOW ANY IP), and 'PING:' (ALLOW ANY IP). Each dropdown is followed by a description of the security setting. At the bottom of the main area is a 'SAVE CONFIG' button.

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden
- IP-Beschränkungen gelten nur auf der Ebene der WAN-Verbindung. Der WiFi-Zugang wird durch den WPA2-Netzwerkschlüssel selbst geschützt. Das heißt, wenn Sie WiFi haben und Sicherheit benötigen, aktivieren Sie WPA2 im Abschnitt WiFi > Basic Settings
- Wenn Sie die Einschränkung „Outgoing connections“ verwenden, denken Sie daran, dass Sie die IP-Adresse des zu verwendenden DNS-Servers angeben müssen, wenn Sie Domännennamen anstelle von IP-Adressen verwenden
- Wenn Sie mehr als 3 zugelassene IP-Adressen benötigen, können Sie in jedem Feld mehrere IP-Adressen angeben, wobei Sie diese durch Komma „“,“ trennen

4.4.3 Firewall > MAC Filter

In diesem Abschnitt können Sie das Gerät so konfigurieren, dass die Kommunikation über die Ethernet- (oder WLAN-) Schnittstelle auf der Grundlage von MAC-Adressen gefiltert wird.

- Modus - Alle MACs erlaubt, außer den aufgelisteten: Alle MAC-Adressen sind erlaubt, mit Ausnahme der in der Liste aufgeführten MAC-Adressen, die gesperrt werden. Das ist die Standardkonfiguration.
- Modus - Nur aufgelistete MAC erlaubt: Alle MAC-Adressen werden gesperrt, mit Ausnahme der in der Liste aufgeführten MAC-Adressen, die zugelassen werden.
- MAC-Liste: Liste der erlaubten oder gesperrten Adressen, abhängig von der Betriebsart.



4.4.4 Firewall > Routen

In diesem Abschnitt können Sie das Gerät so konfigurieren, dass bis zu 5 Leitwege pro Schnittstelle hinzugefügt werden.

- Netzwerk - Gibt das Netzwerk an, für das die Route konfiguriert werden soll.
- Maske - Gibt die Netzmaske für die zu konfigurierende Route an.
- Gateway - IP-Adresse des Gateways, das für die zu konfigurierende Route verwendet werden soll.
- Schnittstelle - Physikalische Schnittstelle der zu konfigurierenden Route.



4.5 Serial Settings > Serial portX

Im Abschnitt „Serial Settings“ können Sie die Konfiguration jeder seriellen Schnittstelle des TITAN-Geräts (Geschwindigkeit, Parität, ...) sowie die spezielle Funktion jeder Schnittstelle (IP-serielle Gateways, Modbus TCP-RTU Gateways, ...) festlegen.

4.5.1 Serial Settings > Serial portX

TITAN-basierte Geräte haben mehrere serielle Schnittstellen. Sie können 4G/3G/2G-Serial- und CSD-Serial-Gateways realisieren, um RS232- oder RS485-Geräte fernzusteuern. Die Anzahl der seriellen Schnittstellen des Typs RS232 oder RS485 hängt vom Modell des verwendeten TITAN-basierten Geräts ab.

- Baudrate: gibt die Geschwindigkeit der seriellen Schnittstelle (115200, ... , 300) an
- Data bits: gibt die Anzahl der Datenbits (7, 8) an
- Parity: gibt die Parität an (none [keine], even [gerade], odd [ungerade])
- Stop bits: Anzahl der Stoppbits (1, 2)
- Flow Control: legt die Durchflussregelung fest (none [keine], Hardware)
- Timeout ms: gibt die Millisekunden an, die gewartet werden soll, bevor Daten über IP gesendet werden, ohne dass Daten über den seriellen Anschluss empfangen werden. Wenn Sie eine „0“ (Standardwert) angeben, werden die Daten über IP gesendet, sobald sie an der seriellen Schnittstelle ankommen. Eine Zahl wie z. B. 10 gibt an, dass keine Daten gesendet werden, wenn nicht mindestens 10 ms lang keine Daten an der seriellen Schnittstelle empfangen werden. Dadurch kommen die Daten weniger fragmentiert am Zielort an.
- Allow local embedded AT Commands: Das Aktivieren dieses Kontrollkästchens ermöglicht das

Senden von LOKALEN AT-Befehlen, die in einem 4G/3G/2G-Serial-Gateway vom Typ Server oder Client eingebettet sind. AT-Befehle müssen über die serielle RS232- oder RS485-Schnittstelle des TITAN-basierten Geräts gesendet werden, jedoch gekapselt zwischen den Tags <MTXTUNNEL> und </MTXTUNNEL>. Wenn zum Beispiel eine Abdeckung gewünscht wird, kann der Befehl <MTXTUNNEL>AT+CSQ</MTXTUNNEL> gesendet werden. Oder wenn Sie ein Gerät aus der Ferne zurücksetzen wollen, können Sie den Befehl <MTXTUNNEL>AT^MTXTUNNEL=REBOOT</MTXTUNNEL> senden.

- Allow remote embedded AT Commands: Wenn Sie dieses Kontrollkästchen aktivieren, können Sie REMOTE-AT-Befehle senden, die in ein 4G/3G/2G-Serial-Gateway vom Typ Server oder Client eingebettet sind. AT-Befehle müssen über die bestehende Gateway-Verbindung gesendet werden, aber gekapselt zwischen den Tags <MTXTUNNELR> und </MTXTUNNELR>. Wenn zum Beispiel eine Abdeckung gewünscht wird, kann der Befehl <MTXTUNNELR>AT+CSQ</MTXTUNNELR> gesendet werden. Oder wenn Sie ein Gerät aus der Ferne zurücksetzen wollen, können Sie den Befehl <MTXTUNNELR>AT^MTXTUNNEL=REBOOT</MTXTUNNELR> senden.
- Allow incoming GSM call (CSD Data Call): Wenn Sie dieses Kontrollkästchen aktivieren, wird ein Anruf vom Typ CSD über die serielle Schnittstelle akzeptiert. Funktioniert nur, wenn der Anschluss als TCP-Server- oder TCP-Client-Gateway konfiguriert ist und in einigen Fällen (z. B. IEC-102-Zählerauslesung), wenn er als „Nothing or Used by External Devices (Nichts oder von externen Geräten verwendet)“ konfiguriert ist. Wenn ein CSD-Anruf empfangen und angenommen wird, werden die IP-Verbindungen unterbrochen, bis der CSD-Anruf beendet ist
- Funktion: Nothing or Used by External Device: Wählen Sie diese Betriebsoption, wenn Sie einen bestimmten seriellen Anschluss nicht als IP-/serielles Gateway verwenden möchten oder wenn der serielle Anschluss (RS232 oder RS485) von einem externen Gerät verwendet werden soll, das im Konfigurationsabschnitt „External Devices“ angegeben ist. Wenn Sie zum Beispiel einen Temperatursensor oder ein anderes im Menü „External Devices“ angegebenes Gerät verwenden möchten, müssen Sie diese Option auswählen
- Funktion: Serial - IP-Gateway (TCP-Server): Wählen Sie diese Betriebsoption, wenn Sie ein transparentes Seriell-4G/3G/2G-Gateway im TCP-Server-Modus einrichten möchten, d.h. ein Szenario, bei dem das TITAN-basierte Gerät auf einem bestimmten TCP-Port lauscht und darauf wartet, eine Verbindung zum Aufbau des Gateways zu erhalten
- TCP Local Port: TCP-Abhörport für das serielle Gateway - 4G/3G/2G
 - Timeout: Zeit (Sekunden) ohne Daten auf dem Gateway, um den Socket automatisch zu schließen.
 - TCP Lokaler Prioritätsanschluss: vorrangiger TCP-Port für serielles Gateway - 4G/3G/2G. Wenn eine aktive Verbindung auf diesem Port besteht, werden Verbindungen auf dem TCP Local Port nicht zugelassen. Nützlich für die Ablesung von Stromzählern mit IP-Anschlusspriorität.
- Temporärer RS232-Client: Wählen Sie diese Option, wenn Sie einen temporären Socket aktivieren möchten, wenn Sie im TCP-Server-Modus arbeiten, aber das IP/Serial-Gateway nicht eingerichtet ist und Sie Daten über die serielle Schnittstelle empfangen. Wenn Sie diese Option aktivieren, müssen die Parameter „Remote IP“, „Remote TCP Port“ und „ID String“ im Abschnitt TCP-Client richtig konfiguriert sein
- Temporärer Client-Wakeup: Mit dieser Option können Sie einen temporären Socket aktivieren, wenn Sie im TCP-Server-Modus arbeiten, aber das IP/Seriell-Gateway nicht eingerichtet ist und die konfigurierte Zeit erreicht ist. Wenn Sie diese Option aktivieren, müssen die Parameter „Remote IP“, „Remote TCP Port“ und „ID String“ im Abschnitt TCP-Client richtig konfiguriert sein
- Temporal client Time: gibt die Zeit an, die ein temporärer Socket aktiv ist

- Temporärer Client Random: Es ist möglich, eine zufällige Zeit in Sekunden für einen temporären Client festzulegen, die zur Wakeup-Zeit hinzugefügt wird. Dies ist nur sinnvoll, wenn Sie eine große Anzahl von Computern haben, die gleichzeitig eine Verbindung herstellen, und Sie eine zufällige Zeit eingeben möchten, um die Anzahl der gleichzeitigen Verbindungen auf einen Server zu verteilen
- SSL/TLS: Wenn TCP Server Gateways gesichert werden müssen, kann dies mit dieser Option erreicht werden. Falls aktiviert, muss auch der Zertifikatsbereich „Serial Settings > SSL Certs“ konfiguriert werden
- Funktion: Serial - IP-Gateway (TCP-Client): Wählen Sie diese Betriebsoption, wenn Sie ein transparentes Seriell - 4G/3G/2G-Gateway im TCP-Client-Modus einrichten möchten, d.h. ein Szenario, bei dem sich das TITAN-basierte Gerät mit einem bestimmten IP-/TCP-Port verbindet, um das Seriell - 4G/3G/2G-Gateway einzurichten
- Remote IP: IP-Adresse, mit der sich das TITAN-basierte Gerät verbinden wird
- Remote TCP Port: TCP-Port, mit dem sich das TITAN-basierte Gerät verbinden wird
- Reconnection time: gibt an, wie viele Millisekunden zwischen den Verbindungsversuchen verbleiben sollen, falls die Verbindung fehlschlägt oder es zu Verbindungsproblemen kommt. 0 = sofortige Wiederherstellung der Verbindung. Seien Sie vorsichtig mit diesem Wert, wenn Sie keine Flatrate-SIM-Karte haben oder wenn Sie ein sehr geringes monatliches Datenvolumen vertraglich vereinbart haben.
- ID String: Zeichenkette, die direkt nach der Einrichtung des Sockets mit der Remote-IP gesendet wird. Anhand dieses Textes können Sie das Gerät identifizieren, das die Verbindung herstellt. Wenn Sie zum Beispiel 100 TITAN-basierte Geräte in dieser Betriebsart haben, können Sie nach einer Verbindung unterscheiden, welches dieser 100 Geräte die Verbindung hergestellt hat.
- Funktion: Seriell - IP-Gateway (Modbus TCP / Modbus RTU): Wählen Sie diese Betriebsoption, wenn Sie ein Seriell - 4G/3G/2G-Gateway mit Modbus TCP - Modbus RTU Protokollumsetzung einrichten wollen. Verwenden Sie diese Option nicht, wenn Ihre Steuerungssoftware Modbus RTU verwendet; ein normales TCP-Server-Gateway würde ausreichen. Verwenden Sie diese Option, wenn Ihre Steuerungssoftware das Modbus TCP-Protokoll verwendet. Wenn Sie Zweifel haben, besuchen Sie bitte contact@webdyn.com
- Seriell - IP-Gateway (MQTT): Wählen Sie diese Option, wenn Sie ein IP-Seriell-Gateway über das MQTT-Protokoll einrichten möchten. Um diese Option zu nutzen, ist es notwendig, den MQTT-Client zu konfigurieren, den Sie unter „Other - MQTT“ finden
- TX Mqtt Topic: Das TITAN-basierte Gerät leitet alle über die serielle Schnittstelle empfangenen Daten (im RAW-Modus gesendete Daten) an das in diesem Parameter definierte MQTT-Topic weiter
- RX Mqtt Topic: Das TITAN-basierte Gerät abonniert das in diesem Parameter definierte MQTT-Topic und sendet alle in diesem Topic empfangenen Daten (im RAW-Modus gesendete Daten) über seine serielle Schnittstelle zurück
- Function: Seriell-IP-Gateway (UDP): Wählen Sie diese Betriebsoption, wenn Sie ein transparentes Seriell-IP-Gateway über das UDP-Protokoll einrichten möchten
- Remote IP: IP-Adresse des Fernservers, an den die Daten über UDP gesendet werden sollen
- Remote UDP-Port: UDP-Port des Fernservers

- Local UDP-Port: UDP abhörenden Port des Geräts


webdyn
flexitron group

powered by **TITAN**

- ★ Mobile
 - Status
 - Basic Settings
 - Keep Online
- ★ Ethernet
 - Basic Settings
- ★ Wifi
 - Basic Settings
 - DHCP Server
- ★ Firewall
 - NAT
 - Authorized IPs
- ★ Serial Settings
 - Serial Port1-RS232
 - Serial Port2-RS485
 - SSL Certificates
- ★ External Devices
 - Logger configuration
 - ModBus Devices
 - Generic Serial Device
 - Temperature Sensor

Serial Gateway ▶ Com1 Settings

Baudrate: Baudrate of serial port

Data bits: Number of data bit

Parity: Parity

Stop bits: Number of stop bits

Flow Control: Flow control of serial port

Timeout ms: msec without serial data before sending (default: 50)

☐ Allow local embedded AT commands Ex.: <MTXTUNNEL>AT</MTXTUNNEL>

☐ Allow remote embedded AT commands Ex.: <MTXTUNNELR>AT</MTXTUNNELR>

☒ Allow incoming GSM call (CSD Data Call) Only TCP Server and TCP Client functions or Nothing

☒ Function: Nothing or used by External Device or Script

☐ Function: Serial - IP Gateway (TCP Server)

- IoT Meter
- W-MBus
- GPS Receiver
- ★ Other
 - AT Command
 - DynDns
 - Private DynDns
 - Sms control
 - Periodic Autoreset
 - Time Servers
 - Remote Console
 - Snmp
 - Tacacs+
 - Mqtt
 - Http / Https
 - User Permissions
 - Passwords Web UI
 - CA Certificates
 - Email Config
 - ModBus Slave
 - Titan Scripts
 - Connectivity tools
 - Digital I/O
 - Custom Skin
 - Led Config
 - Syslog
 - Backup / Factory
 - Firmware Upgrade

TCP Local Port: Listening TCP Port (1 ... 65535)

Temporal client RS232 ☐

Temporal client Wakeup

Temporal client time: Seconds for temporal client

Temporal client Random Seconds. Random time for temporal client Wakeup

SSL/TLS enabled ☐ SSL/TLS Enabled (SSL Certs needed)

☐ Function: Serial - IP Gateway (TCP Client)

Remote IP: Address of remote IP server

Remote TCP Port: Port number of remote server (1 ... 65535)

Reconnection time: Milliseconds between connection attempts

ID String:

SSL/TLS enabled ☐ This identification String is sent in each connection (can be used for device identification)
SSL/TLS Enabled (CA Certs needed)
(SSL Certs needed if client authentication)

☐ Function: Serial - IP Gateway (ModBus TCP / ModBus RTU)

TCP Local Port: Listening TCP Port (1 ... 65535). Normally 502

- Reboot
- Logout

SSL/TLS enabled ☐ SSL/TLS Enabled (SSL Certs needed)

☐ Function: Serial - IP Gateway (MQTT)

TX Mqtt Topic:

RX Mqtt Topic:

All data received by RS232 will be retransmitted to this MQTT topic
All data received by IP in this MQTT topic will be retransmitted by the serial port.

☐ Function: Serial - IP Gateway (UDP)

Remote IP: Address of remote IP server (can be included several IP between ;)

Remote UDP Port: Remote UDP port (1 ... 65535)

Local UDP Port: Local UDP port (1 ... 65535)

SAVE CONFIG

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden
- Wenn eine serielle TTL-Schnittstelle erscheint, handelt es sich um eine interne serielle Schnittstelle des TITAN-basierten Geräts für spezielle Kommunikationskarten (RF868 MHz, GPS, ...), d.h. es handelt sich nicht um eine externe serielle Schnittstelle des Geräts

4.5.2 Serial Settings > SSL Certificates

Die IP-Serial-Gateways von TITAN-basierten Geräten können über SSL/TLS-Verbindungen sowohl auf TCP-Client- als auch auf TCP-Server-Verbindungen aufgebaut werden. Wenn SSL/TLS-Verbindungen verwendet werden, müssen Sie den entsprechenden Zertifikatsabschnitt konfigurieren.

Der Abschnitt Serial Gateway > SSL/TLS Certificates (TCP SERVERS) bezieht sich auf Zertifikate, wenn der COM-Port als TCP-Server-Socket konfiguriert wurde.

The screenshot shows the webdyn web interface. The top header features the webdyn logo (a stylized 'w' in blue and green) and the text 'webdyn powered by TITAN flexitron group'. On the left is a sidebar menu with categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, W-MBus, GPS Receiver). The main content area is titled 'Serial Gateway > SSL/TLS Certificates (TCP SERVERS)'. It contains two sections: 'Certificate for SSL/TLS Servers (PEM format)' and 'Certificates for authorized SSL/TLS clients (if needed) (PEM format)'. The first section has fields for 'Server certificate:' (file 'serial_server.crt') and 'Server KEY:' (file 'serial_server.key'), each with a file selection button ('Seleccionar archivo'), a status indicator ('Ninguno archivo selec.'), an 'Upload' button, and a 'not uploaded' status. Below these is a 'DELETE CERTIFICATE' button. The second section has three rows for 'Client certificate 1:', 'Client certificate 2:', and 'Client certificate 3:', each with similar file selection, status, upload, and 'not uploaded' indicators. Below these are three 'DELETE CERTIFICATE' buttons labeled 1, 2, and 3. At the bottom, there is a 'Client authentication:' checkbox (checked) and a 'Check for client authentication' button. A 'SAVE CONFIG' button is at the very bottom.

- Server Certificate: Zertifikat (PEM-Format), das von den TITAN-basierten Geräten für jeden als TCP-Server konfigurierten Dienst zu verwenden ist.
- Server KEY: privater Schlüssel des Zertifikats, das von den TITAN-basierten Geräten verwendet wird, wenn sie von TCP Server konfiguriert werden.
- Client authentication: Wenn dieses Kästchen aktiviert ist, erlaubt das TITAN-basierte Gerät nur Clients mit autorisierten Client-Zertifikaten eine Verbindung zu seinen TCP-Server-Sockets.
- Client-Zertifikat 1: Bei der Verwendung von „Client authentication“ kann in diesem Feld das autorisierte Zertifikat 1 eingegeben werden.
- Client-Zertifikat 2: Bei der Verwendung von „Client authentication“ kann in diesem Feld das autorisierte Zertifikat 2 eingegeben werden.

- Client-Zertifikat 3: Bei der Verwendung von „Client authentication“ kann in diesem Feld das autorisierte Zertifikat 3 eingegeben werden.

Der Abschnitt Serial Gateway > SSL/TLS Certificates (TCP CLIENT) bezieht sich auf Zertifikate, wenn der COM-Port als TCP-Client-Socket konfiguriert wurde

Zertifikate für TCP-Client-Sockets sind nur erforderlich, wenn der TCP-Fernserver (zu dem der TITAN-basierte Rechner eine Verbindung herstellt) eine Authentifizierung per Zertifikat benötigt.

Serial Gateway > SSL/TLS Certificates (TCP CLIENT)

Certificate for SSL/TLS TCP Client Serial Port 1 (PEM format)

Client Port1 certificate: file 'serial_cli_port1.crt' Ninguno archivo selec. **not uploaded**

Client Port1 KEY: file 'serial_cli_port1.key' Ninguno archivo selec. **not uploaded**

Certificate for SSL/TLS TCP Client Serial Port 2 (PEM format)

Client Port2 certificate: file 'serial_cli_port2.crt' Ninguno archivo selec. **not uploaded**

Client Port2 KEY: file 'serial_cli_port2.key' Ninguno archivo selec. **not uploaded**

Serial Gateway > SSL/TLS Certificates > Tools

With this tool you can generate a pair of files certificate.crt and certificate.key for your tests.

Process Status:

- Client-Port1 Certificate: Zertifikat (PEM-Format), das von TITAN-basierten Geräten verwendet wird, wenn ein serieller Port1 als TCP-Client mit SSL/TLS mit Zertifikatsidentifizierung fungiert
- Client Port1 KEY: privater Schlüssel des Zertifikats, das von TITAN-basierten Geräten verwendet wird, wenn ein serieller Port1 als TCP-Client mit SSL/TLS mit Zertifikatsidentifizierung fungiert
- Client-Port2 Certificate: Zertifikat (PEM-Format), das von TITAN-basierten Geräten verwendet wird, wenn ein serieller Port2 als TCP-Client mit SSL/TLS mit Zertifikatsidentifizierung fungiert
- Client-Port2 KEY: privater Schlüssel des Zertifikats, der von TITAN-basierten Geräten verwendet wird, wenn ein serieller Port2 als TCP-Client mit SSL/TLS mit Zertifikatsidentifizierung fungiert

Der Abschnitt Serial Gateway > SSL/TLS Certificates > ist ein Dienstprogramm, mit dem Sie bequem ein .crt- und .key-Paar für Leistungstests erzeugen können.

4.6 External Devices

In diesem Abschnitt werden der interne Datenlogger sowie externe serielle Peripheriegeräte (Temperaturfühler, Modbus RTU- oder Modbus TCP-Geräte, allgemeine RS232-485-Geräte usw.) konfiguriert.

4.6.1 External Devices > Logger configuration

Wenn Sie die TITAN-basierte Ausrüstung benötigen, um Daten von externen Geräten (Modbus-Geräte, Temperatursensoren, generische serielle Geräte, GPS-Empfänger, W-Mbus-Geräte, IEC-102-Zähler, ...) zu sammeln und an einen externen Server zu senden, müssen Sie zunächst den internen Logger konfigurieren, d.h. wie die Daten gesammelt werden sollen, wo und wie sie gesendet werden sollen. Dafür ist dieser Abschnitt gedacht.

In diesem Abschnitt können Sie die Parameter für den internen Datenlogger konfigurieren. Sie können die Daten über HTTP/HTTPS, FTP/FTPS oder MQTT/MQTTS an einen Server senden. In jedem Fall sind die Daten im JSON-Format zu übermitteln

Allgemeine Parameter



- ID: fakultativ. Es handelt sich um einen Textparameter, der die Eingabe einer Identifizierungszeichenfolge ermöglicht, die in das JSON aufgenommen wird.
- Send mode: FIFO oder LIFO. Im FIFO-Modus werden die Daten in der Reihenfolge ihres Eintreffens an den Server übertragen, d. h. die ersten Daten, die im Datenlogger eingehen, werden auch als erste gesendet. Im LIFO-Modus ist es umgekehrt: Die zuletzt empfangenen Daten werden zuerst gesendet. Der LIFO-Modus kann in Anwendungen nützlich sein, bei denen Sie die Daten immer in Echtzeit auf dem Bildschirm anzeigen möchten. So kann ein Gerät beispielsweise mehrere Tage lang keinen Empfang haben und große Datenmengen speichern, ohne diese übertragen zu können. Sobald die Abdeckung wiederhergestellt ist, kann es einige Zeit dauern, bis alle gesammelten Daten an den Server gesendet werden. Im LIFO-Modus können die zuletzt erfassten Daten zuerst gesendet werden, so dass die Echtzeitdaten schnell auf dem Bildschirm angezeigt werden können, während die restlichen, zuvor erfassten Daten später eintreffen.
- Time format: Das JSON-Datenobjekt enthält immer einen Zeitstempel (Datum und Uhrzeit)

mit der Uhrzeit, zu der die gespeicherten Daten aufgezeichnet wurden. Mit diesem Parameter können Sie das Format des Zeitstempels festlegen.

- Use script: Wenn dieses Kästchen aktiviert ist, können die Daten in einem anderen Format gespeichert werden, bevor das TITAN-basierte Gerät die erfassten Daten (z. B. eine Modbus-Messung) in seinem internen Speicher (Datenlogger) im Standard-JSON-Format des TITAN-basierten Geräts speichert. Dies kann sehr nützlich sein, um Daten an Plattformen zu senden, die eine bestimmte Struktur erfordern. Weitere Informationen finden Sie im Anwendungshinweis zum „JSON Transformer Script“.

Zum Beispiel würden Modbus-Register, die von TITAN-basierten Geräten gelesen werden, standardmäßig im folgenden Format gespeichert:

```
{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:38:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”}
```

Es kann jedoch von Interesse sein, diese Struktur zu ändern, neue benutzerdefinierte Felder hinzuzufügen usw.

```
{“data”:{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:38:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”,“myField1”:123,“MyField2”:456}}
```

Diese Formatänderung kann mit Hilfe der „JSON Transformer Scripts“ vorgenommen werden

Use array: Standardmäßig senden TITAN-basierte Geräte Daten an einen Server (MQTT, HTTP) auf Datensatzbasis, d. h. eine Übertragung pro gesendeten Datensatz. Wenn Sie die Option „Array verwenden“ wählen, werden die Daten als Array gesendet, so dass bis zu 100 Messwerte gleichzeitig gesendet werden können und die Datenübertragung erheblich beschleunigt wird.

Ist dieses Kästchen beispielsweise nicht markiert, werden die Daten im Standard-JSON-Format von TITAN-basierten Geräten übertragen

```
{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:38:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”}
```

Wenn das Kontrollkästchen aktiviert ist, werden die Daten als Array mit einem Inhalt zwischen 1 und 100 Elementen übertragen, je nachdem, welche Daten im Datenlogger gespeichert sind.

```
[{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:38:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”},{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:39:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”},{“IMEI”:“869101054287806”,“TYPE”:“MODB”,“TS”:“2022-06-03T11:40:01Z”,“ID”:“TRES”,“A”:“192.168.1.28:502”,“ST”:“1”,“N”:“6”,“V”:[1,2,3,4,5,6],“P”:“ID0001”}, ... ]
```

Modo HTTP

Communication mode: WEB PLATFORM (HTTP REST)

Enabled: ☐ Communication mode HTTP enabled

Mode: **HTTP GET (JSON)** Method of sending data

Custom parameters: Optional. Ex: &a=1&b=2 only for "HTTP GET/PUT (PARAMETERS)" modes

Custom header1: Optional. Custom header1. For example: Content-type:application/json

Custom header2: Optional. Custom header2. For example: IDENTITY_KEY;YOUR_KEY

Custom header3: Optional. Custom header3.

Server: Destination URL. Example: www.mydomain.com/set.asp?data=

Server Username: Optional. Blank if no server authentication required

Server Password: Optional. Blank if no server authentication required

- Enabled: Klicken Sie hier, um den Modus für das Senden von Daten an eine Webplattform über HTTP/HTTPS zu aktivieren
- Mode: Datenübertragungsmodus. Sie können zwischen HTTP GET (JSON), HTTPS GET (JSON), HTTP POST (JSON), HTTPS POST (JSON) wählen
- Custom parameters: ermöglicht das Hinzufügen optionaler Parameter für HTTP-GET-Methoden
- Custom header1, Custom header2 y Custom header3: ermöglicht das Hinzufügen von Kopfzeilen zu HTTP/HTTPS-Anfragen. Viele WEB-Plattformen verlangen einen Header mit einem identifizierenden Token. In diesem Abschnitt können Sie ihn konfigurieren.
- Server: Vollständige URL zum Senden der im Datenlogger erfassten Daten. Zum Beispiel www.metering.es/json/set.asp?data=
- Server-Login: Wenn Ihre Plattform einen eingeschränkten Zugang hat, geben Sie hier den Benutzernamen ein.
- Server Password: Wenn Ihre Plattform einen eingeschränkten Zugang hat, geben Sie bitte hier Ihr Benutzerpasswort ein.

Modo FTP

- Snmp - Tacacs+ - Mqtt - Http / Https - User Permissions - Passwords Web UI - CA Certificates - Email Config - ModBus Slave - Titan Scripts - Connectivity tools - Digital I/O - Custom Skin - Led Config	Enabled:	☒	Communication mode FTP enabled
	FTP prot.:	FTPS	FTP / FTPS protocol
	FTP Server:		Destination FTP Server. Example: ftp.mydomain.com
	FTP port:		FTP server port. Default 21
	FTP Path:		FTP path. Example: /dev/plcs/
	FTP Username:		FTP Username
	FTP Password:		FTP Password
FTP File Period:	day	FTP File Period (one file every minute, hour, day)	

- Enabled: Klicken Sie auf diese Schaltfläche, um den Modus zum Senden von Daten an einen FTP-Server zu aktivieren, (das Format der Datendatei ist JSON)
- FTP prot.: Hier können Sie das Sendeprotokoll auswählen, entweder FTP oder das sichere FTPS-Protokoll
- FTP-Server: FTP-Server zum Senden von Daten (IP oder DNS)
- FTP port: Port des FTP-Servers, normalerweise 21
- FTP Path: Pfad innerhalb des Servers, auf dem der Datenabzug stattfindet
- FTP Username: der Benutzername eines Kontos auf Ihrem FTP-Server, das beschreibbar ist
- FTP Password: das Passwort eines Kontos auf Ihrem FTP-Server, das beschreibbar ist
- FTP File Period: Wie oft soll der TITAN die gesammelten Daten an Ihren Server senden (jeden Tag, jede Stunde oder jede Minute)

Modo MQTT

- Sms control - Periodic Autoreset - Time Servers - Remote Console - Snmp - Tacacs+ - Mqtt	Communication mode: MQTT		
	Enabled:	☐	Communication mode MQTT enabled
	MQTT Topic		MQTT Topic. Example: [IMEI]/logger
Note: Other>MQTT menu must be configured			

- Enabled: Klicken Sie darauf, um den Modus für das Senden von Daten an einen MQTT-Broker zu aktivieren, (alle Daten werden im JSON-Format gesendet).
- MQTT Topic: MQTT-Topic, an das die im Logger gespeicherten Daten gesendet werden sollen

Real Time Status

Ermöglicht es Ihnen, den Status des internen Datenloggers des TITAN-basierten Geräts und die zur Übertragung anstehenden Daten einzusehen. Es kann auch für einige Anwendungen nützlich sein, bei denen es nicht erwünscht ist, Daten an einen entfernten Server zu übertragen.

Z-Other > Logger Registers (pending of transmission)

```
[{"IMEI": "869101054287806", "TYPE": "MOOB", "TS": "2022-06-03T11:54:01Z", "ID": "UNO", "A": "192.168.1.28:502", "ST": "1", "N": "1"}, {"IMEI": "869101054287806", "TYPE": "MOOB", "TS": "2022-06-03T11:54:01Z", "ID": "DOS", "A": "192.168.1.28:502", "ST": "1", "N": "5"}, {"IMEI": "869101054287806", "TYPE": "MOOB", "TS": "2022-06-03T11:54:01Z", "ID": "TRES", "A": "192.168.1.28:502", "ST": "1", "N": "1"}]
```

Number of listed registers: 3
Size of listed registers: 669 bytes of data
Total registers in Logger: 3

Show: Text filter:

In diesem Bereich können Sie auch alle Daten löschen, die das TITAN-basierte Gerät noch nicht gesendet hat, indem Sie auf die Schaltfläche „DELETE ALL PENDING REGISTERS FROM LOGGER“ klicken. Sie können auch nach Text filtern.

Zusätzliche Hinweise

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden
- Wenn Sie den HTTP- oder MQTT-Sendemodus verwenden, werden die Daten an Ihren Server gesendet, sobald sie erfasst werden. Bei mangelnder 4G/3G/2G-Abdeckung oder bei Problemen mit der Datenübertragung (z. B. bei einem Remote-Server-Absturz) speichert das TITAN-basierte Gerät die Daten und sendet sie später, wenn die Kommunikation wieder normal funktioniert
- Bei Verwendung des FTP-Sendemodus werden die Daten in einer JSON-Datensatzstrukturdatei gespeichert und entsprechend dem gewählten Zeitintervall (Minute, Stunde, Tag) für den Versand gesendet. Bei mangelnder GSM-Abdeckung oder bei Problemen mit der Datenübertragung (z. B. bei einem Remote-Server-Absturz) speichert das TITAN-basierte Gerät die Daten und sendet sie später, wenn die Kommunikation wieder normal funktioniert

- Der Name der FTP-Datei, die auf Ihrem Server erstellt wird, hat das folgende Format:
 IMEI-Jahr-Monat-Tag.txt > Wenn der ausgewählte Zeitraum für das Senden von Daten „jeden Tag“ ist
 IMEI-Jahr-Monat-Tag-Stunde.txt > Wenn der ausgewählte Zeitraum für das Senden von Daten „stündlich“ ist
 IMEI-Jahr-Monat-Tag-Stunde-Minute.txt > Wenn der ausgewählte Zeitraum für das Senden von Daten „jede Minute“ ist
- Wenn Sie den MQTT-Modus verwenden, denken Sie daran, den Abschnitt „OTHER > Mqtt“ richtig zu konfigurieren. In diesem Abschnitt müssen Sie alle Konfigurationsparameter eingeben, die erforderlich sind, um das TITAN-basierte Gerät mit Ihrem MQTT-Broker zu verbinden

4.6.2 External Devices > Temperature Sensor

Wenn Ihr TITAN-basiertes Gerätemodell einen MTX-Temp-RS232-Temperaturfühler unterstützt, können Sie die Temperatur regelmäßig an eine Web-Plattform senden, eine SMS-Warnmeldung senden, wenn die Temperatur über oder unter einem bestimmten Schwellenwert liegt, usw.

- **Enabled:** Markieren Sie dieses Kästchen, wenn Sie einen MTX-Temp-RS232-Temperaturfühler an einen seriellen Anschluss angeschlossen haben.
- **Serial Port:** Wählen Sie den seriellen Anschluss des Geräts aus, an dem der Temperaturfühler MTX-Temp-RS232 angeschlossen ist.
- **Interval:** Wenn Sie beabsichtigen, regelmäßige Temperaturmesswerte an Ihren Webserver zu senden, geben Sie hier den Zeitraum in Minuten an.
- **Logger:** Wenn Sie den internen Logger zum Speichern von Temperaturdaten verwenden möchten (um sie später an eine Webplattform zu senden), müssen Sie diese Option auswählen. Wann sollte diese Option nicht aktiviert werden? Zum Beispiel, wenn Sie nur eine SMS-Warnung senden möchten, wenn die Temperatur außerhalb des Bereichs liegt.
- **Alarms enabled:** Wählen Sie diese Option, wenn Sie die Alarme für Temperaturen außerhalb des Bereichs aktivieren möchten.
- **Max Temperature:** Höchsttemperatur, bei deren Überschreitung ein Hochtemperaturalarm ausgelöst wird.
- **Text alarm on (max):** Alarmtext, der gesendet wird, wenn ein Hochtemperaturalarm auftritt.
- **Text alarm off (max):** Alarmtext, der gesendet wird, wenn ein Hochtemperaturalarm deaktiviert wird.
- **Min Temperature:** Temperatura mínima a partir de la cual se considera alarma por temperatura baja.
- **Text alarm on (min):** Alarmtext, der gesendet wird, wenn ein Niedrigtemperaturalarm auftritt.
- **Text alarm off (min):** Alarmtext, der gesendet wird, wenn ein Niedrigtemperaturalarm deaktiviert wird.
- **Phone numbers:** Telefonnummern (getrennt durch Semikolon „;“), an die SMS-Alarmmeldungen gesendet werden sollen

- Current temperature: zeigt, wenn ein MTX-Temp-RS232 Temperatursensor angeschlossen ist, die aktuelle Temperatur in Echtzeit

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Die vom Gerät verwendete Hysterese beträgt 1 Grad. Wenn Sie z. B. die Höchsttemperatur auf 50 °C einstellen, wird der Alarm ausgelöst, wenn die Temperatur 50 °C erreicht, aber der Alarm gilt erst dann als beendet, wenn die Temperatur auf mindestens 49 °C gesunken ist. Dadurch wird vermieden, dass ständig SMS-Nachrichten gesendet werden, wenn die Temperatur gerade den ausgewählten Schwellenwert erreicht hat.
- Beispiel für das Format des gesendeten JSON-Frames:

```
{„IMEI“:„358884050088207“,„TS“:„25/12/2014 17:40:09“,„TYPE“:„TEMP“, „P“:„1234“,„TEM“:25.5,„TEMH“:0,„TEML“:0}
```

Wo:

IMEI: Identifikationsnummer des Teams. Einzigartig für jedes Team

TS: Zeitstempel TT:MM:JJJJ HH:MM:SS

TYPE: Framenart. Hier, die Temperatur

P: Logger-ID Feld (External Devices > Logger configuration)

TEM: Temperatur

TEMH: Alarm bei hoher Temperatur (0=nein, 1=ja)

TEML: Alarm bei niedriger Temperatur (0=nein, 1=ja)

4.6.3 External Devices > Modbus RTU / TCP

TITAN-basierte Geräte sind darauf vorbereitet, Register von externen Modbus RTU- und Modbus TCP-Geräten zu lesen, zu speichern und an einen externen Server zu senden (über HTTP/HTTPS, FTP oder MQTT/MQTTS). Das heißt, es kann eine regelmäßige Ablesung von bis zu 40 Modbus RTU- und/oder TCP-Geräten planen, die Ableseregister auswählen und dann die Ablesungen über ein JSON-Objekt an einen Server senden.

- **Enabled:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie ein oder mehrere Modbus-RTU-Geräte an einen seriellen Anschluss angeschlossen haben und die Modbus-Register selbständig lesen wollen.
- **Serial Port:** Ermöglicht die Auswahl der seriellen RS232- oder RS485-Schnittstelle des TITAN-basierten Geräts, an das das Modbus RTU-Gerät angeschlossen ist.
- **Logger:** Wenn Sie den internen Logger verwenden möchten, um die gelesenen Modbus-Register zu speichern (um sie später an eine Webplattform zu senden), müssen Sie diese Option auswählen.
- **Device name:** Name, der ein Modbus RTU- oder Modbus TCP-Gerät identifiziert.
- **Address:** Modbus-RTU-Adresse des zu lesenden Geräts. Im Falle eines Modbus-TCP-Geräts müssen IP und Port angegeben werden (Format IP:Port)
- **Command:** Modbus-Befehl Lesen.
- **Start:** Erstleseregister
- **Num Words:** Anzahl der zu lesenden Datensätze
- **Reg type:** Art des zu lesenden Datensatzes
- **Period:** Lesezeitraum, d. h. wie oft, in Minuten, der Satz von Datensätzen gelesen werden soll.

Wichtig: Ausführliche Informationen und Beispiele für die Nutzung dieser Funktionalität von TITAN-basierten Geräten finden Sie in der Application Note AN27 (ANV6_27-Router-TITAN-Modbus-RTU-RTU-TCP-Concentrator-multimap_HTTP.pdf und ANV6_32-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_MQTT.pdf

External Devices > Modbus RTU / TCP

Settings successfully updated. Changes take effect after reboot

Enabled: ☒ Enable Modbus Devices
 Serial Port: Select the connected serial port if needed
 Logger: ☒ Check if logger must be used
 Please, configure logger before using this option

Dev. name / ID	Addr.	Command	Start @	Num word/bit	Reg Type	Period		
UNO	1	0x03	1	10	WORD	1	Del	Test
DOS	192.168.1.28:502	0x03	10	5	WORD	1	Del	Test

Device name / ID: Insert the device name or ID
 Address: Modbus RTU address or IP:port address
 Command: Modbus read command
 Start: Address of the first register
 Number Words / Bits: Words for command 0x03/0x04. Bits for 0x01/0x02
 Reg Type: Type of registers for command 0x03/0x04
 Period: Read period (minutes)

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Wenn Sie ein neues Modbus-RTU-Gerät anlegen möchten, müssen Sie das Formular ausfüllen und auf die Schaltfläche „SAVE DEVICE“ klicken.
- Ein Beispiel für das Format des JSON-Frames, der mit den Messwerten gespeichert wird und an einen Server gesendet werden soll, lautet wie folgt:

```
{„IMEI“:„354740050367237“,„TS“:„17/02/2014 19:02:46“,„TYPE“:„MODB“, „P“:„1234“,„ST“:1,„A“:1,„V“:[1,2,3,4,5,6,7,8,9,10]}
```

Wo:

- IMEI: Identifikationsnummer des Teams. Einzigartig für jedes Team
- TS: timestamp DD:MM:YYYY HH:MM:SS
- TYPE: Datenart. Hier Modbus
- P: Logger-ID Feld (External Devices > Logger configuration)
- ST: erste Datensatz
- A: Modbus-Adresse des gelesenen Geräts
- V: Array mit den gelesenen Datensätzen

- Es wird empfohlen, das Kapitel über die verfügbaren AT-Befehle zu lesen, da die Werte der Modbus-Register über AT-Befehle, von der Web-Konfigurationsumgebung, von der Remote-Konsole (Telnet), SSH oder von SMS usw. gelesen und geändert werden können.

- In den Feldern „Start“ und „Num Words“ können ab Firmware-Version 3.26 auch nicht-fortlaufende Einträge vorgenommen werden. Weitere Informationen und Beispiele finden Sie in den Application Note AN27 (ANV6_27-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_HTTP.pdf) und AN32 ANV6_32-Router-TITAN-Modbus-RTU-TCP-Concentrator-multimap_MQTT.pdf).

4.6.4 - External Devices > GPS Receiver

Dieses Menü ermöglicht die Konfiguration der GPS-Positionsdaten von TITAN-basierten Geräten, die ein internes GPS-Modul verwenden oder, falls kein internes GPS-Modul vorhanden ist, einen NMEA-GPS-Empfänger, der an einen der RS232- oder RS485-Anschlüsse angeschlossen ist

- **Enabled:** Markieren Sie dieses Kästchen, wenn Sie ein internes (oder externes) GPS-Modul an das TITAN-basierte Gerät angeschlossen haben, das Sie verwenden möchten.
- **Serial Port:** Wählen Sie den seriellen Anschluss des TITAN-basierten Geräts, an dem das GPS angeschlossen ist.
- **Interval:** Wählen Sie den Zeitraum der GPS-Messung in Sekunden (Sie erhalten alle Sekunden eine GPS-Position). Geben Sie einen Mindestwert von 30 Sekunden an.
- **Logger:** aktivieren Sie dieses Kontrollkästchen, wenn Sie die gelesenen GPS-Positionen im internen Logger aufzeichnen möchten, um sie z. B. über HTTP/HTTPS, MQTT/MQTTS oder FTP an Ihre Webplattform zu senden. Sehr nützlich, wenn Sie TITAN-basierte Geräte zur Implementierung eines GPS-Flottenmanagementsystems verwenden möchten.
- **Systemzeit:** aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass die Systemzeit mit der vom GPS gelesenen Zeit synchronisiert wird.
- **TCP port listener:** ermöglicht es, NMEA-Frames über eine IP-Verbindung über die TITAN-basierte Ausrüstung zu erhalten. Wenn Sie z. B. einen Socket gegen die IP des TITAN-basierten Geräts zu dem in diesem Punkt angegebenen Port öffnen, können Sie NMEA-Positionierungsrahmen in Echtzeit abrufen.
- **TCP Client IP:** Ermöglicht die Angabe einer IP-Adresse zum Senden von NMEA-Frames an einen externen Server.
- **TCP Client Port:** Ermöglicht die Angabe des TCP-Ports zum Senden von NMEA-Frames von dem im Parameter „TCP Client IP“ angegebenen externen Server.
- **TCP Client Timeout:** gibt die Sekunden an, die das TITAN-basierte Gerät zwischen dem Erkennen einer geschlossenen Steckdose und dem erneuten Öffnen verstreichen lassen soll.

webdyn powered by **TITAN**
flexitron group

External Devices > GPS Receiver

Enabled: ☐ Enable GPS Receiver

Serial Port: Select the connected serial port

Interval: Reading period for logger (seconds, minimum 30)

Logger: ☐ Check if logger must be used. Please, configure logger before using this option

System time: ☐ Check for System time synchronization

TCP port listener: Redirect NMEA data to TCP server socket port if greater than 0 (1 frame / second)

TCP Client IP: If filled with IP or DNS, Titan will send NMEA raw data to this server

TCP Client Port:

TCP Client timeout: If socket closes, will wait this seconds in order to re-open the socket.

SAVE CONFIG

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.6.5 - External Devices > Generic Serial Device

In diesem Abschnitt können Sie einen seriellen RS232- oder RS485-Gerätedatenlogger konfigurieren.

Grundsätzlich liest und speichert das TITAN-basierte Gerät die seriellen Daten, die von einer der oben genannten Schnittstellen erfasst werden, und sendet sie über HTTP/S, MQTT/S oder FTP an eine Web-Plattform.

Besonders geeignet für die Datenerfassung von seriellen Geräten, die in regelmäßigen Abständen einen Datenrahmen senden (Temperatursensoren, Feuchtigkeitssensoren, serielle Alarmer, ...)

- **Enabled:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie ein seriellles Gerät anschließen und das TITAN-basierte Gerät die Datenloggerfunktion übernehmen soll.
- **Serial Port:** Wählen Sie den seriellen Anschluss des TITAN-basierten Geräts, an dem das zu protokollierende serielle Gerät angeschlossen ist.
- **Interval:** Bei der Angabe einer „0“ werden alle empfangenen seriellen Frames gesammelt. Bei der Angabe „1“ wird jedes zweite empfangene Frame erfasst. Bei der Angabe „2“ wird jedes dritte empfangene Frame erfasst.
- **Only changes:** Aktivieren Sie das Kontrollkästchen, wenn Sie nur die Bilder protokollieren möchten, die sich vom vorherigen Frame unterscheiden. Wenn Sie z. B. einen Temperatursensor anschließen, kann es sein, dass dieser Sensor eine ganze Weile lang dieselben seriellen Daten ausgibt, bis sich die Temperatur ändert. Wenn Sie dieses Kästchen ankreuzen, werden nur die seriellen Daten erfasst, wenn sich die Daten ändern.
- **Logger:** aktivieren Sie dieses Kontrollkästchen, wenn Sie die seriellen Daten im internen Logger speichern möchten, um sie später über HTTP/HTTPS, FTP oder MQTT/MQTTS an Ihre Webplattform zu

senden

- TX period: eine Zahl größer als 0 gibt den Zeitraum (in Sekunden) an, in dem die Datenrahmen „TX Frame1“, „TX Frame2“, „TX Frame3“, „TX Frame4“, „TX Frame5“ über die serielle Schnittstelle gesendet werden sollen. Mit dieser Option können Sie serielle Geräte mit proprietären Protokollen „abfragen“.
- TX FrameX: gibt an, dass alle X Sekunden, die im Parameter „TX period“ angegeben sind, ein Datenrahmen über die serielle Schnittstelle weitergeleitet werden soll. Diese Frames müssen im hexadezimalen Format angegeben werden. Beispiel: 0102030A0D...

The screenshot shows the webdyn configuration interface. At the top, the webdyn logo is displayed with the text 'powered by TITAN' and 'flexitron group'. On the left, a sidebar menu lists various configuration categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, W-MBus). The 'Generic Serial Device' option is selected. The main configuration area includes fields for 'Enabled' (checkbox), 'Serial Port' (dropdown menu showing 'Serial Port 1'), 'Interval' (input field with '0'), 'Only changes' (checkbox), 'Mode' (dropdown menu showing 'Raw (Default)'), and 'Logger' (checkbox). Below these are five 'TX Frame' input fields (TX Frame1 to TX Frame5), each with a description of its maximum length (256). At the bottom, there are 'SAVE CONFIG' and 'VIEW LOG' buttons.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.6.6 - External Devices > IEC102 Meter

In diesem Abschnitt können Sie das TITAN-basierte Gerät so konfigurieren, dass es einen Stromzähler mit IEC 60870-5-102-Protokoll ausliest.

- Enabled: Aktivieren Sie dieses Kästchen, wenn Sie einen Stromzähler mit IEC-60870-5-102-Protokoll anschließen wollen, den das TITAN-basierte Gerät selbstständig abfragen soll.
- Serial Port: Wählen Sie den seriellen Anschluss des TITAN-basierten Geräts, an dem der IEC-60870-5-102-Stromzähler angeschlossen ist.
- Period: zeitraum (in Minuten), in dem der IEC-60870-5-102-Stromzähler von dem TITAN-basierten Gerät abgefragt wird, um die Momentanwerte abzulesen.

- **Integrated values:** Aktivieren Sie das Kontrollkästchen, wenn das TITAN-basierte Gerät zusätzlich zum Lesen der Momentanwerte auch die Schließungen lesen muss. Ist das Kästchen angekreuzt, liest und speichert das TITAN-basierte Gerät jede Mitternacht die Zählerabschlüsse.
- **Logger:** aktivieren Sie dieses Kontrollkästchen, wenn Sie die seriellen Daten im internen Logger speichern möchten, um sie später über HTTP/HTTPS, FTP oder MQTT/MQTTS an Ihre Webplattform zu senden
- **ID Meter:** Geben Sie einen identifizierenden Text für den Stromzähler ein.
- **Link Address:** link-Adresse des Stromzählers.
- **Meas. Address:** Adresse des Stromzählers und des Zählpunkts.
- **Password:** Passwort für den Stromzähler.

The screenshot shows the webdyn IEC102 Meter configuration page. The sidebar on the left lists various settings categories: Mobile, Ethernet, Wifi, Firewall, Serial Settings, and External Devices. The main content area is titled 'External Devices > IEC102 Meter'. It contains the following configuration options:

- Enabled:** A checkbox that is checked. Description: Enable Temperature sensor.
- Communication Port:** A dropdown menu showing 'Serial Port 1'. Description: Select the serial port for reading.
- Period:** A dropdown menu showing '1 minute'. Description: Reading period for instant values.
- ID Meter:** A text input field containing 'ID00000'. Description: Customizable label for identification.
- Link address:** A text input field containing '1'. Description: Link address of meter (1...65535).
- Meas. address:** A text input field containing '1'. Description: Measurement address (1...65535).
- Password:** A text input field containing '1'. Description: Password of meter (1...65535).
- Fiscal close:** A checkbox that is checked. Description: Read and send Fiscal close data once per day (Contract 1).
- Fiscal close days:** A text input field containing '31'. Description: Number of days (1 ... 31) Default 31.
- Logger:** A checkbox that is checked. Description: Logger must be used. Please, configure logger before using this option. Recommended 'Register Size': 7000, 'Number of registers': 100.

At the bottom of the configuration area, there are two buttons: 'SAVE CONFIG' and 'VIEW LOG'.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Die von TITAN-basierten Geräten gesendeten Frames haben das folgende Format:

Frames mit Momentanwerten:

```
{ "IMEI": "867962046823806", "TYPE": "IEC102", "TS": "2021-11-02T15:14:04Z", "P": "1234", "ID": "ID00000", "VABA": "0", "VABRI": "0", "VABRC": "0", "PAT": "0", "PRT": "0", "FPT": "100" }
```

Wo:

IMEI:	TITAN-basierte Geräte-Identifikationsnummer
TYPE:	JSON-Typ. Hier Typ IEC102
TS:	Zeitstempel, wann die Daten erfasst wurden
P:	Optionales Identifikationsfeld (vom Logger)
VABA:	Absolute Wirkenergie
VABRI:	Absolute induktive Blindleistung
VABRC:	Absolute induktive Blindleistung
PAT:	Gesamt-Wirkleistung
PRT:	Gesamtblindleistung
FPT:	Gesamtleistungsfaktor
PAF1:	Wirkleistung Phase I
PRF1:	Phase I Blindleistung
FPF1:	Leistungsfaktor Phase I
PAF2:	Wirkleistung Phase II
PRF2:	Phase II Blindleistung
FPF2:	Leistungsfaktor Phase II
PAF3:	Wirkleistung Phase III
PRF3:	Phase III Blindleistung
FPF3:	Leistungsfaktor Phase III
IF1:	Intensität der Phase I
TF1:	Phase I Spannung
IF2:	Intensität der Phase II
TF2:	Phase II Spannung
IF3:	Intensität der Phase III
TF3:	Phase III Spannung



Siehe Anwendungshinweis ANV6_51-Router-TITAN-Metering-IEC-60870-5-102.pdf

4.7 Other

4.7.1 Other > AT Command

Von diesem Bereich aus ist es möglich, einen AT-Befehl direkt an das interne Modem des TITAN-basierten Geräts zu senden. So kann es beispielsweise interessant sein, die Netzabdeckung zu überprüfen, umliegende Telefoniezellen zu identifizieren usw.

Andererseits ist es auch möglich, bis zu 5 spezielle AT-Befehle zu konfigurieren, mit denen das Gerät beim Booten konfiguriert werden kann.

- AT Command: AT-Befehl zur Echtzeitausführung (z. B. AT+CSQ). Sobald die Taste „SEND AT COMMAND“ gedrückt wird, soll der AT-Befehl ausgeführt werden.

- AT1, ... AT5: initialisierungs-AT-Befehle.



Zusätzliche Hinweise.

- Wenn Sie AT-Befehle zur Initialisierung eingestellt haben, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.2 Other > DynDns

TITAN-basierte Geräte sind mit DynDNS und No-IP-Service kompatibel. Wenn Sie nicht über eine SIM-Karte mit fester IP verfügen und die externen Dienste DynDNS oder NO-IP nutzen möchten, können Sie sie in diesem Abschnitt konfigurieren.

- Enabled: Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Verwendung von DynDNS oder NO-IP aktivieren möchten.
- Server: Geben Sie den Dienstserver an (members.dyndns.org oder dynupdate.no-ip.com).
- Domain: geben Sie die von Ihnen erstellte DNS ein (z. B. mydomain.dyndns.org)

- **Login:** Anmeldung bei Ihrem DynDNS- oder NO-IP-Konto
- **Password:** Kennwort für Ihr DynDNS- oder NO-IP-Konto
- **Period:** Zeitraum in Minuten, in dem die aktuelle IP auf den DynDNS- oder NO-IP-Servern aufgefrischt wird
- **Hide WAN IP:** wenn das Kontrollkästchen aktiviert ist, wird die IP vom DynDNS-Server erkannt. Muss aktiviert werden, wenn Sie DynDNS über den Ethernet- oder Wifi-Port des TITAN-basierten Geräts als Internet-Port verwenden möchten.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Die IP wird auf den DynDNS- oder NO-IP-Servern jedes Mal aktualisiert, wenn sie sich ändert. Es wird jedoch empfohlen, den Konfigurationsparameter „Periode“ zu verwenden, z. B. mit einem Wert von 60, so dass alles, was passiert, jede Stunde gesendet wird.

4.7.3 Other > Private DynDns

Der Private DynDNS-Dienst ermöglicht das Senden der aktuellen IP-Adresse des TITAN-basierten Geräts und bestimmter Statuswerte an einen eigenen Server. Die Daten können entweder über HTTP (HTTP/S GET, HTTP/S POST) oder durch Senden eines bestimmten Frames über einen Socket an einen konfigurierbaren TCP-Port und auch über MQTT gesendet werden.

HTTP- oder TCP-Socket-Methode

- **Enabled:** Markieren Sie dieses Feld, wenn Sie die Verwendung von Private DNS aktivieren möchten.
- **Mode:** Sie können zwischen TCP-Socket und HTTP/S GET, HTTP/S POST und HTTP/S PUT wählen
- **Server:** Die IP oder DNS des entfernten Servers
- **Server Login:** Anmeldung über Ihren Webserver (wenn Sie einen „HTTP“-Modus verwenden)
- **Password:** Passwort Ihres Webservers (wenn Sie einen „HTTP“-Modus verwenden)
- **TCP Port:** TCP-Anschluss bei Verwendung des „Socket“-Modus
- **ID:** Identifizierungszeichenfolge (entweder für den Modus „http get“ oder „socket“)
- **Period:** Der Zeitraum in Minuten, in dem die aktuelle IP auf Ihrem Server aktualisiert wird. Beachten Sie, dass unabhängig von diesem Zeitraum die öffentliche IP-Adresse gesendet wird, sobald sie sich ändert.
- **Custom header1:** Benutzerdefinierte HTTP-Kopfzeile 1
- **Custom header2:** Benutzerdefinierte HTTP-Kopfzeile 2
- **Custom header3:** Benutzerdefinierte HTTP-Kopfzeile 3
- **IO-Status:** Aktivieren Sie diese Option, wenn Sie auch den Status von digitalen Ein- und Ausgängen und Zählern senden möchten.

MQTT-Verfahren

- **Enabled:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Verwendung von MQTT aktivieren möchten
- **Period:** Zeitraum in Minuten, in dem die aktuelle IP über MQTT an Ihren Server gesendet wird. Beachten Sie, dass unabhängig von diesem Zeitraum die öffentliche IP-Adresse auch gesendet wird, sobald sie sich ändert.
- **MQTT Topic:** Thema MQTT für die Berichterstattung mit IP zu verwenden
- **MQTT QoS:** Dienstqualität, die von MQTT für das Senden der IP verwendet wird
- **IO-Status:** Aktivieren Sie diese Option, wenn Sie auch den Status von digitalen Ein- und Ausgängen und Zählern senden möchten.

webdyn powered by **TITAN**
flexitron group

★ **Mobile**

- Status
- Basic Settings
- Keep Online

★ **Ethernet**

- Basic Settings

★ **Wifi**

- Basic Settings
- DHCP Server

★ **Firewall**

- NAT
- Authorized IPs

★ **Serial Settings**

- Serial Port1-RS232
- Serial Port2-RS485
- SSL Certificates

★ **External Devices**

- Logger configuration
- ModBus Devices
- Generic Serial Device
- Temperature Sensor
- IEC102 Meter
- W-MBus
- GPS Receiver

★ **Other**

- AT Command
- DynDns
- Private DynDns
- Sms control
- Periodic Autoreset
- Time Servers
- Remote Console
- Snmp
- Tacacs+
- Mqtt

► **Other ► Private DynDns**

Use script: ☐ Check for customized json using Json Transformed Script in [Script section](#).

Communication mode: WEB PLATFORM (HTTP REST)

Enabled: ☐ Enable Private DynDNS

Mode: Communication mode

Server: IP or DNS of remote server. Example: www.myweb.com/set.asp?data=

Server Login: User (only for "http get" mode)

Server Password: Password (only for "http get" mode)

TCP Port: TCP port of remote server (only "socket" mode)

ID: String for device identification

Period: Minutes. Public IP in sent every time it changes. But it is recommended force an update every 60 minutes

Custom header1: Optional. Custom header1. For example: Content-type:application/json

Custom header2: Optional. Custom header2. For example: IDENTITY_KEY:YOUR_KEY

Custom header3: Optional. Custom header3.

I/O status: ☐ Send I/O status and counters

Communication mode: MQTT

Enabled: ☐ Communication mode MQTT enabled

Period: Minutes. Public IP in sent every time it changes. But it is recommended force an update every 60 minutes

MQTT Topic: MQTT Topic. Example: [IMEI]/dns

MQTT QoS: MQTT QoS for DNS. Normally 0

I/O status: ☐ Send I/O status and counters

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Beispiel für das Format des gesendeten JSON-Frames

Wo:

TYPE: Framenart. Hier DNS.

IMEI: Identifikationsnummer des Teams. Einzigartig für jedes Team

P: Logger-ID Feld (External Devices > Logger configuration)

IP: IP of WAN interface (2g / 3g)

CSQ: 0...31 (signal strength)

MOD: TITAN-basiertes Ausstattungsmodell

Siehe: FW-Version

IMSI: SIM-Karte IMSI

TECH: verwendete Technologie (2G, 3G, 4G)

TS: Zeitstempel

CID: Kennung der verwendeten Telefoniezelle

RSSI: Signalstärkepegel.

RSRP: 3G rsrp

RSRQ: 3G rsrq

IOx: aktueller Wert des digitalen Eingangs/Ausgangs „x“

COx: aktueller Wert des Impulszählers, der dem Digitaleingang „x“ zugeordnet ist

4.7.4 Other > SMS Control

In diesem Abschnitt können Sie die SMS-Steuerung des Geräts konfigurieren. Sie können diesen Bereich z. B. so konfigurieren, dass das Gerät einen digitalen Ausgang neu startet oder ändert, wenn eine SMS empfangen wird, oder Sie können die für diesen Zweck autorisierten Telefonnummern angeben.

- AT enabled: aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass das TITAN-basierte Gerät AT-Befehle per SMS akzeptiert, z. B. um die Reichweite aus der Ferne zu erfahren, einen Reset durchzuführen, eine Konfiguration zu ändern, ..
- AT header: geben Sie hier den Kopfzeilentext des Befehls SMS-Nachrichten ein. Wenn Sie beispielsweise in dieses Feld den Text „mtx“ schreiben, müssen Sie, wenn Sie einen AT-Befehl per SMS senden, z. B. den Befehl „AT+CSQ“, um die Reichweite des Geräts zu erfahren, eine SMS mit dem Text „mtx AT+CSQ“ senden
- All phones: aktivieren Sie dieses Kontrollkästchen, wenn alle Telefone in der Lage sein sollen, AT-Befehle an das Gerät zu senden. Kreuzen Sie dieses Feld nicht an, wenn Sie autorisierte Telefonnummern angeben möchten.
- Authorized Number X: in diesen Feldern können Sie bis zu 10 autorisierte Telefonnummern angeben.
- Alias / ATCommand: Es können bis zu 10 Aliasnamen zur Ausführung von SMS-Befehlen eingegeben werden. Stellen Sie sich vor, Sie möchten eine SMS senden, um ein bestimmtes MODBUS-Register eines externen Geräts zu aktualisieren. Sie können zum Beispiel einen ALIAS so konfigurieren, dass das TITAN-basierte Gerät, wenn es den Text „reg on“ empfängt, intern den AT-Befehl ausführt: at^mtxtunnel=setmodbus,1;5;16;2 durch Schreiben des Wertes 2 in das Register 5 des Geräts mit der Modbus-Adresse 1.
- Alias Result OK: Text, der als Antwort auf die erfolgreiche Ausführung eines ALIAS-Befehls gesendet wird. Wenn Sie möchten, können Sie für jeden ALIAS eine angepasste Antwort zurückgeben, die die Antwort zwischen den Tags angibt: <a1>Ok</a1><a2>Perfekt</a2>..
- Alias Result ERROR: Text, der im Falle einer fehlgeschlagenen Ausführung eines ALIAS-Befehls als Antwort gesendet wird. Wenn Sie möchten, können Sie für jeden ALIAS eine persönliche Antwort verfassen und die Antwort zwischen den Tags angeben: <a1>Error</a1><a2>Upsss</a2>...



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Weitere Informationen und Beispiele finden Sie im Anwendungshinweis ANV6_3. Sie werden auch sehen, wie man dem ALIAS Parameter hinzufügt

4.7.5 Other > Periodic autoreset

In diesem Bereich können Sie einen programmierten Autoreset der TITAN-basierten Geräte konfigurieren.

- Autoreset not enabled: Aktivieren Sie die Option, wenn Sie nicht wollen, dass die TITAN-basierten Geräte automatisch zurückgesetzt werden.
- Autoreset every X hours: Aktivieren Sie die Option, wenn Sie möchten, dass sich das TITAN-basierte Gerät nach einer bestimmten Anzahl von Stunden automatisch zurücksetzt.
- Number of hours: Wenn Sie eine automatische Rückstellung alle X Stunden wählen, müssen Sie in diesem Feld X angeben, d. h. die Anzahl der Stunden, nach denen die Rückstellung erfolgt. Geben Sie 24 für eine tägliche Rückstellung an.
- Auto-reset at specific time: Wählen Sie diese Option, wenn Sie möchten, dass sich das TITAN-basierte Gerät zu einer bestimmten Tageszeit automatisch zurücksetzt
- Time for autoreset: Bestimmte Zeit für die tägliche automatische Rückstellung.
- Auto-reset if router can't obtain IP after X minutes: Eine sehr empfehlenswerte Option für Situationen, in denen der Kontext verloren geht. So können Sie beispielsweise die Minuten angeben, nach denen das TITAN-basierte Gerät automatisch starten soll, wenn es keine IP-Adresse erhalten kann.

- ★ **Mobile**
 - Status
 - Basic Settings
 - Keep Online
- ★ **Ethernet**
 - Basic Settings
- ★ **Wifi**
 - Basic Settings
 - DHCP Server
- ★ **Firewall**
 - NAT
 - Authorized IPs
- ★ **Serial Settings**
 - Serial Port1-RS232
 - Serial Port2-RS485
 - SSL Certificates
- ★ **External Devices**
 - Logger configuration
 - ModBus Devices
 - Generic Serial Device
 - Temperature Sensor
 - IEC102 Meter
 - W-MBus

► **Other** ► **Periodic Autoreset**

☒ **Autoreset not enabled**

☐ **Autoreset every X hours**
 Number of hour: Every X hours device will be rebooted

☐ **Autoreset at specific hour**
 Hour for autoreset 0 ... 23

☐ **Reset if router can't obtain IP after X minutes**
 Time for reset 5 ... 1440 min.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.6 Other > Time Servers (NTP)

Das auf dem TITAN basierende Gerät verfügt über eine Echtzeituhr, die es ermöglicht, die Zeit auch nach einem mehrstündigen Stromausfall beizubehalten. Diese interne Uhr muss in regelmäßigen Abständen über das NTP-Protokoll mit Zeitservern synchronisiert werden.

- **Enabled:** markieren Sie dieses Feld, wenn Sie NTP-Zeitserver verwenden möchten.
- **NTP Server 1:** IP-Adresse oder DNS des NTP-Zeitserver 1
- **NTP Server 1 port:** NTP-Zeitserver-Anschluss 1
- **NTP Server 2:** IP-Adresse oder DNS des NTP-Zeitserver 2
- **NTP Server 2 port:** NTP-Zeitserver-Anschluss 2
- **Time Zone:** Hier können Sie die Zeitzone angeben.

Time Servers (NTP) > Local Time Server.

- **Enabled:** Aktivieren Sie dieses Feld, wenn Sie den Titan-Router als NTP-Zeitserver verwenden möchten.
- **NTP Server port:** NTP-Serveranschluss des Titan-Routers

The screenshot shows the webdyn configuration interface. At the top, the webdyn logo is displayed with the text 'powered by TITAN' and 'flexitron group'. The sidebar on the left contains navigation links: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), and Serial Settings (Serial Port1-RS232, Serial Port2-RS485). The main content area is titled 'WAN Time Server (NTP)'. It includes a 'Enabled' checkbox which is checked. Below this are fields for 'NTP Server 1' (ntp.roa.es), 'NTP Server 1 port' (123), 'NTP Server 2' (es.pool.ntp.org), and 'NTP Server 2 port' (123). A 'Time zone' dropdown menu is set to 'Europe/Madrid'. The 'Current Time' is displayed as '02-08-2022 10:38:48'. To the right of these fields, there are labels: 'Enable NTP', 'IP or DNS address', 'UDP port. Default 123', 'Select the timezone', and 'Current date & time of the system'. A 'SAVE CONFIG' button is located at the bottom left of the main area.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.7 Other > Remote console (TCP Server)

Falls Sie einmal eine spezielle Operation auf dem TITAN-basierten Gerät über eine „Telnet“- oder „SSH“-Verbindung durchführen müssen, können Sie dies durch Konfiguration dieses Abschnitts erreichen. Das heißt, diese spezielle Verbindung ermöglicht es auch, AT-Befehle über eine TELNET- oder SSH-Verbindung an das TITAN-basierte Gerät zu senden. So können Sie die Konfiguration des Geräts ändern, einen digitalen Ausgang schalten usw. Eine Liste der verfügbaren AT-Befehle finden Sie in Abschnitt 5 dieses Handbuchs.

- Enabled: markieren Sie dieses Kästchen, wenn Sie diese spezielle Verbindung verwenden möchten.
- TCP Port: TCP Listening Port des Geräts, über den die Verbindung hergestellt werden soll.
- Login: den Benutzernamen, der nach der Anmeldung abgefragt wird.
- Password: Benutzerpasswort, das nach der Eingabe des Benutzernamens abgefragt wird
- SSH: Markieren Sie das Kästchen, wenn Sie SSH anstelle von Telnet verwenden möchten.



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden. Wenn Sie das SSH-Kontrollkästchen aktivieren/deaktivieren, müssen Sie auch das Passwort erneut eingeben.
- Der Zugriff auf die Remote-Konsole kann sowohl lokal (Ethernet oder Wifi) als auch aus der Ferne über eine 4G/3G/2G-Verbindung erfolgen.

4.7.8 Other > SNMP

TITAN-basierte Geräte verfügen über das SNMP-Protokoll. Über SNMP können Sie SET- und GET-Operationen von Standard-SNMP-Anwendungen aus durchführen

- Enabled: Wählen Sie aus, ob Sie den SNMP-Dienst des TITAN-basierten Geräts aktivieren möchten
- SNMP-Version: Es kann zwischen SNMPv2c und SNMP v3 gewählt werden
- UDP-Port: Der Standard-UDP-Port für SNMP ist 161, Sie können aber auch einen eigenen Port angeben.
- Custom OID: Ermöglicht es Ihnen, die OID des Unternehmensprodukts gegenüber dem Standardwert (.45711.1.1) zu ändern, falls Sie sie an Ihre Unternehmenswerte anpassen möchten.
- Community: Das Passwort, um SET- und GET-Befehle ausführen zu können. Nur für SNMPv2 erforderlich
- Benutzername: Benutzername bei Verwendung von SNMPv3 (nicht erforderlich bei SNMPv2)
- Auth Password: Authentifizierungskennwort für SNMPv3 (nicht erforderlich für SNMPv2)
- Priv Password: Datenschutz-Passwort für SNMPv3 (nicht erforderlich für SNMPv2)
- Auth Protocol: Protokoll für die Authentifizierung (MD5 oder SHA)
- Priv Protocol: Verschlüsselungsprotokoll (DES, AES128)

- Traps – Enabled: Aktivieren von TITAN-basierten Gerätefällen
- Traps – UDP Port: Geben Sie den Port für SNMP-TRAPS an.
- Traps – IP: IP-Adresse für das Senden von TRAPS SNMP.
- Traps – Community: Community-Feld zum Senden von TRAPS (nur für SNMPv2c)
- Alarm OS: Ermöglicht die Alarmtraps des Betriebssystems des Geräts im Falle einer kritischen Störung.
- Number traps alarm on: Gibt die Anzahl der Traps an, die gesendet werden sollen, wenn ein Alarmtrap ausgelöst wird.
- Number traps alarm off: Gibt die Anzahl der Traps an, die gesendet werden sollen, wenn ein Alarmtrap deaktiviert wird.
- Zeitraum der Falle: Gibt den Zeitraum in Sekunden an, in dem Alarmtraps gesendet werden.



webdyn powered by **TITAN**
flexitron group

★ **Mobile**

- ◉ Status
- ◉ Basic Settings
- ◉ Keep Online

★ **Ethernet**

- ◉ Basic Settings

★ **Wifi**

- ◉ Basic Settings
- ◉ DHCP Server

★ **Firewall**

- ◉ NAT
- ◉ Authorized IPs

★ **Serial Settings**

- ◉ Serial Port1-RS232
- ◉ Serial Port2-RS485
- ◉ SSL Certificates

★ **External Devices**

- ◉ Logger configuration
- ◉ ModBus Devices
- ◉ Generic Serial Device
- ◉ Temperature Sensor
- ◉ IEC102 Meter
- ◉ W-MBus
- ◉ GPS Receiver

★ **Other**

- ◉ AT Command
- ◉ DynDns
- ◉ Private DynDns
- ◉ Sms control
- ◉ Periodic Autoreset
- ◉ Time Servers
- ◉ Remote Console
- ◉ Smm

► **Other ► SNMP**

Enabled: ☒ Enable SNMP v2c

SNMP Version: SNMPv2 or SNMPv3

UDP Port: Default UDP port 161

Custom OID: Enterprise-Product OID. Default: .45711.1.1

Community: Only SNMPv2. Password for GET and SET commands

Username: Only SNMPv3.

Auth Password: Only SNMPv3 (min 8 char)

Priv. Password: Only SNMPv3 (min 8 char)

Auth Protocol: Only SNMPv3.

Priv Protocol: Only SNMPv3.

Engine ID: Only SNMPv3. "AUTO" or custom HEX

Traps Enabled: ☒ Enable Traps

Traps - UDP Port: Default: UDP port 162

Traps - IP: IP for sending traps

Traps - Community: Only SNMPv2. Community for traps

Alarm OS: ☐ Enable trap for Oper. System alarm

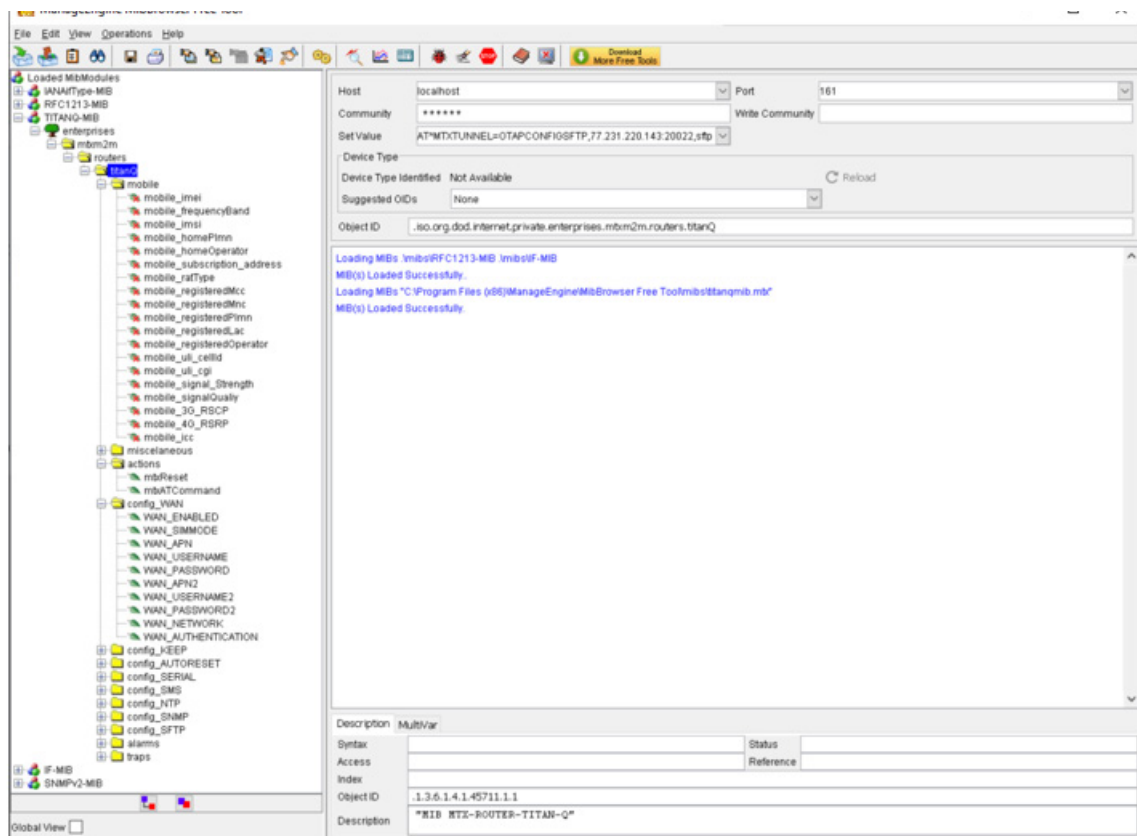
Number traps alarm ON: Number the traps sent when an alarm is activated. 0 ... 1440

Number traps alarm OFF: Number the traps sent when an alarm is deactivated. 0 ... 1440

Trap period: Period between traps (10...3600 sec)

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Auf dem vorherigen Bildschirm befindet sich ein Link mit dem Text „Click here for download MIB“. Laden Sie die Datei herunter, um die MIB mit den OIDs zu erhalten.
- Mit SNMP können Sie das Gerät überwachen, indem Sie z. B. die RSSI (Reichweite), das Datum und die Uhrzeit, die Betriebszeit, die Betriebsart 4G/3G/2G oder den verwendeten Betreiber abfragen.
- Eine sehr interessante Option ist der Bereich „Action“. Darin werden Sie sehen, dass Sie 2 Dinge tun können. Eine davon ist das Zurücksetzen des Geräts aus der Ferne. Zum anderen können Sie einen AT-Befehl über SNMP aus der Ferne ausführen (durch Schreiben in die Registrierung wird der AT-Befehl ausgeführt, und durch Lesen erhalten Sie die Antwort). Durch das Senden von AT-Befehlen können Sie über SNMP alles Mögliche tun, z. B. ein mit dem Gerät verbundenes Modbus-Gerät auslesen, Konfigurationsparameter ändern, eine GPS-Position auslesen, einen digitalen Eingang auslesen, den Status eines digitalen Ausgangs ändern ..



4.7.9 Sonstiges >> TACACS+

TITAN-basierte Geräte haben die Möglichkeit der Authentifizierung durch Tacacs+. Diese Funktion soll die externe Authentifizierung für HTTP-, Telnet- und SSH-Dienste von TITAN-basierten Geräten ermöglichen. Um diese Funktion zu nutzen, muss dieser Bereich konfiguriert werden.

- **Server:** IP- oder DNS-Adresse des Tacacs+-Servers
- **Port:** #ort, an dem der Tacacs+ Server abgehört wird (Standardwert 49).
- **KEY:** Passwort für die Verschlüsselung.
- **Service http:** Aktivieren Sie das Kontrollkästchen, wenn Sie möchten, dass der HTTP-Zugang zu den TITAN-basierten Geräten den Tacacs+-Authentifizierungsdienst verwendet.
- **Service Console:** Aktivieren Sie das Kontrollkästchen, wenn Sie möchten, dass der TELNET- oder SSH-Zugang (Remote Console) zu den TITAN-basierten Geräten den Tacacs+-Authentifizierungsdienst verwendet.

The screenshot shows the webdyn configuration interface, powered by TITAN. The interface has a sidebar on the left with navigation links: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), and Serial Settings. The main content area is titled 'Other > Tacacs+ authentication'. It contains the following fields and options:

- Server:** A text input field with the placeholder 'IP or DNS of Tacacs+ server'.
- Port:** A text input field with the value '49' and a range indicator '0 ... 65535 (default 49)'.
- Key:** A text input field with the placeholder 'KEY for tacacs+'.
- Service Http:** A checkbox with the label 'Check if tacacs+ is needed for HTTP (WAN)'.
- Service Console:** A checkbox with the label 'Check if tacacs+ is needed for CONSOLE'.

Below these fields, there is a note: 'Note: although tacacs+ "service http" to be active, the "admin" user will be able to use the local password.' At the bottom of the configuration area is a 'SAVE CONFIG' button.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.10 Other > MQTT

TITAN-basierte Geräte können als MQTT-Client arbeiten, indem sie sich mit einem MQTT / MQTT-Broker verbinden. Die Konfiguration des TITAN-basierten Geräts als MQTT-Client ermöglicht das Senden der

im internen Datenlogger gesammelten Daten (Daten von Sensoren, Modbus-Geräten, ...) über MQTT. Sie müssen diesen Abschnitt ordnungsgemäß konfigurieren, wenn Sie im Abschnitt LOGGER das Senden per MQTT auswählen.

- Enabled: Wählen Sie aus, ob Sie den MQTT-Client-Dienst aktivieren möchten
- Benutzername: Username MQTT. Leer, wenn nicht verwendet.
- Password: Password MQTT. Leer, wenn nicht verwendet
- ID: Feld für die Geräteidentifikation
- QoS: Qualität der Dienstleistung (0,1,2)
- KeepAlive: Sekunden für Keepalive (empfohlen 300)
- Beharrlichkeit: Wählen Sie, ob die Daten dauerhaft sein sollen
- AT Topic: Thema 1, für das sich TITAN-basierte Geräte anmelden werden. AT-Befehle, die Sie an dieses Thema senden, werden auf dem Gerät ausgeführt.
- AT Resp Topic: Antworten auf AT-Befehle, die über MQTT von TITAN-basierten Geräten im „AT Topic“ empfangen werden, werden über MQTT an dieses Topic gesendet.
- AT Topic 2: Thema 2, für das sich TITAN-basierte Geräte anmelden werden. AT-Befehle, die Sie an dieses Thema senden, werden auf dem Gerät ausgeführt.
- AT Resp Topic 2: Antworten auf AT-Befehle, die über MQTT vom TITAN-basierten Team im „AT Topic 2“-Thema empfangen werden, werden über MQTT an dieses Thema gesendet
- AT Topic 3: Thema 3, für das sich TITAN-basierte Geräte anmelden werden. AT-Befehle, die Sie an dieses Thema senden, werden auf dem Gerät ausgeführt.
- AT Resp Topic 3: Antworten auf AT-Befehle, die über MQTT vom TITAN-basierten Team im „AT Topic 3“-Thema empfangen werden, werden über MQTT an dieses Thema gesendet
- MQTT Script Topic 1: Thema MQTT, in dem ein anpassbares Script beim Empfang von Daten ausgeführt wird. Weitere Informationen finden Sie im Abschnitt Scripte in diesem Handbuch und in den Anwendungshinweisen.
- MQTT Script Topic 2: Thema MQTT, in dem ein anpassbares Script beim Empfang von Daten ausgeführt wird. Weitere Informationen finden Sie im Abschnitt Scripte in diesem Handbuch und in den Anwendungshinweisen.
- Client Certificate: Bei der Verwendung von MQTTS mit Client-Authentifizierung muss in dieses Feld die .key-Datei des Client-Zertifikats (PEM-Format) eingegeben werden.

- Serial Port2-485
- SSL Certificates

★ **External Devices**

- Logger configuration
- ModBus Devices
- Generic Serial Device
- Temperature Sensor
- IEC102 Meter
- W-MBus
- GPS Receiver

★ **Other**

- AT Command
- DynDns
- Private DynDns
- Sms control
- Periodic Autoreset
- Time Servers
- Remote Console
- Snmp
- Tacacs+
- Mqtt
- Http / Https
- User Permissions
- Passwords Web UI
- CA Certificates
- Email Config
- ModBus Slave
- Titan Scripts
- Connectivity tools
- Digital I/O
- Custom Skin
- Led Config
- Syslog
- Backup / Factory
- Firmware Upgrade
- Reboot
- Logout

► **Other ► MQTT Client**

Enabled: ☐ Enable MQTT client

Destination MQTT Broker. Examples:
tcp://test.mosquitto.org:1883
ssl://test.mosquitto.org:8883 (certificate needed)
ssl://test.mosquitto.org:8884 (certificates needed)

MQTT Broker:

MQTT Username: MQTT Username (blank if not used)

MQTT Password: MQTT Password (blank if not used)

MQTT ID: Device identification

MQTT Qos: MQTT Quality Of Service (0 ... 2)

MQTT Keepalive: Seconds for keepalive (30 ... 3600)

MQTT Persistence: ☐ Data persistence

MQTT AT Topic: This topic will be subscribed for receiving AT Commands (usefull for individual device)

MQTT AT Resp Topic: This topic will be used for publishing the AT Command Responses of AT Topic

MQTT AT Topic 2: This topic will be subscribed for receiving AT Commands (usefull for groups)

MQTT AT Resp Topic 2: This topic will be used for publishing the AT Command Responses of AT Topic 2

MQTT AT Topic 3: This topic will be subscribed for receiving AT Commands (usefull for all devices)

MQTT AT Resp Topic 3: This topic will be used for publishing the AT Command Responses of AT Topic 3

MQTT Script Topic 1: When data is received in this topic the 'Topic Script' will be executed.

MQTT Script Topic 2: When data is received in this topic the 'Topic Script' will be executed.

SAVE CONFIG

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Beachten Sie, dass Sie den Text [IMEI] anstelle der IMEI-Nummer eingeben können. Das heißt, wenn die IMEI 01234567678912345 lautet, wäre es dasselbe, das TOPIC /0123456789012345/TEST zu verwenden wie das Topic /[IMEI]/TEST
- Beachten Sie, dass Sie bei Verwendung von MQTTS möglicherweise das vom MQTT-Broker verwendete CA-Zertifikat in den Abschnitt „Andere àCA-Zertifikate“ aufnehmen müssen.
- In früheren TITAN-Firmware-Versionen wurden die Antworten auf AT-Befehle in einem beliebigen Topic an ein einziges Topic gesendet. Wenn Sie das gleiche Verhalten wünschen, können Sie den gleichen Wert in den Themen „AT Resp Topic“, „AT Resp Topic 2“, „AT Resp Topic 3“ einstellen

4.7.11 Other > HTTP / HTTPS

HTTP-Konfiguration und HTTPS-Aktivierung für die Konfigurationsumgebung.

- **HTTP Port:** gibt den TCP-Port für die Fernkonfiguration über HTTP an. Wenn Sie zum Beispiel 8080 angeben, lautet die Konfigurations-URL `http://x.x.x.x:8080`. Standardmässig ist der Port 80, aber wenn Sie auf den TCP80-Port eines ETH-internen Geräts (IP-Kamera, SPS) NAT machen wollen, müssen Sie ihn auf z. B. 8080 ändern. Der HTTP-Dienst ist nicht aus der Ferne nutzbar, wenn HTTPS aktiviert ist.
- **HTTPS Enabled:** Aktiviert den HTTPS-Dienst (Zertifikate werden nach dem Neustart automatisch generiert).
- **HTTP Port:** Gibt den TCP-Port der Konfiguration über HTTPS an. Standard 443.
- **HTTPS Key and Cert:** Für den HTTPS-Server des TITAN-basierten Teams können Sie Ihr eigenes Zertifikat verwenden. In diesem Feld kann man das ZERTIFIKAT und den SCHLÜSSEL in der gleichen Datei (PEM-Format) eingeben

The screenshot shows the webdyn configuration interface. The sidebar on the left contains a menu with the following items: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), and External Devices. The main content area is titled 'Other > Http/Https'. It contains the following fields and controls: 'HTTP port:' with a value of 80 and a note 'HTTP port for remote WAN connections. Not used if HTTPS is enabled.'; 'HTTPS enabled:' with an unchecked checkbox and a note 'Enable HTTPS Web Server. First certificate is generated automatically'; 'HTTPS port:' with a value of 443 and a note 'HTTPS port for remote WAN connections'. Below these is a 'SAVE CONFIG' button. Further down is a section 'Custom KEY and Certificate for HTTPS WebServer (PEM format)' containing a file selection button 'Seleccionar archivo', a text field 'Ninguno archivo selec.', an 'Upload' button, and the status 'not uploaded'.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Wenn Sie versuchen, sich über HTTPS mit TITAN-basierten Geräten zu verbinden, wird Ihr Browser wahrscheinlich eine Warnmeldung bezüglich des selbstsignierten digitalen Zertifikats anzeigen. Das ist völlig normal.

4.7.12 Other > User Permissions.

In diesem Abschnitt können Sie die Berechtigungen konfigurieren, auf die der „user“ und „guest“ Zugriff haben werden. Die Konfigurationsoptionen, die Sie nicht auswählen, werden nicht im linken Menü der Konfigurationsumgebung angezeigt, wenn Sie sich mit dem Benutzer „user“ oder „guest“ am Gerät anmelden.



powered by **TITAN**

- ★ **Mobile**
 - Status
 - Basic Settings
 - Keep Online
- ★ **Ethernet**
 - Basic Settings
- ★ **WiFi**
 - Basic Settings
 - DHCP Server
- ★ **Firewall**
 - NAT
 - Authorized IPs
- ★ **Serial Settings**
 - Serial Port1-RS232
 - Serial Port2-RS485
 - SSL Certificates
- ★ **External Devices**
 - Logger configuration
 - Modbus Devices
 - Generic Serial Device
 - Temperature Sensor
- IEC102 Meter
- W-Mbus
- GPS Receiver
- ★ **Other**
 - AT Command
 - DynDNS
 - Private DynDNS
 - Sns control
 - Periodic Autoreset
 - Time Servers
 - Remote Console
 - Sntp
 - Tacacs+
 - Mqtt
 - Http / Https
 - User Permissions
 - Passwords Web UI
 - CA Certificates
 - Email Config
 - Modbus Slave
 - Titan Scripts
 - Connectivity tools
 - Digital I/O
 - Custom Skin
 - Led Config
 - Syslog
 - Backup / Factory
 - Firmware Upgrade
 - Reboot
 - Logout

► **Other ► User Permissions**

Mobile	Basic Settings	☐
	Keep Online	☐
Ethernet	Basic Settings	☐
WiFi	Basic Settings	☐
	DHCP Server	☐
Firewall	NAT	☐
	Authorized IPs	☐
Serial Settings	Serial Port 1	☐
	Serial Port 2	☐
	SSL Certificates	☐
External devices	Logger config.	☐
	Modbus devices	☐
	Generic serial	☐
	Temperature sen.	☐
	IEC102 meter	☐
	W-Mbus	☐
	GPS Receiver	☐
Other	DynDNS	☐
	Private DynDNS	☐
	SMS Control	☐
	Periodic autoreset	☐
	Time Servers	☐
	Remote Console	☐
	Sntp	☐
	Tacacs+	☐
	Mqtt	☐
	Http / Https	☐
	CA-Certificates	☐
	Email config	☐
	Modbus Slave	☐
	Titan Scripts	☐
	Connectivity tools	☐
	Digital I/O	☐
	Custom Skin	☐
	Led Config	☐
	Syslog	☐
	Backup / Factory	☐
	Firmware Upgrade	☐
	Reboot	☐

SAVE CONFIG

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.13 Other > Passwords.

Für den Zugang zur Konfiguration des Geräts gibt es drei Benutzernamen. Der „admin“-Benutzer, über den Sie Zugriff auf die gesamte Konfiguration des Geräts haben, und der „user“-Benutzer, über den Sie Zugriff auf die von Ihnen ausgewählten Konfigurationen haben (sehr nützlich, wenn Sie das Gerät mit Ihren Logos personalisieren). In diesem Bereich können Sie das Passwort beider Benutzer ändern. Außerdem gibt es den „guest“-Benutzer, mit dem Sie auf die gleichen Menüs wie der „user“-Benutzer zugreifen können, ohne jedoch Konfigurationsänderungen vornehmen zu können.

The screenshot shows the webdyn configuration interface. The sidebar on the left contains a menu with the following items:

- ★ Mobile
 - ◊ Status
 - ◊ Basic Settings
 - ◊ Keep Online
- ★ Ethernet
 - ◊ Basic Settings
- ★ Wifi
 - ◊ Basic Settings
 - ◊ DHCP Server
- ★ Firewall
 - ◊ NAT
 - ◊ Authorized IPs
- ★ Serial Settings
 - ◊ Serial Port1-RS232
 - ◊ Serial Port2-RS485
 - ◊ SSL Certificates
- ★ External Devices
 - ◊ Logger configuration
 - ◊ ModBus Devices
 - ◊ Generic Serial Device
 - ◊ Temperature Sensor
 - ◊ IEC102 Meter
 - ◊ W-MBus
 - ◊ GPS Receiver

The main content area is titled 'Other > Password Web UI'. It contains two sections:

Administrator

Username: Mandatory. Default 'admin'

Password: Password for router administration

Re enter Password: Re-enter password for router administration

General User

Username: Blank is not used

Password: Password for router administration (user)

Re enter Password: Re-enter password for router administration (user)

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.14 Other > CA Certificates

Alle Dienste, die sichere Verbindungen über SSL/TLS mit HTTPS- oder MQTTS-Servern nutzen, benötigen das von diesem Server verwendete CA-Root-Zertifikat, um das Zertifikat des Servers zu überprüfen. Über diesen Abschnitt können Sie bis zu 2 benutzerdefinierte CA-Root-Server (im PEM-Format) eingeben.

Es besteht auch die Möglichkeit, die Option „Allow all certificates“ zu wählen. Diese Option wird nicht empfohlen, es sei denn, Sie verfügen über eine sichere Verbindung (IPSec, OpenVPN, SIM mit privatem APN usw.), da das Zertifikat eines Remote-Servers nicht überprüft wird.



Zusätzliche Hinweise.

- TITAN-basierte Geräte verfügen über eine interne Liste der gängigsten Root-CA-Zertifikate. Wenn Sie ein Zertifikat benötigen, das nicht verfügbar ist, können Sie es hier eingeben.

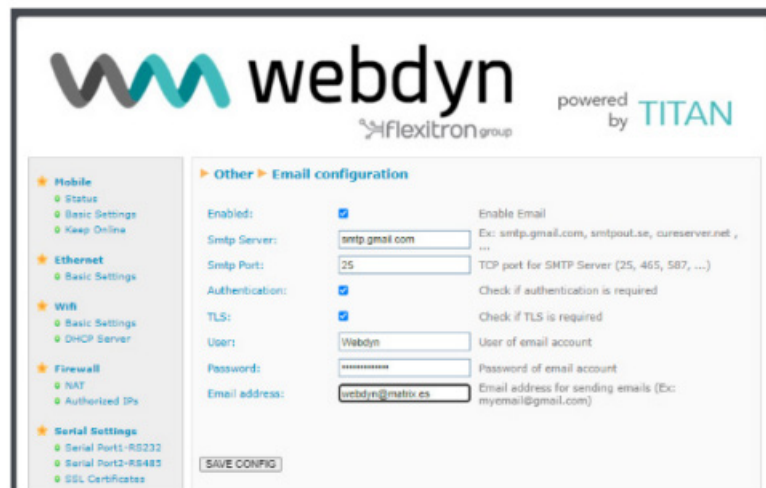
4.7.15 Other > Email Configuration

TITAN-basierte Geräte ermöglichen den Versand von E-Mail-Benachrichtigungen. Sie ermöglichen auch den Versand von E-Mails über AT-Befehle (z. B. wenn Sie eine SPS haben und eine SMS oder EMAIL senden wollen, können Sie dies tun, indem Sie einen AT-Befehl an das TITAN-basierte Gerät senden).

TITAN-basierte Geräte müssen vorkonfiguriert sein, um E-Mails versenden zu können. Das heißt, Sie müssen den SMTP-Server konfigurieren, der in diesem Abschnitt verwendet werden soll.

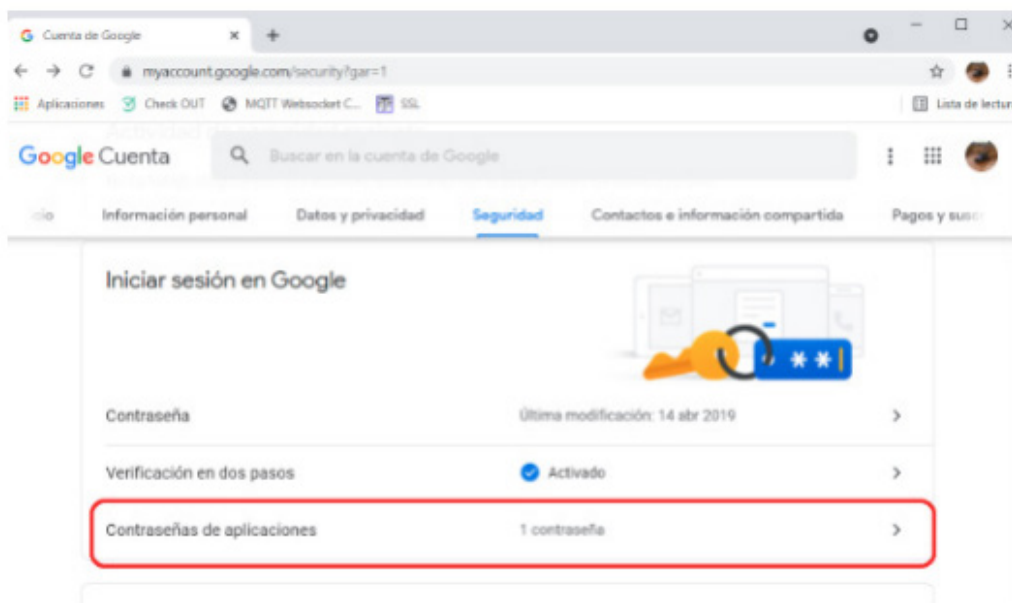
- Enabled: Aktiviert den E-Mail-Dienst.
- Smtip-Server: Gibt die IP- oder DNS-Adresse des SMTP-Servers an (z. B. smtp.gmail.com, smtpout.secureserver.net, ...)

- Smtip Port: SMTP-Server TCP-Anschluss
- Authentication: Wählen Sie aus, ob der SMTP-Server eine Authentifizierung erfordert (normalerweise ja)
- TLS: Wählen Sie, ob der SMTP-Server TLS benötigt
- Benutzer: Benutzernamen des E-Mail-Kontos des Absenders
- Password: Passwort des Quell-E-Mail-Kontos
- Email address: Quell-E-Mail-Adresse, von der aus die E-Mails gesendet werden sollen



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Beachten Sie, dass Sie bei Verwendung des GMAIL SMTP-Servers ein „Anwendungskennwort“ erstellen müssen. Gehen Sie dazu in Ihren „Google Account Manager“, wählen Sie das Menü „Sicherheit“ und fügen Sie ein „Passwort für Anwendungen“ hinzu.



4.7.16 Other> Modbus Slave

TITAN-basierte Geräte können so konfiguriert werden, dass sie als Modbus TCP-Slave-Gerät und/oder als Modbus RTU-Slave fungieren. Mit dem Modbus-Protokoll können Sie z. B. aus der Ferne (über 4G/3G/2G, Ethernet oder Wifi) die digitalen Ausgänge des Geräts schalten, den Status der digitalen Eingänge abfragen, sowie SMS senden, SMS empfangen oder sogar E-Mails über Modbus versenden.

Die Speichertabelle mit den Modbus-Adressen der Register des TITAN-basierten Gerätes ist dann verfügbar. Die unterstützten Modbus-Befehle sind: 0x03 zum Lesen und 0x10 zum Schreiben.

Datensatz-ID	R/W	Mögliche werte	Beschreibung
1	R	0 ... 32635	Firmware Version
2	R	0 ... 32635	Firmware-Subversion
6	R	0 ... 31	GSM-Signal RSSI
7	R	2,3,4	Eingesetzte Technologie (2=2g,3=3g,4=4g)
8	R	1....31	tag
9	R	1.....12	monat
10	R	2000...2099	jahr
11	R	0....23	stunde
12	R	0.....59	protokoll
13	R	0.....59	Nachschlag

20	W	1	Zurücksetzen ausführen
30	RW	0,1	GPIO 0
31	RW	0,1	GPIO 1
32	RW	0,1	GPIO 2
33	RW	0,1	GPIO 3
34	RW	0,1	GPIO 4
98	W	0 ... 32635	Länge des auszuführenden AT-Befehls
99	R	0 ... 32635	Länge der AT-Befehlsantwort
100..354	W	ASCII	AT-Befehltext (in ASCII)
500...754	R	ASCII	AT-Befehlsantworttext (in ASCII)
1000	R/W	0,1	1 zeigt an, dass neue SMS empfangen wurden. Eine SPS muss nach dem Lesen der SMS eine 0 schreiben.
1001	R	0.....18	Länge des Telefons, das die SMS gesendet hat
1002...1019	R	ASCII	Telefonnummer, mit der die SMS gesendet wurde
1020	R	0....160	Länge des SMS-Nachrichtentexts
1021...1180	R	ASCII	SMS-Nachrichtentext
1021...1180	R	ASCII	SMS-Nachrichtentext
10000	RW	0....65535	Benutzerregistrierung 10000
10001...19998	RW	ASCII	Benutzerregistrierung von 10001 bis 19998
19999	RW	0...65535	Benutzerregistrierung 10999

AT-Befehle über Modbus-Protokoll

Ein weiteres sehr interessantes Merkmal der TITAN-basierten Geräte ist, dass sie die Ausführung von AT-Befehlen über das Modbus-Protokoll ermöglichen. Wenn Sie zum Beispiel eine SPS haben, die als Modbus TCP Master fungiert, können Sie über das Modbus TCP Protokoll einen Befehl an das Gerät senden, um einen AT-Befehl auszuführen, um Daten wie die Reichweite zu erhalten, eine SMS zu senden, die Uhrzeit zu erhalten, das Gerät zurückzusetzen, usw.

Im Folgenden wird beschrieben, wie Sie einen AT-Befehl über Modbus ausführen

Vorgehensweise bei der Ausführung eines AT-Befehls über Modbus

Das Verfahren zum Ausführen eines AT-Befehls über Modbus ist sehr einfach. Dies lässt sich am besten anhand eines Beispiels nachvollziehen. Nehmen wir an, dass wir den Befehl AT+CSQ ausführen wollen, um die Reichweite zu ermitteln

1- Schreiben Sie den AT-Befehl in ASCII, beginnend mit Register 100.

Registrierungs-ID	wert	Beschreibung
100	65	Buchstabe ASCII: A
101	84	Buchstabe ASCII: T
102	43	Buchstabe ASCII: +
103	67	Buchstabe ASCII: C
104	83	Buchstabe ASCII: S
105	81	Buchstabe ASCII: Q

2- Der Befehl AT+CSQ besteht aus 6 Zeichen. Um den AT-Befehl auszuführen, schreiben wir eine 6 in das Register 98. Nach dem Beschreiben des Registers 98 soll der AT-Befehl sofort ausgeführt werden.

Registrierungs-ID	wert	Beschreibung
98	6	Größe des auszuführenden Befehls

3.- Wir überprüfen das Ergebnis der Ausführung des AT-Befehls, indem wir das Register 99 lesen. Der gelesene Wert ist die Länge der Antwort. Ein Wert von 0 bedeutet, dass noch keine Antwort vorliegt (die Ausführung ist noch nicht abgeschlossen, was in der Regel weniger als 1 Sekunde dauert). Ein Wert >0 gibt die Länge der Antwort an.

Registrierungs-ID	wert	Beschreibung
99	28	Größe der Befehlsantwort

4.- Schließlich lesen wir die 28 Register, in denen die Antwort enthalten ist, ab Register 500 aus

Registrierungs-ID	wert	Beschreibung
500	65	A
501	84	T
502	43	+
503	67	C
504	83	S
505	81	Q
506	13	\r
507	13	\r
508	10	\n
509	43	+
510	67	C
511	83	S
512	81	Q
513	58	:
514	32	SPACE
515	49	1
516	54	6
517	44	
518	57	9
519	57	9
520	13	\r
521	10	\n
522	13	\r
523	10	\n
524	79	O
525	75	K
526	13	\r
527	10	\n

Im Falle dieses AT-Befehls sind die relevanten Register 515 und 516, die eine Abdeckung des Wertes „16“ anzeigen.

P.S. Denken Sie daran, dass Sie den in dieser Anleitung angegebenen AT-Befehl verwenden müssen, wenn Sie diese Funktion zum Senden einer SMS nutzen möchten: AT^MTXTUNNEL=SMS,Telefon,Nachricht

Verfahren für den Empfang einer SMS

Das Verfahren zum Empfang von SMS-Nachrichten über Modbus TCP ist sehr einfach. Ihre SPS muss regelmäßig das Register 1000 überprüfen. Wenn der gelesene Wert eine „1“ ist, bedeutet dies, dass eine neue SMS-Nachricht eingetroffen ist. Sie müssen sie dann über die beteiligten Register 1001-1180 lesen. Nach dem Lesen müssen Sie eine „0“ in das Register 1000 schreiben.



Zusätzliche Hinweise.

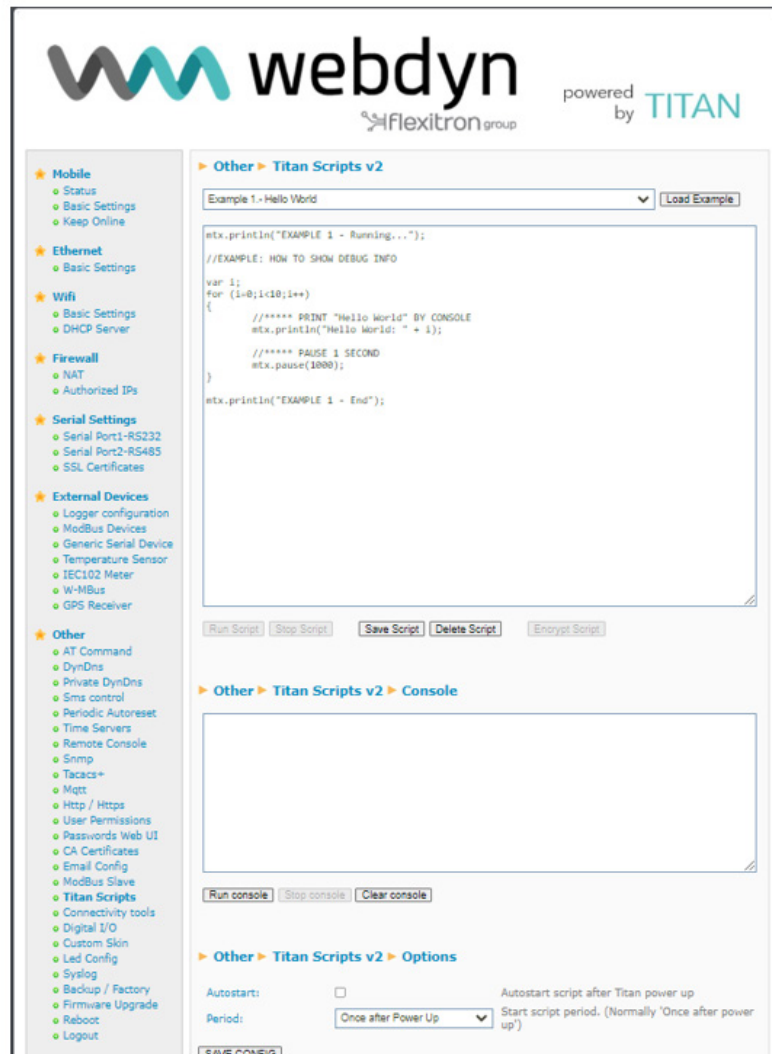
- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Siehe die Tabelle der Modbus-Register in den Konfigurationsmenüs des TITAN-Geräts selbst, im Abschnitt Other > Modbus Slave

4.7.17 Other > TITAN Scripts

TITAN-basierte Geräte ermöglichen die Ausführung eines benutzerprogrammierbaren Scripte in JAVASCRIPT-Sprache (ECMAScript 5) <https://www.w3schools.com/jsref/default.asp>. Von diesem Skript aus können Sie auf verschiedene Funktionen der TITAN-basierten Einheit zugreifen, um kleine Anpassungen vorzunehmen (z. B. Lesen von Geräten über die serielle Schnittstelle, Lesen von digitalen Eingängen, Ändern eines digitalen Ausgangs, Lesen eines Modbus-Geräts, Senden einer SMS-Nachricht,

Senden einer EMAIL, einer MQTT-Nachricht an ein bestimmtes Thema, Senden eines SNMP-TRAP, Speichern und Lesen von Dateien in der Einheit usw. (Siehe die verschiedenen Beispiele der TITAN-basierten Einheit zum besseren Verständnis).

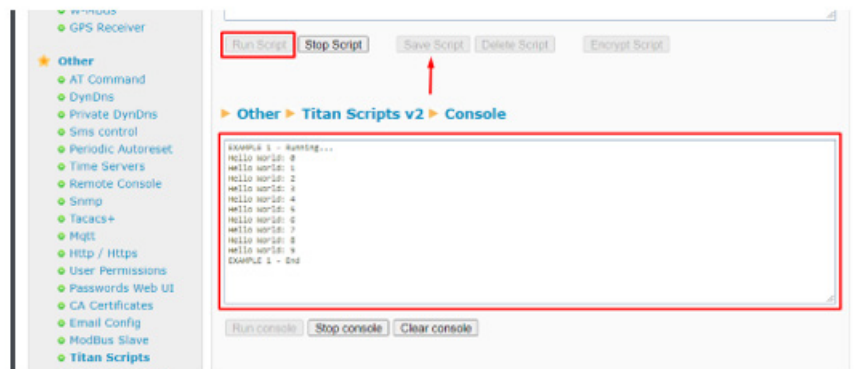
Der Konfigurationsbildschirm für TITAN-Skripte sieht wie folgt aus:



Im Dropdown-Menü oben finden Sie mehrere Beispiele für alle Funktionen, die Sie verwenden können. Um ein Beispiel zu laden, wählen Sie das Beispiel Ihrer Wahl aus dem Dropdown-Menü aus (für das erste Mal wird das Beispiel „Hello World“ empfohlen) und klicken dann auf die Schaltfläche „Load Example“. Nach dieser Aktion wird der Quellcode des Beispiels auf dem Bildschirm angezeigt.

Klicken Sie dann auf die Schaltfläche „Save Script“, um den Beispielcode im Ausführungsspeicher des TITAN-basierten Geräts zu speichern. Danach können Sie auf die Schaltfläche „Run Script“ klicken, um das Skript auszuführen. In wenigen Sekunden werden Sie im Konsolenbereich die Spuren des

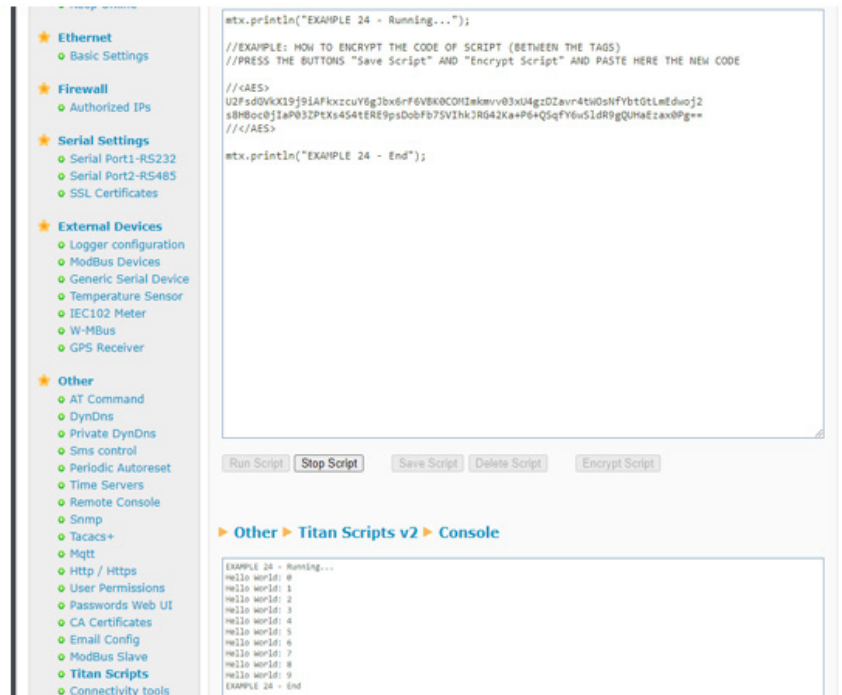
Programms „mtx.println()“ sehen.



Wenn Sie den Scriptcode verschlüsseln möchten, klicken Sie auf die Schaltfläche „Encrypt Script“, woraufhin ein Popup-Fenster mit einem neuen Code angezeigt wird.



Nachdem dieser neue Code in das Script eingefügt wurde, kann der TITAN-basierte Computer das Script auf dieselbe Weise ausführen.



Weitere Informationen zur Scriptverschlüsselung finden Sie in den Beispielen 24 und 25.

TITAN-Skripte Konfigurationsoptionen

Sobald Sie Ihr Script entwickelt haben und es läuft, möchten Sie, dass es bei jedem Neustart des TITAN-Computers selbstständig läuft. Dazu müssen Sie das Kontrollkästchen „Autostart“ aktivieren. Wenn dieses Kästchen markiert ist, müssen Sie den Autostart-Modus angeben. Der übliche Weg ist „Once after Power Up“, d. h. das Script wird einmal nach dem Hochfahren des TITAN-basierten Computers ausgeführt. Dies ist für die meisten Anwendungen dieser Art optimal:

```
while (true) {  
  
...  
  
}
```

bei dem der Code zyklisch ausgeführt wird. Vielleicht finden Sie es aber bequemer, das Script automatisch in bestimmten Zeitabständen (alle 1 Minute, 2 Minuten, 5 Minuten usw.) ausführen zu lassen, um bestimmte Aufgaben zu erledigen. Stellen Sie sich beispielsweise den Fall vor, dass Sie ein Script benötigen, das alle 15 Minuten ein Modbus-RTU-Gerät ausliest und den Messwert an einen MQTT-Server sendet. In diesem Fall ist es vielleicht günstiger, das Script alle 15 Minuten auszuführen.

Das TITANSkripts „mtx“-Objekt.

Wie in den vorangegangenen Abschnitten erwähnt, können Sie mit TITANSkripts kleine Scripte in der Sprache JavaScript (ECMAScript 5) programmieren, um mit bestimmten Funktionen von TITAN-basierten Geräten zu interagieren. Der Zugriff auf diese Funktionen erfolgt über bestimmte Funktionen eines „mtx“-Objekts. Jede dieser Funktionen wird im Folgenden beschrieben. Es wird dringend empfohlen, zum besseren Verständnis die kleinen Beispiele im Abschnitt „Other à TITAN Scripts“ zu studieren. Beachten Sie, dass TITAN-Scripte dazu gedacht sind, kleine Anpassungen im Verhalten von TITAN-basierten Geräten

vorzunehmen, und nicht, um irgendeine Art von Anwendung zu programmieren, wie es in anderen Sprachen wie „Java“, „C++“, „Python“ usw. möglich wäre. Im Grunde genommen ist alles, was Sie tun können, in den mitgelieferten Beispielen enthalten.

IOx DIGITAL INPUTS / OUTPUTS bezogene Funktionen:

In den „Hinweisen“ zu jeder Funktion finden Sie eine Liste von Beispielskripten, die diese Funktion verwenden. Diese Beispiele werden im Router selbst über das Menü „Other à TITAN Scripts“ bereitgestellt.

- **Funktion: `mtx.ioGet(idIO)`**

Beschreibung: ermöglicht die Abfrage des Status eines digitalen Eingangs/Ausgangs.

Parameter: idIO: int 0,1,2,3,4, ... (IO-Bezeichner)

Antwort: int (0=Eingang nicht aktiviert, 1=Eingang aktiviert, -1=Fehler)

Hinweis: siehe Beispiele: 3, 15 16

- **Funktion: `mtx.ioSet(idIO, Wert)`**

Beschreibung: ermöglicht die Änderung des Status eines digitalen Ausgangs.

Parameter: idIO: (int) 0,1,2,3,4, ... (IO-Bezeichner)

Wert: (int) 0,1 (logischer Wert des digitalen Ausgangs)

Antwort: boolesch (true=Operation OK, false=Operation ERROR)

Hinweis: siehe Beispiele: 16

- **Funktion: `mtx.counterGet(idIO)`**

Beschreibung: ermöglicht es, den Wert des einem Eingang zugeordneten Impulszählers zu erhalten.

Parameter: idIO: int 0,1,2,3,4, ... (Kennung des digitalen Eingangs)

Antwort: long Zählerstand

Hinweis: siehe Beispiele: 34

- **Funktion: `mtx.counterSet(idIO, Wert)`**

Beschreibung: ermöglicht es, den Anfangswert eines Impulszählers ändern

Parameter: idIO: (int) 0,1,2,3,4, ... (IO-Bezeichner)

Wert: (long) (Zählerstand)

Antwort: boolesch (true=Operation OK, false=Operation ERROR)

Hinweis: siehe Beispiele: 34

Funktionen im Zusammenhang mit den LEDS des Routers:

- **Funktion: `mtx.ledSet(idLed, Wert)`**

Beschreibung: ermöglicht das Ein- und Ausschalten einer LED

Parameter: idLed: (int) 0,1,2, ... (Kennung des LED der geführten Geräte)
Wert: (int) 0=aus, 1=ein, 2=langsames Blinken, 3=schnelles Blinken.

Antwort: boolesch (true=Operation OK, false=Operation ERROR)

Hinweis: siehe Beispiele: 21

Funktionen im Zusammenhang mit AT COMMANDS:

- **Funktion: `mtx.atSend(command, timeout)`**

Beschreibung: ermöglicht die Ausführung eines AT-Befehls auf dem TITAN-basierten Gerät selbst

Parameter: Befehl: (String) auszuführender AT-Befehl
timeout: (int) Millisekunden der Zeitüberschreitung

Antwort: String: Antwort auf den AT-Befehl. „“= Fehler

Hinweis: siehe Beispiele: 2

MQTT-bezogene Funktionen:

- **Funktion: `mtx.mqttIsConnected()`**

Beschreibung: gibt zurück, ob das TITAN-basierte Gerät mit einem MQTT-Broker verbunden ist

Parameter: keine.

Antwort: boolesch (true=Ja, false=Nein)

Hinweis: siehe Beispiele: 4, 35

- **Funktion: `mtx.mqttSend(message, topic, qos)`**

Beschreibung: ermöglicht es Ihnen, eine MQTT-Textnachricht an ein bestimmtes mqtt-Topic zu senden mit einer bestimmten QoS

Parameter: Nachricht: (String) zu sendende Textnachricht
topic: (String) Topic mqtt, an das die Nachricht gesendet werden soll
qos: (int) Sende-QoS (0,1,2)

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 4, 8 35

- **Funktion: `mtx.mqttSendArray(array byte, topic, qos)`**

Beschreibung: ermöglicht das Senden einer MQTT-Nachricht aus einem Array von Bytes an ein bestimmtes mqtt-Topic mit einer bestimmten QoS

Parameter: Nachricht: (array-Byte) Zu versendende Textnachricht
topic: (String) Topic mqtt, an das die Nachricht gesendet werden soll
qos: (int) Sende-QoS (0,1,2)

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 35

- **Funktion: `mtx.mqttSubscribe(Thema)`**

Beschreibung: die TITAN-Scripte ermöglichen das Abonnement von 1 MQTT-Topic, um Mitteilungen von einem Broker zu empfangen. Mit dieser Funktion kann man sich für dieses Thema anmelden.

Parameter: Thema: (String) Thema mqtt, das die TITAN-Scripte empfangen sollen
nachrichten

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 35

- **Funktion: `mtx.mqttGetArray()`**

Beschreibung: Funktion, mit der geprüft und empfangen werden kann, ob Daten in dem durch die vorherige Funktion `mtx.mqttSubscribe(topic)` konfigurierten Thema angekommen sind

Parameter: keine

Antwort: Array-Bytes: (null=keine Daten, !null=Byte-Array mit Daten)

Hinweis: siehe Beispiele: 35

TRAPS SNMP-bezogene Funktionen:

- **Funktion: `mtx.trapSend(oid, message, severity)`**

Beschreibung: sendet einen SNMP-Trap

Parameter: oid: (String) OID des SNMP-Trap

message: (String) Mit dem SNMP-Trap verbundener Text
severity (int) Schweregrad der Trap (1, ... ,7)
Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)
Hinweis: siehe Beispiele: 5, 9

SMS-bezogene Funktionen:

- **Funktion: `mtx.smsSend(phoneNumber, textMessage)`**

Beschreibung: sendet eine SMS-Nachricht an eine Rufnummer

Parameter: phoneNumber: (String) Telefonnummer des Senders
textMessage: (String) Text der SMS-Nachricht

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 3 10 17 18,40

- **Funktion: `mtx.smsRead()`**

Beschreibung: prüft, ob eine neue SMS-Nachricht eingetroffen ist

Parameter: keine

Antwort: String-Array: (null=keine neue SMS, data[0]=Telefonnummer
data[1]=SMS-Nachricht)

Hinweis: siehe Beispiele: 40

HTTP-bezogene Funktionen:

- **Funktion: `mtx.httpRequest(url, headers,method,data,dataType)`**

Beschreibung: sendet eine E-Mail an eine E-Mail-Adresse

Parameter: url: (String) Verbindungsurl
headers: (HashMap) Benutzerdefinierte HTTP-Header
method: (String) GET oder POST
data: (String) Daten, die mit der http-Anfrage gesendet werden
dataType: (String) Datentyp, der mit der http-Anfrage gesendet werden soll

Hinweis: siehe Beispiele: 39

EMAILS-bezogene Funktionen:

- **Funktion** `mtx.emailSend(address, subject)`

Beschreibung: sendet eine E-Mail an eine E-Mail-Adresse

Parameter: address: (String) Ziel-E-Mail-Adresse
subject : (String) Betreff der gesendeten E-Mail

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 6, 11

Funktionen im Zusammenhang mit TELEGRAM:

- **Funktion:** `mtx.telegramSendMessage(apiToken, chatID,message)`

Beschreibung: sendet eine Textnachricht an einen Telegram-Gruppenchat

Parameter: apiToken: (String) Telegram Bot API-Token
chatID : (String) Chat-Identifikator, an den die Nachricht gesendet werden soll
message: (String) zu sendende Textnachricht

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 41, 42

SIM CARD-bezogene Funktionen

- **Funktion:** `mtx.simID()`

Beschreibung: gibt die benutzte SIM-Karte zurück

Parameter: keine

Antwort: int: (-1=FEHLER, 0=keine SIM, 1=SIM1, 2=SIM2)

Hinweis: siehe Beispiele: 18

- **Funktion:** `mtx.simInserted()`

Beschreibung: gibt zurück, ob die aktuelle SIM-Karte eingelegt ist

Parameter: keine

Antwort: int: (-1=FEHLER, 0=nicht eingefügt, 1=eingefügt)

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.simStatus()`**

Beschreibung: gibt den Status der aktuellen SIM zurück

Parameter: keine

Antwort: int: (-1=FEHLER, 0=SIMULATIONSFEHLER, 1=SIMULATIONSFÄHIG)

Hinweis: siehe Beispiele: 18

Funktionen im Zusammenhang mit SERIAL PORTS:

Funktion: `mtx.serialOpen(idPort,baudrate,databits,parity,stopbits,flowcontrol)`

Beschreibung: öffnet eine serielle Schnittstelle

Parameter:

<code>idPort:</code>	(int) Kennung der seriellen Schnittstelle (1,2)
<code>baudrate:</code>	(int) Geschwindigkeit (460800, 230400, ... , 1200, 600, 300)
<code>datenbits:</code>	(int) Anzahl der Bits pro Daten (8,7)
<code>parität:</code>	(int) 0=keine, 1=gerade, 2=gerade
<code>stopbits:</code>	(int) 1.2
<code>flowcontrol:</code>	(int) 0=kein, 1=Hardware (falls vorhanden)

Antwort: boolesch: true: OK, false: ERROR

Hinweis: siehe Beispiele: 19

- **Funktion: `mtx.serialClose(idPort)`**

Beschreibung: schließt eine serielle Schnittstelle

Parameter: `idPort:` (int) Kennung der seriellen Schnittstelle (1,2)

Antwort: boolean: true: OK, false: ERROR

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.serialRead(idPort)`**

Beschreibung: liest und gibt Daten zurück, die von einer seriellen RS232- oder RS485-Schnittstelle gelesen wurden

Parameter: `idPort:` (int) Kennung der seriellen Schnittstelle (1,2)

Feedback:

<code>byte []:</code>	Byte-Array mit gelesenen Daten
<code>null:</code>	keine Daten gelesen.

Hinweis: siehe Beispiele: 19

- **Funktion:** **mtx.serialWrite(idPort,data,start,length)**

Beschreibung: sendet ein Array von Bytes über die serielle Schnittstelle

Parameter: idPort: (int) Kennung der seriellen Schnittstelle (1,2)
data: (byte[]) Byte-Array für e
start: (int) Startindex des sendenden Byte-Arrays
length: (int) Anzahl der zu sendenden Bytes.

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 19

MODBUS-bezogene Funktionen:

- **Funktion:** **mtx.modbusRTUGetWords(address, command, start, numRegisters)**

Beschreibung: liest und gibt die Modbus-Register eines Modbus-RTU-Geräts zurück

Parameter: Adresse: (int) Modbus RTU-Adresse (1 ... 254)
command: (int) Modbus-Befehl 3 oder 4
start: (int) erste zu lesende Registeradresse
numRegisters: (int) Anzahl der zu lesenden Datensätze (1 ... 64)

Feedback: int []: Array von WORDS mit gelesenen Daten (Werte 0 ... 65535)
null: LesenFEHLER.

Hinweis: siehe Beispiele: 7, 8, 9, 10, 11, 12, 22, 30

- **Funktion:** **mtx.modbusRTUSetWords(address, command, start, values[])**

Beschreibung: schreibt Modbus-Register in ein Modbus-RTU-Gerät

Parameter: address: (int) Modbus RTU-Adresse (1 ... 254)
command: (int) Modbus-Befehl (16)
start: (int) erste zu schreibende Registeradresse
values[]: (int[]) Array mit den zu schreibenden WORDS

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 12

- **Funktion:** **mtx.modbusRTUGetBits(address, command, start, numBits)**

Beschreibung: liest die Bit-Typ-Modbus-Register eines Modbus-RTU-Geräts und gibt sie zurück

Parameter: address: (int) Modbus RTU-Adresse (1 ... 254)
command: (int) Modbus-Befehl 1 oder 2
start: (int) Adresse des ersten zu lesenden Registerbits (1 ... 65535)
numBits: (int) Anzahl der zu lesenden Bits (1 ... 64)
Antwort: int []: Array von BITS mit den gelesenen Bits (Werte 0,1)
null: LesenFEHLER.
Hinweis: siehe Beispiele: 13

• **Funktion** **mtx.modbusRTUSetBit(address, command, start, value)**

Beschreibung: schreibt 1 bitartiges Modbus-Register in ein Modbus-RTU-Gerät

Parameter: address: (int) Modbus RTU-Adresse (1 ... 254)
command: (int) Modbus-Befehl (5)
start: (int) Adresse des ersten zu schreibenden Registerbits
values: (int) zu schreibender Wert (0,1)
Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)
Hinweis: siehe Beispiele: 14

• **Funktion:** **mtx.modbusTCPGetWords(ip, port, command, start, numRegisters)**

Beschreibung: liest und liefert Modbus-Register von einem Modbus-TCP-Gerät

Parameter: ip: (String) IP-Adresse des Modbus-TCP-Geräts
Anschluss: (int) TCP-Port des Modbus-TCP-Geräts
command: (int) Modbus-Befehl 3 oder 4
start: (int) erste zu lesende Registeradresse
numRegisters: (int) Anzahl der zu lesenden Datensätze (1 ... 64)
Feedback: int []: Array von WORDS mit gelesenen Daten (Werte 0 ... 65535)
null: LesenFEHLER.
Hinweis: siehe Beispiele: ---

• **Funktion:** **mtx.modbusTCPSetWords(ip, port, command, start, values[])**

Beschreibung: schreibt Modbus-Register in ein Modbus-TCP-Gerät

Parameter: ip: (String) IP-Adresse des Modbus-TCP-Geräts
Anschluss: (int) TCP-Port des Modbus-TCP-Geräts

command: (int) Modbus-Befehl (16)
start: (int) erste zu schreibende Registeradresse
values[]: (int[]) Array mit den zu schreibenden WORDS

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: 22

- **Funktion:** **mtx.modbusTCPGetBits(ip, port, command, start, numBits)**

Beschreibung: liest die Bit-Typ-Modbus-Register eines Modbus-TCP-Geräts und gibt sie zurück

Parameter: ip: (String) IP-Adresse des Modbus-TCP-Geräts
Anschluss: (int) TCP-Port des Modbus-TCP-Geräts
command: (int) Modbus-Befehl 1 oder 2
start: (int) Adresse des ersten zu lesenden Registerbits (1 ... 65535)
numBits: (int) Anzahl der zu lesenden Bits (1 ... 64)

Antwort: int []: Array von BITS mit den gelesenen Bits (Werte 0,1)

null: LesenFEHLER.

Hinweis: siehe Beispiele: ---

- **Funktion:** **mtx.modbusTCPSetBit(ip, port, command, start, value)**

Beschreibung: schreibt 1 bitartiges Modbus-Register an ein Modbus-TCP-Gerät

Parameter: ip: (String) IP-Adresse des Modbus-TCP-Geräts
Anschluss: (int) TCP-Port des Modbus-TCP-Geräts
command: (int) Modbus-Befehl (5)
start: (int) Adresse des ersten zu schreibenden Registerbits
values: (int) zu schreibender Wert (0,1)

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweis: siehe Beispiele: ---

IEC-102-Zähler bezogene Funktionen:

- **Funktion:** **mtx.modbusSaveWord(idRegister, registerValue)**

Beschreibung: Schreibt einen Wert vom Typ word in den Anwenderspeicherbereich

Parameter: idRegister: (int) Registeradresse (10000 ... 19999)

registerValue: (int) Registerwert (0 ... 65535)

Antwort: boolean: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweise: siehe Beispiele: —

- **Funktion: `mtx.modbusSaveDWord(idRegister, registerValue)`**

Beschreibung: Schreibt einen double word Wert in den Anwenderspeicherbereich

Parameter: idRegister: (int) Registeradresse (10000 ... 19999)

registerValue: (long) Registerwert (0 ... 4294967295)

Antwort: boolesch: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweise: siehe Beispiele: 49

- **Funktion: `mtx.modbusReadWord(idRegister)`**

Beschreibung: Liest einen Wert vom Typ word aus dem Anwenderspeicherbereich

Parameter: idRegister: (int) Registeradresse (10000 ... 19999)

Antwort: int: gelesenen Registerwert (0 ... 65535)

-1: Fehler

Hinweise: siehe Beispiele: —

- **Funktion: `mtx.modbusReadDWord(idRegister)`**

Beschreibung: Liest einen Wert double word aus dem Anwenderspeicherbereich

Parameter: idRegister: (int) Registeradresse (10000 ... 19999)

Antwort: long: gelesenen Registerwert (0 ... 4294967295)

-1: Fehler

Hinweise: siehe Beispiele: —

- **Funktion: `mtx.iec102AddMeter(idMeter,linkAddress,measAddress,password)`**

Beschreibung: Fügt dem Zählermanager einen Zähler hinzu. Maximal 100.

Parameter: idMeter (String) Kennung des Zählers

linkAddress (int) Link-Adresse des Zählers

measAddress (int) Messstellenadresse des Zählers

password (long) Passwort des Zählers

Antwort: boolean true: Zähler wurde korrekt hinzugefügt.

false: Fehler

Hinweise: siehe Beispiele: 32 47 48 49

- **Funktion:** **mtx.iec102DeleteAllMeters()**

Beschreibung: Entfernt alle Zähler aus dem Zählermanager.

Parameter:

Antwort: boolean true: Zähler wurden korrekt entfernt.
 false: Fehler

Hinweise: siehe Beispiele: 32 47 48 49

- **Funktion:** **mtx.iec102GetAllMeters()**

Beschreibung: Gibt eine Liste aller im Zählermanager gespeicherten Zähler zurück.

Parameter:

Antwort: ArrayList [] Liste aller Zählerkennungen

Hinweise: siehe Beispiele: 48, 49

- **Funktion:** **mtx.iec102GetPresence()**

Beschreibung: Prüft das Vorhandensein eines Zählers

Parameter: idMeter(String) Zählerkennung

Antwort: int -2: noch nicht initialisiert
 -1: Bus beschäftigt mit Auslesen
 0: Zähler erkannt
 >0: Fehler

Hinweise: siehe Beispiele: 47

-

- (String) Zählerkennung

- liest die Momentwerte des Zählers (String) Zählerkennung

JSON mit den vom Zähler gelesenen Daten Funktion: mtx.iec102SetFiscalClose(idMeter, hourIni, minutelIni, dayIni, monthIni, yearIni, hourEnd, minuteEnd, dayEnd, monthEnd, yearEnd)

Beschreibung: führt den Befehl zum Lesen der Steuerabschlüsse aus

Parameter: idMeter(String) Kennung des Zählers
 hourIni (int) Anfangsstunde (0 ... 23)

minuteIni (int) Anfangsminute (0 ... 59)
 dayIni (int) Anfangstag (1 ... 31)
 monthIni (int) Anfangsmonat (1 ... 12) yearIni (int) Anfangsjahr (22 .. 99)
 hourEnd (int) Endstunde (0 ... 23)
 minuteEnd (int) Endminute (0 ... 59)
 dayEnd (int) Endtag (1 ... 31)
 monthEnd (int) Endmonat (1 ... 12)
 yearEnd (int) Endjahr (22 ... 99)

Antwort: boolean: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweise: siehe Beispiele: ---

- Funktion: `mtx.iec102GetFiscalClose(idMeter)`

Beschreibung: Liest die Abschlusswerte des Zählers

Parameter: `idMeter (String)` Kennung des Zählers

Antwort: String JSON mit den vom Zähler gelesenen Daten
 „ ERROR

Hinweise: siehe Beispiele: ---

- Funktion: `mtx.iec102SetIntegratedTotal(idMeter, hourIni, minuteIni, dayIni, monthIni, monthIni, yearIni, hourEnd, minuteEnd, dayEnd, monthEnd, yearEnd, mode, period)`

Beschreibung: führt den Befehl zum Auslesen der integrierten Summen (Lastganglinie) aus

Parameter: `idMeter(String)` Kennung des Zählers

hourIni (int) Anfangsstunde (0 ... 23)
 minuteIni (int) Anfangsminute (0 ... 59)
 dayIni (int) Anfangstag (1 ... 31)
 monthIni (int) Anfangsmonat (1 ... 12)
 yearIni (int) Anfangsjahr (22 ... 99)
 hourEnd (int) Endstunde (0 .. 23)
 minuteEnd (int) letzte Minute (0 ... 59)
 dayEnd (int) letzter Tag (1 ... 31)
 monthEnd (int) letzter Monat (1 ... 12)
 yearEnd (int) letztes Jahr (22 ... 99)
 period (int) 0 = stündlich, 1 = viertelstündlich

absolut, 1 = inkrementell
 mode (int) 0 =

Antwort: boolean: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweise: siehe Beispiele: 52

- Funktion: `mtx.iec102GetIntegratedTotal(idMeter)`

Beschreibung: Liest die integrierten Gesamtwerte (Lastkurve) aus dem Zähler

Parameter: `idMeter(String)` Kennung des Zählers

Antwort: String JSON mit den vom Zähler gelesenen Daten

„ ERROR

Hinweise: siehe Beispiele: 52

GPS-bezogene Funktionen:

- **Funktion:** `mtx.gpsGetData()`

Beschreibung: Gibt die aktuelle GPS-Position des TITAN-basierten Geräts zurück.

Parameter: keine

Antwort: String JSON mit GPS-Daten

„ FEHLER (wenn keine NMEA-Frames erkannt werden)

Hinweis: siehe Beispiele: 33

LOGGER-bezogene Funktionen:

- **Funktion:** `mtx.loggerWrite(Daten)`

Beschreibung: Schreibt die Daten in den internen Logger des TITAN-basierten Geräts

Parameter: Daten: (String) Daten, die im Logger gespeichert werden sollen

Antwort: boolean true = erfolgreiche Operation

false = Fehler (z. B. Datenlänge größer als
die Logger-Datensatzgröße).

Hinweis: siehe Beispiele: 26

Funktionen im Zusammenhang mit FILES:

- **Funktion: `mtx.fileWrite(index, data, append)`**

Beschreibung: Schreibt Daten in eine Datei innerhalb des TITAN-basierten Geräts

Parameter: Index: (int) Datei-Index (0 ... 9)
data: (String) Daten, die in die Datei geschrieben werden sollen
Append: (boolean) true=Fügt Text zur bestehenden Datei hinzu
false=Löschen der Datei und Speichern des Textes

Antwort: boolean true = erfolgreiche Operation
false = Fehler (z.B. Datenlänge der Datei größer als 100 KB).

Hinweis: siehe Beispiele: 27, 28 30

- **Funktion: `mtx.fileRead(index)`**

Beschreibung: Liest Daten aus einer TITAN-basierten Gerätedatei

Parameter: Index: (int) Datei-Index (0 ... 9)

Antwort: In der Datei enthaltene String-Daten

Hinweis: siehe Beispiele: 27, 29

- **Funktion: `mtx.fileSize(index)`**

Beschreibung: Gibt die Datenlänge einer Datei zurück

Parameter: Index: (int) Datei-Index (0 ... 9)

Antwort: Lange Dateigröße (in Bytes)

Hinweis: siehe Beispiele: 28, 30

- **Funktion: `mtx.fileFtpDownload(tls, Index, Server, Port, Benutzernamen, Pass, Remote-Datei, Timeout, AddExtension)`**

Beschreibung: Empfangen einer TITAN-Datendatei von einem Remote-Server über FTP

Parameter: tls: (int) 0=FTP, 1=FTPS
Index: (int) Index der Datei (0 ... 9), in der die Daten gespeichert werden sollen
Server: (String) IP oder DNS des Remote-FTP-Servers
Anschluss: (int) 0 ... 65535
Benutzernamen: (String) Benutzernamen des FTP-Servers

Benutzername: (String) Benutzername des FTP-Servers
 Pass: (String) Passwort des FTP-Servers
 currentFileName (String) Aktueller Name der Remote-Datei
 newFileName (String) Neuer Name der Remote-Datei
 timeout: (int) Timeout-Sekunden bis zum Abschluss des Vorgangs

Antwort: boolean true = erfolgreiche Operation
 false = Fehler

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.scriptFtpDownload(tls, Server, Port, Benutzername, Pass, remoteFile, Timeout, AddExtension)`**

Beschreibung: Download der Scriptdatei von einem FTP-Server

Parameter: tls: (int) 0=FTP, 1=FTPS
 Server: (String) IP oder DNS des Remote-FTP-Servers
 Anschluss: (int) 0 ... 65535
 Benutzername: (String) Benutzername des FTP-Servers
 Pass: (String) Passwort des FTP-Servers
 RemoteFile: (String) Remote-Script, das heruntergeladen werden soll
 timeout: (int) Timeout-Sekunden bis zum Abschluss des Downloads
 AddExtension: (String) Beim Herunterladen der Datei wird diese Erweiterung hinzugefügt

Antwort: boolean true = erfolgreiche Operation
 false = Fehler

Hinweis: siehe Beispiele: 31

MODEM-bezogene Funktionen:

- **Funktion: `mtx.imeiCheck(imei, Nachricht)`**

Beschreibung: Prüft, ob die als Parameter übergebene IMEI korrekt ist

Parameter: imei: (String) zu prüfende Imei
 message: (String) Nachricht, die bei einem Fehler zurückgegeben wird

Antwort: nichtig
Hinweis: siehe Beispiele: 25

- **Funktion: `mtx.imeiGet()`**

Beschreibung: Gibt die IMEI des internen Modems des TITAN-basierten Geräts zurück

Parameter: keine

Antwort: String Die Imei des internen Modems des TITAN-basierten Geräts

Hinweis: siehe Beispiele: 30

OTAP-bezogene Funktionen:

Funktion: `mtx.otapFTPConfig(tls, Server, Port, Benutzer, Pass, remoteConfigFile, secTimeout, addExtension);`

Beschreibung: Führt einen Downloadbefehl zur Remote-Konfiguration über FTP/FTPS aus.

Wenn die Konfiguration korrekt heruntergeladen wurde, ist es möglich, die Remote-Datei umzubenennen (damit sie nicht erneut heruntergeladen wird) und die Konfiguration zu installieren:

Parameter:

- `tls:` (int) 0=kein TLS, 1= ja TLS
- `Server:` (String) FTP-Server
- `Anschluss:` (int) FTP-Anschluss
- `Benutzer:` (String) FTP-Benutzername
- `Pass:` (String) FTP-Passwort
- `remoteConfigFile:` (String) Remote-Datei (z. B. path1/path2/file)
- `sectimeout:` (int) Sekunden des Timeouts
- `AddExtension:` (String) Beim Herunterladen wird diese Erweiterung an die Remote-Datei angehängt (damit sie nicht erneut heruntergeladen wird)

Antwort: boolean true=Prozess gestartet , false: Prozess nicht gestartet

Hinweis: siehe Beispiele: 37

- **Funktion: `mtx.otapFTPLastStatus()`**

Beschreibung: Gibt den aktuellen Status eines OTAP-Prozesses zurück

Parameter:

Antwort: int 0=keiner, 1=läuft, 2=OK, 3=FEHLER

Hinweis: siehe Beispiele: 37

WATCHDOG-bezogene Funktionen:

- **Funktion: `mtx.watchdogSet(mode, timeout)`**

Beschreibung: Initialisiert den Watchdog

Parameter: int mode: (int) 0=Modus-Reset
timeout: (int) Sekunden bis zum Reset, wenn keine Aktualisierung erfolgt (0, 30 ... 100000). 0=Deaktiviert.

Antwort: boolean true=OK, false: ERROR

Hinweis: siehe Beispiele: 20

- **Funktion: `mtx.watchdogKick()`**

Beschreibung: Aktualisiert den Watchdog, damit er das Modem nicht neu startet

Parameter: keine

Antwort: boolean true=OK, false: ERROR

Hinweis: siehe Beispiele: 20

Zeitbezogene Funktionen:

- **Funktion: `mtx.pause(mseconds)`**

Beschreibung: Erzeugt eine Pause mit der Dauer der konfigurierten Millisekunden

Parameter: mseconds (long) Millisekunden Wartezeit

Antwort: boolean true = erfolgreiche Operation
 false = Fehler

Hinweis: siehe Beispiele: 1, 2, 3, 4, 5, ... , 35

- **Funktion: `mtx.timestamp()`**

Beschreibung: Gibt das Datum und die Uhrzeit des TITAN-basierten Geräts zurück

Parameter: keine

Antwort: String Datum und Uhrzeit des TITAN-basierten Geräts

Hinweis: siehe Beispiele: 28, 30

- **Funktion: `mtx.timeGetYear()`**

Beschreibung: Gibt das Jahr zurück

Parameter: keine

Antwort: Int aktuelles Jahr mit vier Ziffern

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.timeGetMonth()`**

Beschreibung: Gibt den Monat zurück

Parameter: keine

Antwort: Int aktueller Monat (1=Januar ... 12=Dezember)

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.timeGetDay()`**

Beschreibung: Gibt den Tag zurück

Parameter: keine

Antwort: Int aktueller Tag (1 ... 31)

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.timeGetHour()`**

Beschreibung: Gibt die Uhrzeit zurück

Parameter: keine

Antwort: Int aktuelle Uhrzeit (0 ... 23)

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.timeGetMinute()`**

Beschreibung: Gibt die Minuten zurück

Parameter: keine

Antwort: Int aktuelle Minute (0 ... 59)

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.timeGetSecond()`**

Beschreibung: Gibt die Sekunden zurück

Parameter: keine

Antwort: Int aktuelle Sekunde (0 ... 59)

Hinweis: siehe Beispiele: ---

Funktionen im Zusammenhang mit Sockets:

- **Funktion: `mtx.socketOpen (idSocket,ssl,ip,port)`**

Beschreibung: Öffnen eines TCP-Client-Sockets gegen eine IP/DNS

Parameter: idSocket (int) Socket-Kennung (0 ... 9)
ssl (int) 0=no, 1=yes
idSocket (String) IP- oder DNS-Adresse des Remoteservers
TCP-Port (int) TCP-Port des Remoteservers (0 ... 65535)

Antwort: boolean true = erfolgreiche Operation
false = Fehler

Hinweise: siehe Beispiele: 45, 46

- **Funktion: `mtx.socketClose (idSocket)`**

Beschreibung: Schließen eines TCP-Client Socket

Parameter: idSocket (int) Socket-Kennung (0 ... 9)

Antwort: boolean true = erfolgreiche Operation

false = Fehler

Hinweise: siehe Beispiele: 45, 46

- **Funktion: mtX.socketIsOpen(idSocket)**

Beschreibung: Prüft, ob ein TCP-Client-Socket eine bestehende Verbindung hat

Parameter: idSocket (int) Socket-Kennung (0 ... 9)

Antwort: boolean true = ja, es besteht eine bestehende Verbindung
false = nein, keine Verbindung aufgebaut.

Hinweise: siehe Beispiele: 45, 46

- **Funktion: mtX.socketSend(idSocket, data[])**

Beschreibung: Sendet Daten über einen TCP(IP)-Socket

Parameter: idSocket (int) Socket-Kennung (0 ... 9)
values[]: (byte[]) Array mit zu sendenden Bytes

Antwort: boolean: (true=Betrieb OK, false=Betrieb FEHLER)

Hinweise: siehe Beispiele: 45, 46

- **Funktion: mtX.socketIsData(idSocket)**

Beschreibung: Prüft, ob auf einem TCP-Client-Socket Daten zum Lesen anstehen

Parameter: idSocket (int) Socket-Kennung (0 ... 9)

Antwort: boolean true = es stehen Daten an
false = es stehen keine Daten an

Hinweise: siehe Beispiele: 45, 46

- **Funktion: mtX.socketRead(idSocket)**

Beschreibung: Liest die auf einem TCP-Client Socket verfügbaren Bytes

Parameter: idSocket (int) Socket-Kennung (0 ... 9)

Antwort: byte[] Array von Bytes mit den empfangenen Daten
null: Fehler

Hinweise: siehe Beispiele: 45, 46

- **Funktion: `mtx.mobileGetIP()`**

Beschreibung: Gibt die mit dem Mobile WAN verbundene IP-Adresse zurück

Parameter: keine

Antwort: String „“ = Keine, „x.x.x.x“

Hinweis: siehe Beispiele: ---

- **Funktion: `mtx.powerStatus()`**

Beschreibung: Gibt an, ob der Router über eine externe Stromversorgung verfügt. Geräte-Tool mit interner Batterie oder Supercap.

Parameter: keine

Antwort: Int 0=Nein, 1=Ja, -1=Fehler

Hinweis: siehe Beispiele: 6

- **Funktion: `mtx.println(Daten)`**

Beschreibung: Sendet Textdaten an die Debug-Konsole

Parameter: data (String) Textdaten, die von der Konsole geschrieben werden sollen

Antwort: nichtig

Hinweis: siehe Beispiele: 1, 2, 3, 4, 5, ... , 35

- **Funktion: `mtx.ping(ip, timeout)`**

Beschreibung: Erzeugt einen Ping an eine IP oder Remote-DNS

Parameter: ip (String) IP oder Remote-DNS zur Durchführung des PING

Timeout (int) Timeout in Millisekunden

Antwort: boolean true = Ping erfolgreich

false = Ping-Fehler

Hinweis: siehe Beispiele: 17

- **Funktion: `mtx.base64Encode(Daten)`**

Beschreibung: kodiert ein Byte-Array in base64

Parameter: data (byte[]) zu kodierender Byte-Array

Antwort: String in base64 kodierte Daten
„“ = Fehler

Hinweis: siehe Beispiele: 26

- **Funktion:** **mtx.stringToByteArray(data)**

Beschreibung: konvertiert einen String in ein Byte-Array

Parameter: data (String) Daten, die in ein Byte-Array konvertiert werden sollen

Antwort: byte[] byte array
null = error

Hinweise: siehe Beispiele: 51

- **Funktion:** **mtx.byteArrayToString (data, init, length)**

Beschreibung: wandelt ein Array von Bytes in einen String um

Parameter: data (byte[]) Array von Bytes
init (int) Position
length (int) Anzahl der zu konvertierenden Bytes

Antwort: String String mit Konvertierung
„“ = Fehler

Hinweise: siehe Beispiele: —

Liste der Beispiele.

In der WEB-Umgebung der Router-Konfiguration finden Sie im Abschnitt „Other à TITAN Scripts“ eine Reihe von Script-Beispielen. Nachfolgend finden Sie eine kurze Beschreibung zu jedem Einzelnen.

Beispiel 1 - Hallo Welt

Einfaches Beispiel für das Schreiben von Debug-Ablaufverfolgungen für die Standardausgabe.

Beispiel 2 - AT-Befehlsanforderung

Beispiel für das Senden von AT-Befehlen an das interne Modem des Geräts (um den Netzempfang zu erreichen, die Identifizierung der verwendeten Telefonfunkzelle, ...)

Beispiel 3 - Senden einer SMS bei GPIO-Änderung

Beispiel für das Senden einer SMS-Nachricht, wenn eine Änderung an einem digitalen Eingang des Geräts erkannt wird.

Beispiel 4 - Senden einer MQTT-Nachricht an den Broker

Beispiel für das Senden einer MQTT-Nachricht an den Broker, mit dem das Gerät verbunden ist.

Beispiel 5. - Senden von SNMP TRAP

Beispiel für das Senden eines SNMP-TRAP.

Beispiel 6 - Senden einer E-MAIL bei Stromausfall

Beispiel für den Versand einer E-Mail. In diesem Beispiel wird die E-Mail gesendet, wenn ein Stromausfall festgestellt wird. Beispiel gilt nur für Router-Modelle mit internem Akku oder Supercap.

Beispiel 7 - Lesen des Modbus RTU Wortregisters

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD aus TITAN-Scripts.

Beispiel 7b: Lesen des Modbus TCP Wortregisters

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD aus TITAN-Scripts.

Beispiel 8 - Lesen des Modbus RTU Wortregisters und Senden über MQTT

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD und das Senden der gelesenen Daten an ein MQTT-Topic.

Beispiel 9. - Lesen des Modbus RTU Wortregisters und Senden von TRAP

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD und das Senden eines SNMP-TRAP auf der Grundlage des gelesenen Registerwerts.

Beispiel 10. - Lesen des Modbus RTU Wortregisters und Senden von SMS

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD und Senden einer SMS in Abhängigkeit vom Wert des gelesenen Registers.

Beispiel 11. - Lesen des Modbus RTU Wortregisters und Senden von EMAIL

Beispiel für das Lesen eines Modbus-Registers vom Typ WORD und Senden einer EMAIL in Abhängigkeit vom Wert des gelesenen Registers.

Beispiel 12 - Schreiben von Modbus-RTU-Wortregistern

Beispiel für das Schreiben in ein Modbus-Register vom Typ WORD.

Beispiel 13 - Lesen des Modbus-RTU-Bitregisters

Beispiel für das Lesen eines Modbus-Registers vom Typ Bit.

Beispiel 14 - Schreiben des Modbus-RTU-Bitregisters

Beispiel für das Schreiben in ein Modbus-Register vom Typ Bit.

Beispiel 14b: Lesen von Modbus-RTU-Wortregistern, Speichern von Daten im LOGGER für zeitgesteuertes Senden

Beispiel für das Lesen von Modbus-RTU-Registern von einem externen Gerät über die serielle RS485-Schnittstelle, das Erstellen eines JSON mit einer benutzerdefinierten Datenstruktur und das Speichern dieses JSON im Titan-Datenlogger, um es über die konfigurierte Methode (MQTT, HTTP, FTP) zu senden.

Beispiel 15 - Lesen aller digitalen Eingänge

Beispiel für das Lesen aller IOs (digitale Eingänge und/oder Ausgänge) des Geräts. Gilt nur für Geräte mit digitalen Ein- und/oder Ausgängen.

Beispiel 16. - Schreiben eines digitalen Ausgangs

Beispiel für die Änderung des Zustands eines digitalen Ausgangs am Gerät. Gilt nur für Geräte mit digitalen Ausgängen.

Beispiel 17 - Ping ip und Senden einer SMS bei Problemen mit dem Ping

Beispiel für die Durchführung eines PING an einer Vorrichtung, die an das Gerät angeschlossen ist, und das Senden einer SMS bei Problemen mit dem PING, z. B. um eine Fehlfunktion eines angeschlossenen Geräts zu erkennen.

Beispiel 18 - Senden eines SMS-Alarms, wenn die Backup-SIM 2 verwendet wird

Beispiel, das eine Warn-SMS sendet, wenn die zweite SIM-Karte in Betrieb genommen wird. Gilt nur für DUAL SIM-Geräte.

Beispiel 19 - Lesen und Schreiben von Daten über den SERIAL PORT

Beispiel für die Durchführung von Lese- und Schreibvorgängen an einer seriellen Schnittstelle. Beispiel gilt nur für Geräte mit einer oder mehreren seriellen RS232- und/oder RS485-Schnittstellen

Beispiel 20 - Verwendung des WATCHDOG

Beispiel für die Verwendung des Watchdogs der TITAN Scripts. Neustart im Falle einer Fehlfunktion des Scripts.

Beispiel 21 - Verwendung von LEDs für kundenspezifische Anzeigen

Beispiel für die kundenspezifische Verwendung der LEDs, wobei das Ein- und Ausschalten über ein Script gesteuert wird.

Beispiel 22 - TITAN als MODBUS-Konzentrator speichert Daten im internen Speicher

Beispiel für die Verwendung des Geräts als Modbus-Konzentrator mit Speicherung der gelesenen Daten im internen Speicher. So ist es zum Beispiel möglich, verschiedene Modbus-RTU-Sensoren autonom auszulesen und die ausgelesenen Register an verschiedenen Stellen im Speicher des Geräts zu speichern und von einem Remote-Standort aus über Modbus TCP die Daten der im Gerät gespeicherten Register zu lesen.

Beispiel 23. - Austausch von Daten über AT-Befehle, die per SMS, MQTT, Telnet, SSH, HTTP ... gesendet werden

Beispiel für den Datenaustausch über AT-Befehle von Scripts, die per SMS, MQTT, Telnet usw. gesendet werden. Das heißt, Sie können einen AT-Befehl über SMS, MQTT, Telnet usw. an das Gerät senden, und mit dem von Ihnen programmierten Script diese Daten empfangen und entsprechend handeln.

Beispiel 24 - Verschlüsselung des Script-Codes

Beispiel für die Verschlüsselung des Codes eines Scripts. Wenn Sie zum Beispiel einem Dritten einen Computer mit einem vorprogrammierten Script zur Verfügung stellen und den Quellcode nicht zeigen wollen, können Sie das Script wie in diesem Beispiel verschlüsseln.

Beispiel 25: Verschlüsselung des Script-Codes, um eine Raubkopie des Scripts zu verhindern

Beispiel für die Verschlüsselung des Codes eines Scripts. Wenn Sie beispielsweise einem Dritten einen Computer mit einem vorprogrammierten Script zur Verfügung stellen und den Quellcode nicht zeigen wollen, damit er nicht kopiert oder gehackt werden kann, können Sie das Script wie in diesem Beispiel verschlüsseln.

Beispiel 26. - Speichern von DATEN im internen TITAN-LOGGER.

Beispiel für die Speicherung von Daten im internen Speicher des Geräts. Auf diese Weise werden die automatischen Mechanismen des Geräts mit seinem Speicher genutzt, um die Daten an einen MQTT-Broker, HTTP-Server usw. zu senden.

Beispiel 27 - Verwendung von Benutzer-FILES zum Lesen, Schreiben und Anhängen von Daten.

Beispiel für die Erstellung von Benutzerdateien zum Schreiben, Lesen und Anhängen von Daten.

Beispiel 28 - Upload von Benutzer-DATEIEN über FTP

Beispiel für das Senden von Benutzerdateien über FTP.

Beispiel 29 - Download von Benutzer-DATEIEN über FTP

Beispiel für den Empfang von Benutzerdateien über FTP.

Beispiel 30 - Modbus RTU lesen, Daten in DATEI speichern und über FTP senden

Beispiel für das Lesen von Modbus-RTU-Daten aus einem Script, das Speichern der Daten in einer Benutzerdatei und das Senden der Datei über FTP.

Beispiel 31 - Herunterladen und Installieren einer neuen Version von SCRIPT vom FTP-Server

Beispiel für die Remote-Aktualisierung eines Benutzerscripts.

Beispiel 32 - Lesen von Augenblickswerten eines IEC-60870-5-102 Zählers

Beispiel für das Auslesen der Augenblickswerte eines Energiezählers mit IEC-60870-5-102-Protokoll aus einem Script.

Beispiel 33 - Lesen von GPS-Daten aus TITAN

Beispiel für das Abrufen der GPS-Position über ein Script. Nur gültig für Geräte mit GPS.

Beispiel 34 - Lesen der digitalen ZÄHLER

Beispiel für das Ablesen des Wertes der Impulszähler. Gilt nur für Geräte mit digitalen Eingängen.

Beispiel 35 - Abonnieren eines MQTT-Topic. Lesen und Senden von Byte-Array-Daten

Beispiel für das Abonnieren eines MQTT-Topics zum Empfang eines Daten-Arrays.

Beispiel 36 - IO Line Passing durch MQTT. Senden des digitalen Eingangsstatus an den digitalen Remote-Ausgang.

Beispiel für die Verwendung von 2 TITAN-basierten Geräten mit digitalen Ein- und Ausgängen. Wenn sich der Status eines digitalen EINGANGS eines Geräts ändert, muss sich der Status eines digitalen AUSGANGS im Remote-Gerät ändern. Das heißt, es wird gezeigt, wie ein digitaler Eingang auf einen

digitalen Remote-Ausgang repliziert wird.

Beispiel 37.- Überprüfen und Herunterladen einer Remote-Router-Konfiguration über FTPS.

Dieses Beispiel zeigt, wie es möglich ist, ein TITAN-basiertes Gerät dazu zu bringen, eine Sicherungsdatei der Konfiguration über FTPS herunterzuladen. Der Router lädt die Datei herunter, benennt sie auf dem Remote-Server um (damit sie nicht erneut heruntergeladen werden muss) und installiert die heruntergeladene Konfiguration.

Beispiel 38 - Download einer Remote-Datei mit AT über FTPS und deren Ausführung

Dieses Beispiel zeigt, wie es möglich ist, ein TITAN-basiertes Gerät dazu zu bringen, eine Datei mit AT-Befehlen über FTPS herunterzuladen. Sobald die Datei heruntergeladen wurde, führt das TITAN-basierte Gerät die aus der Datei gelesenen AT-Befehle aus.

Beispiel 39 - Senden von Daten per HTTP GET und HTTP POST mit benutzerdefinierten Kopfzeilen

Anschauungsbeispiel für HTTP/HTTPS-Anfragen mit GET- und POST-Methoden, die auch die Verwendung benutzerdefinierter Kopfzeilen ermöglichen.

Beispiel 40 - Lesen aller empfangenen SMS aus SCRIPT

Beispiel für das Auslesen aller im TITAN-Gerät empfangenen SMS aus einem Script. Das Script ermöglicht es, nach dem Empfang der SMS die Telefonnummer des SMS-Absenders und die zugehörige Textnachricht abzurufen.

Beispiel 41.- TELEGRAM-Nachricht senden, wenn sich ein GPIO ändert.

Beispiel für das Senden einer Textnachricht an einen Gruppenchat der Telegram-Messaging-Anwendung, wenn sich ein digitaler Eingang des TITAN-basierten Geräts ändert. Weitere Informationen finden Sie in den Anwendungshinweisen.

Beispiel 42.- TELEGRAM-Nachricht senden, wenn sich ein MODBUS-Register ändert.

Beispiel für das Senden einer Textnachricht an eine Chat-Gruppe der Telegram-Messaging-Anwendung, wenn sich der Wert eines Modbus-Registers ändert, das vom TITAN-basierten Gerät über Modbus RTU von einem über den RS485-Port angeschlossenen Gerät gelesen wird. Weitere Informationen finden Sie in den Anwendungshinweisen.

Beispiel 43.- CellID lesen und ungefähre Längen- und Breitengrade von Drittanbietern erhalten.

Beispiel für die Ermittlung der Länge und des Breitengrads aus den Informationen, die von der vom Modem verwendeten Telefonfunktelle stammen. Zusätzlich wird eine API eines Drittanbieters verwendet.

Beispiel 44.- Lesen Sie die günstigste Energiestunde von der REE-Website per HTTP REST api ab.

Beispiel für den Download der Stundentarife des regulierten Strommarktes in Spanien von REE (Red Eléctrica de España) über HTTP GET (REST API). Sobald die stündlichen Energiepreistarife heruntergeladen wurden, suchen Sie nach der Stunde mit dem niedrigsten Energiepreis. Der digitale Ausgang des Geräts wird nur während dieser Stunde aktiviert (z.B. um einen elektrischen Warmwasserboiler zu aktivieren), um so viel wie möglich an Stromkosten zu sparen.

Beispiel 45: Lesen und Senden von Daten über einen TCP-Client SOCKET.

Beispiel für das Einrichten eines TCP-Client-Sockets gegen einen Server und für das Senden und Empfangen von Daten über diesen Socket.

Beispiel 46: Lesen und Senden von Daten über einen TSSL/TLS CP-Client SOCKET.

Beispiel für das Einrichten eines TCP-Client-Sockets mit SSL/TLS-Sicherheit gegenüber einem Server und für das Senden und Empfangen von Daten über diesen Socket.

Beispiel 47: Prüfung auf das Vorhandensein eines IEC-60870-5-102-Zählers und Senden einen SMS-Alarm, wenn er nicht erkannt wird

Beispiel für die periodische Überprüfung des Vorhandenseins eines IEC-60870-5-102-Zählers. Im Falle eines Anwesenheitsfehlers sendet es eine Alarm-SMS-Nachricht, um die Situation zu melden.

Beispiel 48 - Lesen von Momentwerten mehrerer IEC-60870-5-102 Zähler und Speichern der Daten im LOGGER

Beispiel für das Auslesen der Augenblickswerte eines Energiezählers mit IEC-60870-5-102-Protokoll aus einem Script. Die Daten werden im internen LOGGER gespeichert, um sie dann über HTTP, MQTT oder FTP an eine WEB-Plattform zu senden

Beispiel 49: Konfiguration von IEC-60870-5-102 zu MODBUS TCP/RTU Gateway

Beispiel für einen IEC-60870-5-102 zu Modbus Konverter. Das Beispiel zeigt, wie die Momentwerte eines Zählers mit IEC-60870-5-102-Protokoll gelesen und im Anwenderspeicherbereich abgelegt werden, so dass sie über Modbus TCP oder Modbus RTU von einem externen Gerät (z. B. einer SPS) gelesen werden können.

Beispiel 50: Kommunikation mit ANDROID-App über MQTT

Beispiel für die Interaktion eines Skripts mit einer vom Benutzer gestalteten Android-App. Bitte beachten Sie unbedingt den Anwendungshinweis 61

Beispiel 51: Weiterleitung aller empfangenen SMS über die serielle Schnittstelle RS232

Beispiel für den Empfang einer SMS-Nachricht von einem Skript und die direkte Weiterleitung des Inhalts

der Nachricht über die serielle RS232-Schnittstelle.

Beispiel 52: Lesen der INTEGRIERTEN Werte von IEC-60870-5-102-Zählern und Speichern der Daten im LOGGER

Beispiel für das Auslesen der Lastkurven (integrierte Werte) eines IEC-60870-5-102-Zählers jeden Tag um 2 Uhr morgens und das Speichern der Daten im LOGGER-Speicher, damit die Daten automatisch wie konfiguriert gesendet werden (MQTT, HTTP, FTP).

JSON-Transformator Funktions-Script

Mit dem Funktions-Script des JSON-Transformators können Sie das Datenformat ändern, bevor Sie es über HTTP, MQTT oder FTP an eine WEB-Plattform senden. Auf diese Weise können Sie das Format der von den TITAN-basierten Geräten gesendeten Daten an das von der Plattform benötigte Format anpassen. In der Anmerkung zur Anwendung ANV6_57- Router-TITAN-Json_Transformer_Script finden Sie alle Einzelheiten zu dieser Funktion.

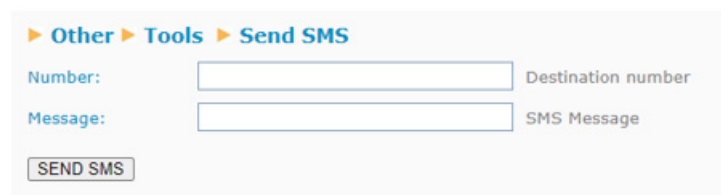
Funktions-Script für MQTT-Themen

Diese Eigenschaft ermöglicht die Ausführung eines Scripts, wenn das TITAN-basierte Gerät Daten zu bestimmten MQTT-Themen empfängt. Auf diese Weise kann es Daten, die von einer MQTT-Webplattform empfangen werden, unabhängig vom Datenformat empfangen und verarbeiten. Vollständige Informationen zu dieser Eigenschaft finden Sie in der Anmerkung zur Anwendung ANV6_58- Router-TITAN-Mqtt_Topic_Function_Script.

4.7.18 Sonstiges > Konnektivitätswerkzeuge

Manchmal ist es nützlich, die Nummer der in das TITAN-basierte Gerät eingelegten SIM-Karte zu kennen oder die Konnektivität mit einer bestimmten IP oder DNS aus Sicht des Geräts zu prüfen oder die Konnektivität mit einem TCP-Anschluss eines externen Servers zu prüfen oder einfach zu wissen, ob der E-Mail-Konfigurationsabschnitt korrekt ist. Dieser Abschnitt enthält eine Reihe von grundlegenden Instrumenten, die all diese Anforderungen erfüllen.

- **Dienstprogramm „SMS senden“.**



Wie der Name schon sagt, ist es mit diesem Dienstprogramm sehr einfach, eine SMS-Nachricht von einem TITAN-basierten Gerät an ein Mobiltelefon zu senden. Es kann nützlich sein, um die Telefonnummer der SIM-Karte schnell zu ermitteln.

- Dienstprogramm „PING senden“.

Dieses Dienstprogramm ermöglicht es, einen PING vom TITAN-basierten Gerät aus zu einer bestimmten IP oder DNS durchzuführen, um die Konnektivität zwischen beiden Einheiten zu überprüfen.

- Dienstprogramm „EMAIL senden“.

Mit diesem Dienstprogramm können Sie die korrekte Konfiguration für den Versand von E-Mails von TITAN-basierten Geräten überprüfen. Dazu muss zunächst der Bereich „Other→Email“ konfiguriert werden.

- Dienstprogramm „TCP-Verbindung prüfen“.

Mit diesem Dienstprogramm können Sie überprüfen, ob ein TCP-Anschluss aus Sicht der TITAN-basierten Geräte für eine Verbindung verfügbar ist. Um diese Konnektivität zu überprüfen, erstellt das Gerät einen TCP-Client-Socket, der versucht, eine Verbindung mit der angegebenen IP/DNS und dem TCP-Anschluss herzustellen. Gelingt es, die Verbindung herzustellen, wird das Ergebnis als erfolgreich angezeigt. Optional ist es möglich, ein zusätzliches ASCII-Datenfeld hinzuzufügen, das das TITAN-basierte Gerät nach dem Verbindungsaufbau über den Socket sendet.

Im unteren Teil des Bildschirms wird ein Abschnitt „Ergebnisse“ angezeigt, in dem die Ergebnisse der oben genannten Tools erscheinen. Das folgende Beispiel zeigt das Ergebnis eines Verbindungsversuchs zur Adresse www.google.com und TCP-Anschluss 80.

► Other ► Tools ► Check TCP Connection

IP or DNS: IP or DNS of remote host

TCP port: TCP port (1 ... 65535)

ASCII Data: (Optional) Send ascii test data if connection is successful

► Other ► Tools ► Results

SUCCESSFUL CONNECTION. Connection with IP or DNS (www.google.com:80) can be established

4.7.19 Sonstiges >> Digitale E/A

Viele Modelle von Modems und TITAN-basierten Geräten haben digitale Ein- und/oder Ausgänge. In diesem Abschnitt können sie konfiguriert werden.

 **webdyn** powered by **TITAN**
flexitron group

★ **Mobile**

- ◉ Status
- ◉ Basic Settings
- ◉ Keep Online

★ **Ethernet**

- ◉ Basic Settings

★ **Wifi**

- ◉ Basic Settings
- ◉ DHCP Server

★ **Firewall**

- ◉ NAT
- ◉ Authorized IPs

★ **Serial Settings**

- ◉ Serial Port1-RS232
- ◉ Serial Port2-RS485
- ◉ SSL Certificates

★ **External Devices**

- ◉ Logger configuration
- ◉ ModBus Devices
- ◉ Generic Serial Device
- ◉ Temperature Sensor
- ◉ IEC102 Meter
- ◉ W-MBus
- ◉ GPS Receiver

► Other ► Digital I/O

Enable: ☒ Enable digital inputs and outputs

Period: Period (minutes) for saving IO status and counters in Logger. Please, [configure logger](#) before using

► Other ► Digital I/O ► Digital Inputs

Digital Input IO0: Special functions of Digital Input IO-0

► Other ► Digital I/O ► Digital Outputs

Digital Output IO1: Special functions of Digital Output IO-1

Remember: you can also use I/O with "[Titan Scripts](#)" for special functionality

- **Aktiviert.** Aktiviert den TITAN-basierten Eingangs-/Ausgangsdienst des Geräts. Wenn Sie ihn nutzen wollen, müssen Sie ihn aktivieren.
- **Zeitraum.** Erlaubt die Einstellung einer Zeitspanne (in Minuten), in der die digitalen Ein- und Ausgänge sowie die Impulszähler gelesen werden, und den Messwert im internen Datenlogger des TITAN-basierten Geräts zu speichern, um ihn anschließend über HTTP/S oder MQTT/S an eine Plattform zu senden.

Nach der Aktivierung der Option und dem Neustart des Geräts können Sie das Verhalten der digitalen Eingänge und der digitalen Ausgänge konfigurieren, indem Sie die entsprechende Taste „CONFIG“ drücken. Denken Sie daran, dass die digitalen Ein- und Ausgänge auch über das TITAN-Script verwaltet werden können.

Konfiguration der digitalen Eingänge.

Der Konfigurationsbildschirm für die digitalen Eingänge sieht wie folgt aus.

The screenshot shows the webdyn configuration interface. At the top, the logo 'webdyn' is displayed with 'powered by TITAN' and 'Flexitron group' below it. On the left, a sidebar menu lists various configuration categories: Mobile (Status, Basic Settings, Keep Online), Ethernet (Basic Settings), Wifi (Basic Settings, DHCP Server), Firewall (NAT, Authorized IPs), Serial Settings (Serial Port1-RS232, Serial Port2-RS485, SSL Certificates), External Devices (Logger configuration, ModBus Devices, Generic Serial Device, Temperature Sensor, IEC102 Meter, W-MBus, GPS Receiver), and Other (AT Command). The main content area is titled 'Other > Digital I/O > Digital Input IO-0'. It contains a 'Digital input mode:' dropdown menu set to 'Normal' with a description 'Select the mode of digital input IO-0'. Below this, there is a section for 'Alarm' configuration. It includes an 'SMS:' checkbox labeled 'enabled' with the note 'When alarm, send SMS message'. There are three input fields for 'Phone numbers:', 'Text SMS Alarm On', and 'Text SMS Alarm Off', with corresponding descriptions: 'Phone numbers separated with ;', 'SMS text when alarm is activated', and 'SMS text when alarm is deactivated'. A 'Logger:' checkbox is also present with the note 'Check if logger must be used for alarms. Please, configure logger before using this option'. A 'SAVE CONFIG' button is located below the logger checkbox. At the bottom, there is a 'Status' section with a 'READ INPUT' button and a display showing '0', with the instruction 'Click for read the status of digital input IO-0'.

- **Digitaler Eingangsmodus:** Gibt das Verhalten des digitalen Eingangs an. Sie können „normal“ wählen, wenn Sie den Eingang nicht für Alarime verwenden wollen, oder Sie wählen „Alarm (Pin 0 à 1)“ oder „Alarm (Pin 1 à 0)“, wenn Sie einen Alarm konfigurieren wollen, der ausgelöst wird, wenn

der logische Wert des digitalen Eingangs von 0 auf 1 oder umgekehrt wechselt.

- **SMS enabled:** Muss aktiviert werden, wenn das TITAN-basierte Gerät bei Aktivierung oder Deaktivierung eines Alarms eine SMS-Nachricht senden soll.
- **Phone numbers:** Geben Sie hier die Telefonnummern ein, an die SMS-Nachrichten gesendet werden sollen. Wenn sie an mehrere Telefonnummern gesendet werden sollen, können Sie mehrere Telefonnummern durch „;“ getrennt angeben.
- **Test-SMS-Alarm Ein:** Text der SMS-Nachricht, die bei Auslösung des Alarms gesendet werden soll.
- **Test-SMS-Alarm Aus:** Text der SMS-Nachricht, die bei Deaktivierung des Alarms gesendet werden soll.
- **Logger aktiviert:** Muss aktiviert werden, wenn das TITAN-basierte Gerät die Änderung des digitalen Eingangs im Logger speichern soll, um sie über HTTP/HTTPS, MQTT/MQTTS oder FTP an eine Plattform zu senden.

Wenn LOGGER aktiviert ist, ist dies das JSON-Objekt, das an den Server gesendet wird.

```
{“IMEI”:”867962046823806”,”TYPE”:”GPIO”,”TS”:”2021-11-03T08:16:00Z”,”ID”:0,”VALUE”:1,”DIR”:”INPUT”,”P”:”ID0001”}
```

Wo:

IMEI: Modem-IMEI

TYPE: Framenart. In diesem Fall „GPIO“

TS: Zeitstempel, wann das Ereignis eingetreten ist

ID: IO-Identifikator (0, 1, ...)

WERT: Logischer Wert des digitalen Eingangs (0, 1)

DIR: Zeigt an, ob der GPIO vom Typ INPUT oder OUTPUT ist

P: ID-Feld im Abschnitt LOGGER eingestellt

Es ist auch möglich, den Wert des Digitaleingangs durch Drücken der Taste „READ INPUT“ in Echtzeit zu lesen.



Konfiguration der digitalen Ausgänge.

Der Konfigurationsbildschirm für die digitalen Ausgänge sieht wie folgt aus



Von diesem Bildschirm aus ist es möglich, den Status eines digitalen Ausgangs zu ändern und den aktuellen Status des Ausgangs abzulesen. Denken Sie daran, dass es auch möglich ist, den Zustand eines digitalen Ausgangs über TITAN-Scripts zu ändern.

4.7.20 Sonstiges > Benutzerdefinierter Skin

TITAN-basierte Geräte ermöglichen es Ihnen, die Kopfzeile der Web-Konfigurationsumgebung sowie den Titel und die Fußzeile der Seite mit Ihren eigenen Logos zu gestalten. Dadurch kann bis zu einem gewissen Grad der Anschein eines maßgeschneiderten Produkts oder einer Eigenmarke erweckt werden.

- Benutzerdefiniertes Bild einstellen: Wählen Sie ein Bild von 922 x 172 Pixel (Typ GIF) für den Kopfbereich.
- Benutzerdefinierte Labels einstellen: Geben Sie den Text ein, der im Titel und in der Fußzeile der Webkonfigurationsumgebung erscheinen soll.



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern.
- Beachten Sie, dass es nicht sinnvoll ist, den Abschnitt „Sonstige > Benutzerrechte“ nicht zu verwenden, wenn Sie das Gerät mit Ihren individuellen Kopfzeilen und Texten so einrichten, dass sie von Dritten gesehen werden können. Verwenden Sie diesen Abschnitt, damit der Benutzer „user“ keinen Zugriff auf den Abschnitt „Other > Custom Skin“ hat.

4.7.21 Sonstiges > Benutzerdefinierte LED

TITAN-basierte Geräte haben mehrere konfigurierbare LEDs. In diesem Abschnitt können Sie ihm das Verhalten geben, das Ihren Bedürfnissen am besten entspricht.

- **Nicht verwendet:** Die LED ist immer ausgeschaltet, wenn sie nicht genutzt wird.
- **IP:** Die LED leuchtet, wenn das Gerät eine IP-Adresse hat (WAN 4G/3G/2G)
- **RSSI:** Die LED blinkt, wenn der Empfang schlecht ist, und leuchtet, ohne zu blinken, wenn der Empfang gut ist. Aus bedeutet kritischer oder kein Empfang.
- **SIM-Fehler:** Die LED leuchtet auf, wenn ein Ausfall der SIM-Karte erkannt wird
- **TITAN-Scripts:** Die LED wird aus dem Bereich TITAN-Scripts des Geräts verwendet



Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.22 Other > SYSLOG

Von diesem Bereich aus ist es möglich, auf ein internes Protokoll des TITAN-basierten Geräts zuzugreifen, in dem der Status des Geräts selbst (Abdeckung, Registrierung im Netz, Betreiber, Ergebnis des Sendens an Server...), die von den Benutzern durchgeführten Aktionen usw. angezeigt werden.



Klicken Sie auf die Schaltfläche „**SYSLOG CONFIG**“, um den Bereich SYSLOG-Konfiguration aufzurufen. In diesem Konfigurationsbereich können Sie die folgenden Konfigurationen vornehmen.

- **Aktiviert Lokal:** „Deaktiviert“: Verwendet das SYSLOG nicht. „RAM“ (empfohlene Option) soll das SYSLOG im RAM speichern. „FLASH“ (nur bei einigen TITAN-basierten Geräten verfügbar) speichert das SYSLOG im Flash. Nur für die Fehlersuche und nicht für den Dauereinsatz empfohlen, da der FLASH-Speicher bei ständigem Gebrauch übermäßig abgenutzt werden kann.
- **Aktiviert Server 1:** Wenn Sie das Kontrollkästchen aktivieren, wird das SYSLOG über UDP an einen Remote-Server gesendet.
- **Remote-Server 1:** IP oder DNS des Remote-Servers 1, der das SYSLOG empfangen soll
- **Remote-Anschluss 1:** Remote-Server 1 USD-Anschluss
- **Aktiviert Server 2** Wenn Sie das Kontrollkästchen aktivieren, wird das SYSLOG über UDP an einen zweiten Remote-Server gesendet.
- **Remote-Server 2** IP oder DNS des Remote-Servers 2, der das SYSLOG empfangen soll
- **Remote-Anschluss 2:** Remote-Server 2 USD-Anschluss
- **MQTT Topic:** Wenn ein MQTT-Topic angegeben ist, wird das Echtzeit-Syslog an das angegebene MQTT-Topic gesendet. Der Abschnitt Other à MQTT muss konfiguriert werden.
- **Netzwerk-Log:** Wenn Sie dieses Kontrollkästchen aktivieren, wird der Netzwerkstatus

regelmäßig in das SYSLOG aufgenommen.

webdyn powered by TITAN flexitron group

★ Mobile

- Status
- Basic Settings
- Keep Online

★ Ethernet

- Basic Settings

★ Wifi

- Basic Settings
- DHCP Server

★ Firewall

- NAT
- Authorized IPs

★ Serial Settings

- Serial Port1-RS232
- Serial Port2-RS485
- SSL Certificates

★ External Devices

- Logger configuration
- ModBus Devices
- Generic Serial Device
- Temperature Sensor
- IEC102 Meter
- W-MBus
- GPS Receiver

Other > SYSLOG Config

Enabled Local: RAM (Recommended) Enable Local Syslog

Enabled Server 1: ☐ Enable Remote Syslog Server 1

Remote Server 1: 0.0.0.0 Remote Server 1 (DNS or IP)

Remote Port 1: 514 Remote Server 1 UDP port

Enabled Server 2: ☐ Enable Remote Syslog Server 2

Remote Server 2: 0.0.0.0 Remote Server 2 (DNS or IP)

Remote Port 2: 514 Remote Server 2 UDP port

Mqtt topic: Only for debug purposes (mqtt config needed). Field blank = disabled

Mobile Network Log: ☒ Enable network log (rssi, tech, oper)

SAVE CONFIG

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.

4.7.23 Sonstiges > Backup / Fabrik

In diesem Menü können Sie eine vollständige Sicherung der Gerätekongfiguration vornehmen. Sie können die Konfiguration in einer Datei speichern und bei Bedarf wieder auf Ihrem Computer ablegen. Außerdem können Sie das Gerät auf die Werkseinstellungen zurücksetzen.

- **Schaltfläche „Werkseinstellungen“:** Drücken Sie diese Taste, wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten.
- **Taste „Einstellungen herunterladen“:** Klicken Sie auf der Taste, um die Konfiguration des Geräts in eine Datei namens „config.mtx“ herunterzuladen
- **Schaltfläche „Datei auswählen“:** Um eine gespeicherte Konfiguration wiederherzustellen, drücken Sie nach Angabe der zu verwendenden Konfigurationsdatei die Schaltfläche „Upload“, um die Datei hochzuladen



4.7.24 Sonstiges > Neustart.

Von diesem Bereich aus kann das Gerät neu gestartet werden. Zum Beispiel, um Änderungen nach einer Konfigurationsänderung zu übernehmen. Drücken Sie dazu einfach die Schaltfläche „Neustart“

Je nach Gerät ist auch die Option „Ausschalten“ verfügbar. Mit dieser Option ist es möglich, ein Gerätemodell mit internem Akku, wie z. B. das Modell MTX-Router-Q, auszuschalten. Bevor Sie die Taste „Ausschalten“ drücken, müssen Sie das Gerät von der Stromversorgung (220 Vac) trennen und dann die Taste drücken. Nach ein paar Sekunden schalten sich alle LEDs aus.



4.8 VPN

4.8.1 VPN > OpenVPN-Server

TITAN-basierte Geräte können als OpenVPN-Server fungieren. Durch den Aufbau eines VPN sind alle Geräte, die am Ethernet-Bus des Geräts hängen, oder auch IP-RS232/485-Gateways, vom anderen Ende des VPN-Netzes aus sicher erreichbar. Eine VPN-Infrastruktur ist sehr nützlich, um die meisten Probleme mit Proxys, Firewalls usw. zu umgehen, insbesondere bei der Verwendung von SIM-Karten eines Betreibers, der private IP-Adressen (10.x.x.x) vergibt

webdyn powered by **TITAN** flexitron group

★ **Mobile**

- Status
- Basic Settings
- Keep Online

★ **Ethernet**

- Basic Settings
- DHCP Server

★ **Firewall**

- NAT
- Authorized IPs

★ **External Devices**

- Logger configuration
- ModBus Devices

★ **VPN**

- IPSec
- OpenVPN Client
- OpenVPN Server

★ **Other**

- AT Command
- DynDns
- Private DynDns
- Sme control

▶ **VPN > OpenVPN Server**

Enabled: ☐ Enable OpenVPN Server

Mode: Always on or under request (ex, by SMS)

Protocol: Communication protocol

Port: Default tcp / udp port: 1194

LZO compression: ☒ Enable LZO compression. Normally yes.

Auth: Authentication

Cipher: Cipher

Server subnet: Example 10.8.0.0 (Titan will take 10.8.0.1)

Server mask: Example 255.255.255.0

Allow LAN access: ☐ Click for allow access to devices connected to MTX

Client 1			Subnet and Mask (Ex: 192.168.1.0 / 255.255.255.0)
Client 2			Subnet and Mask (Ex: 192.168.2.0 / 255.255.255.0)
Client 3			Subnet and Mask (Ex: 192.168.3.0 / 255.255.255.0)

- **Enabled:** Markieren Sie dieses Feld, wenn Sie den OpenVPN-Dienst im Servermodus aktivieren möchten
- **Mode:** Ermöglicht die Einstellung des VPN-Verbindungsmodus. Mit der Einstellung „Immer eingeschaltet“ bleibt das VPN immer aktiv. Mit dem Wert „Unter Anfrage“ wird das VPN so lange aktiviert, wie Sie es wünschen. Sie können zum Beispiel daran interessiert sein, das VPN nur zu ganz bestimmten Zeiten für Wartungsarbeiten zu aktivieren. Wenn Sie das VPN aktivieren wollen, brauchen Sie nur einen AT-Befehl (siehe Kapitel 5 über AT-Befehle) per SMS, Telnet, Webserver, SNMP oder sogar Modbus TCP zu senden. Nach Ablauf der konfigurierten Zeit wird das VPN geschlossen.
- **Protokoll:** Sie können das Einrichtungsprotokoll einstellen. Es kann sowohl UDP- als auch TCP-Protokolle verwenden.
- **Anschluss:** Der Standardanschluss ist 1194, aber Sie können einen VPN-Anschluss Ihrer Wahl angeben.

- **LZO-Kompression:** Markieren Sie das Kästchen, wenn Sie diese Option aktivieren möchten.
- **Autor:** Hier können Sie die Authentifizierungsmethode auswählen.
- **Chiffre:** Hier können Sie den Verschlüsselungsalgorithmus auswählen.
- **Server-Subnetz:** Geben Sie das Subnetz an, das nach der VPN-Erstellung erstellt werden soll. Wenn Sie z.B. das Subnetz 10.8.0.0 angeben, wird das TITAN-basierte Gerät bei Aktivierung des VPN die Adresse 10.8.0.1 annehmen.
- **Server-Maske:** Geben Sie die Netzmaske an, die auf das VPN angewendet werden soll
- **LAN-Zugang zulassen:** Aktivieren Sie das Kontrollkästchen, wenn Sie in der Lage sein möchten, per Fernzugriff auf die Geräte zuzugreifen, die am Ethernet-Anschluss Ihres Computers hängen. Aktivieren Sie sie nicht, wenn Sie nur auf die TITAN-basierten Geräte und die von ihnen verwalteten IP-RS232/485-Gateways zugreifen wollen.
- Für OpenVPN erforderliche Dateien

Um TITAN-basierte Geräte als OpenVPN-Server zu verwenden, müssen Sie die Dateien ca.crt (Autoritätszertifikat), server.crt (Serverzertifikat), server.key (privater Serverschlüssel) und dh1024.pem (Diffie Hellman-Parameter) erstellen und hochladen.

Am unteren Ende des Bildschirms sehen Sie, dass Sie Demodateien herunterladen können, die nur zu Testzwecken verwendet werden sollten. Denken Sie daran, dass Sie in einer echten Anwendung Ihre eigenen Zertifikate erstellen müssen.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Anwendungshinweise (PDF-Dokumente außerhalb dieses Dokuments) mit Beispielen für die OpenVPN-Funktionalität mit TITAN-basierten Geräten sind verfügbar.

4.8.2 VPN > OpenVPN-Client

TITAN-basierte Geräte können als OpenVPN-Client fungieren. Durch den Aufbau eines VPN sind alle Geräte, die am Ethernet-Bus des Geräts hängen, oder auch IP-RS232/485-Gateways, vom anderen Ende des VPN-Netzes aus sicher erreichbar. Eine VPN-Infrastruktur ist sehr nützlich, um die meisten Probleme mit Proxys, Firewalls usw. zu umgehen, insbesondere bei der Verwendung von SIM-Karten eines Betreibers, der private IP-Adressen (10.x.x.x) vergibt

- ★ **Mobile**
 - Status
 - Basic Settings
 - Keep Online
- ★ **Ethernet**
 - Basic Settings
 - DHCP Server
- ★ **Firewall**
 - NAT
 - Authorized IPs
- ★ **External Devices**
 - Logger configuration
 - ModBus Devices
- ★ **VPN**
 - IPsec
 - OpenVPN Client
 - OpenVPN Server
- ★ **Other**
 - AT Command
 - DynDns
 - Private DynDns
 - Sms control
 - Periodic Autoreset
 - Time Servers
 - Remote Console

VPN > OpenVPN Client

Enabled: ☐

Mode:

Protocol:

LZO compression: ☒

Auth:

Cipher:

IP Server:

Port Server:

Username:

Password:

Enable OpenVPN Client

Always on or under request (ex, by SMS)

Communication protocol

Enable LZO compression. Normally yes.

Authentication

Cipher

IP of remote OpenVPN Server

Port of remote OpenVPN Server (def 1194)

Username. Blank if not used

Password. Blank if not used

Certificate Authority:

Client certificate:

Client KEY:

Seleccionar archivo

Ninguno archivo selec.

Upload

not uploaded

Seleccionar archivo

Ninguno archivo selec.

Upload

not uploaded

Seleccionar archivo

Ninguno archivo selec.

Upload

not uploaded

- **Enabled:** Aktivieren Sie dieses Feld, wenn Sie den OpenVPN-Dienst im Client-Modus aktivieren möchten
- **Mode:** Ermöglicht die Einstellung des VPN-Verbindungsmodus. Mit der Einstellung „Immer eingeschaltet“ bleibt das VPN immer aktiv. Mit dem Wert „Unter Anfrage“ wird das VPN so lange aktiviert, wie Sie es wünschen. Sie können zum Beispiel daran interessiert sein, das VPN nur zu ganz bestimmten Zeiten für Wartungsarbeiten zu aktivieren. Wenn Sie das VPN aktivieren wollen, brauchen Sie nur einen AT-Befehl (siehe Kapitel 5 über AT-Befehle) per SMS, Telnet, Webserver, SNMP oder sogar Modbus TCP zu senden. Nach Ablauf der konfigurierten Zeit wird das VPN geschlossen.
- **Protokoll:** Sie können das Einrichtungsprotokoll einstellen. Es kann sowohl UDP- als auch TCP-Protokolle verwenden.
- **Anschluss:** Der Standardanschluss ist 1194, aber Sie können einen VPN-Anschluss Ihrer Wahl angeben.
- **LZO-Kompression:** Markieren Sie das Kästchen, wenn Sie diese Option aktivieren möchten.
- **Autor:** Hier können Sie die Authentifizierungsmethode auswählen.
- **Chiffre:** Hier können Sie den Verschlüsselungsalgorithmus auswählen.
- **IP-Server:** Geben Sie die öffentliche IP-Adresse des Remote-Servers ein, der als OpenVPN-Server fungieren soll
- Für OpenVPN erforderliche Dateien

Um TITAN-basierte Geräte als OpenVPN-Client zu verwenden, müssen Sie die Dateien ca.crt (Autoritätszertifikat), client.crt (Client-Zertifikat) und client.key (privater Client-Schlüssel) erstellen und hochladen.

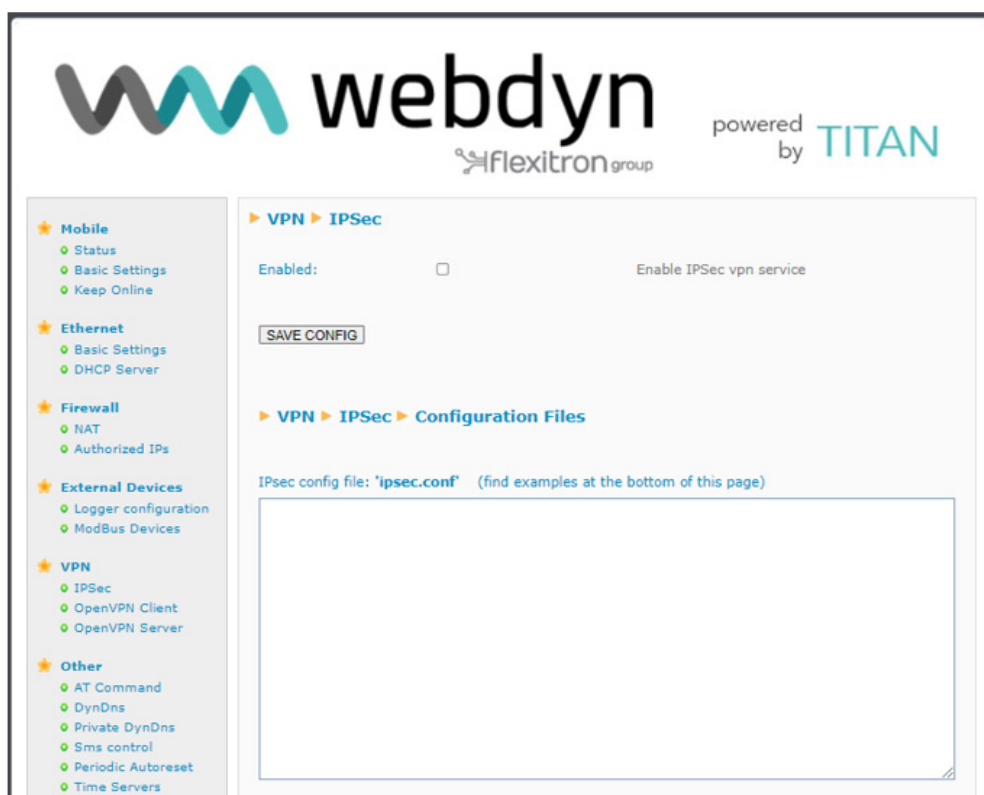
Am unteren Ende des Bildschirms sehen Sie, dass Sie Demodateien herunterladen können, die nur zu Testzwecken verwendet werden sollten. Denken Sie daran, dass Sie in einer echten Anwendung Ihre eigenen Zertifikate erstellen müssen.

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Anwendungshinweise (PDF-Dokumente außerhalb dieses Dokuments) mit Beispielen für die OpenVPN-Funktionalität mit TITAN-basierten Geräten sind verfügbar.

4.8.3 VPN > IPsec

TITAN-basierte Geräte verfügen über die IPSEC-Funktion. Durch den Aufbau eines VPN sind alle Geräte, die am Ethernet-Bus des Geräts hängen, oder auch IP-RS232/485-Gateways, vom anderen Ende des VPN-Netzes aus sicher erreichbar. Eine VPN-Infrastruktur ist sehr nützlich, um die meisten Probleme mit Proxys, Firewalls usw. zu umgehen, insbesondere bei der Verwendung von SIM-Karten eines Betreibers, der private IP-Adressen (10.x.x.x.x) vergibt



- **Enabled:** Aktivieren Sie dieses Feld, wenn Sie den IPsec-Dienst aktivieren möchten

- **ipsec.conf:** Geben Sie hier Ihre IPSec-VPN-Konfigurationsdatei ein. Sie können die Beispiele am unteren Rand des Bildschirms konsultieren und an Ihre Bedürfnisse anpassen.
- **ipsec.secrets:** Tragen Sie hier den Inhalt der Datei ipsec.secrets Ihres IPSec-VPNs ein. Sie können die Beispiele am unteren Rand des Bildschirms konsultieren und an Ihre Bedürfnisse anpassen.

TITAN-basierte Geräte, die als IPSec-Client fungieren:

- xca1-cert.pem: Datei mit dem Root-CA-Zertifikat Ihres IPSEC-Servers
- xclient1-cert.pem: Datei mit dem Client-Zertifikat
- xclient1-key.pem: Datei mit dem KEY

TITAN-basierte Geräte, die als IPSec-Server fungieren:

- ca-cert.pem: Root-CA-Datei des TITAN-basierten Geräts
- ca-key.pem: Datei mit dem KEY der CA des TITAN-basierten Geräts
- server-cert.pem: Zertifikatsdatei des TITAN-basierten Geräts
- server-key.pem: Datei mit dem KEY des TITAN-basierten Geräts
- client1-cert.pem: Datei mit dem Zertifikat von Client 1, der zur Verbindung berechtigt ist
- client2-cert.pem: Datei mit dem Zertifikat von Client 1, der zur Verbindung berechtigt ist
- client3-cert.pem: Datei mit dem Zertifikat von Client 1, der zur Verbindung berechtigt ist

Zusätzliche Hinweise.

- Sobald die Konfiguration abgeschlossen ist, drücken Sie die Taste „SAVE CONFIG“, um die Änderungen zu speichern. Denken Sie daran, Ihren Computer neu zu starten, damit die neuen Änderungen wirksam werden.
- Anwendungshinweise (PDF-Dokumente außerhalb dieses Dokuments) mit Beispielen für die IPSec-Funktionalität mit TITAN-basierten Geräten sind verfügbar.

5. AT-Befehle

Bei TITAN-basierten Geräten können AT-Befehle über mehrere Schnittstellen direkt an das interne Modem gesendet werden:

1. Über einen seriellen Anschluss.
2. Über ein seriellles 4G/3G/2G-Gateway (über IP WAN, Ethernet oder Wifi) durch integrierte AT-Befehle.
3. Per SMS
4. Über Telnet (Remote-Konsole, über 4G/3G/2G, Ethernet oder Wifi). Über SSH (Remote-Konsole, über 4G/3G/2G, Ethernet oder Wifi)
5. Über Webserver (über 4G/3G/2G, Ethernet oder Wifi)
6. Über Modbus RTU (über die serielle Schnittstelle RS232 oder RS485)
7. Über Modbus TCP (über 4G/3G/2G, Ethernet oder Wifi)
8. Über SNMP (über 4G/3G/2G, Ethernet oder Wifi)
9. Über URL. Wird am Ende dieses Punktes erklärt.

Daher können Sie auf eigene Gefahr AT-Befehle an das Gerät senden.

- **AT^MTXTUNNEL=NEUSTART**

- **Aktion:** Setzt das TITAN-basierte Gerät zurück.

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel:** AT^MTXTUNNEL=REBOOT

OK

- **AT^MTXTUNNEL=VERSION**

- **Aktion:** Gibt die Firmware-Version des TITAN-basierten Geräts zurück.

- **Gibt die Firmware-Version des TITAN-basierten Geräts zurück**

Ergebnis:

OK: Befehl wurde korrekt ausgeführt.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel: AT^MTXTUNNEL=VERSION**

5.2.6.17

OK

- **AT^MTXTUNNEL=GETIP**

- **Aktion:** Gibt die WAN-IP-Adresse zurück (2G / 3G / 4G)

Ergebnis:

OK: Befehl wurde korrekt ausgeführt.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel: AT^MTXTUNNEL=GETIP**

88.28.221.14

OK

Ergebnis:

OK: Befehl wurde korrekt ausgeführt.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel: AT^MTXTUNNEL=GETIMEI**

869101054255506

OK

- **AT^MTXTUNNEL=GETCELLID**

Handlung: gibt die vom Modem verwendete Telefoneizelle zurück.

Ergebnis:

OK: Befehl wurde korrekt ausgeführt.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel: AT^MTXTUNNEL=GETCELLID**

[4;214;07;219B;15F2D2A]

OK

Wo: 4 = verwendete Technologie (2=2g,3=3)

214 = MCC (Mobiler Ländercode)

07 = MNC (Mobilnetz-Code)
07 = LAC (Ortsnetzkennzahl)
15F2D2A = CID (Zellen-ID)

AT-Befehle im Zusammenhang mit der Nachrichtenübermittlung:

- **AT^MTXTUNNEL=TRAP,OID;myMessage;mySeverity**

- **Aktion:** Ermöglicht das Senden eines SNMP-TRAP mit einer bestimmten OID, der zugehörigen Nachricht und dem Schweregrad.

- **Parameter:**

<OID>: OID des Traps, der von SNMP <myMessage> gesendet werden soll: zu sendende Textnachricht

<mySeverity>: 0 ... 7 Trap-Schweregrad

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. Nachricht gesendet.

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel:** AT^MTXTUNNEL=TRAP,.1.3.6.1.4.1.45711.1.1.11.1.1;myMessage;5

- **AT^MTXTUNNEL=SMS,Rufnummer,Nachricht**

- **Aktion:** Ermöglicht es Ihnen, eine SMS-Nachricht an eine bestimmte Rufnummer zu senden.

- **Parameter:**

<telephoneNumber>: Rufnummer, an welche die SMS-Nachricht <message> gesendet werden soll: zu sendende Textnachricht

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. SMS-Nachricht an die Ausgabewarteschlange gesendet.

ERROR:Befehl wurde mit Fehler ausgeführt

OK

- **AT^MTXTUNNEL=EMAIL,destinationAddress,Betreff**

- **Aktion:** Ermöglicht es Ihnen, eine E-Mail (nur Betreff) an eine bestimmte E-Mail-Adresse zu senden. Um die E-Mail zu versenden, müssen Sie zuvor den Abschnitt „Sonstiges > E-Mail-Konfiguration“ konfiguriert haben.

- **>,<subject>Parameter:**

<destinationAddress>: ziel-E-Mail-Adresse

<subject>: per E-Mail zu versendende Nachricht

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. E-Mail gesendet.

ERROR:Befehl wurde mit Fehler ausgeführt

OK

- **Beispiel:** AT^MTXTUNNEL=EMAIL,jgallego@matrix.es,Temperaturalarm
- **AT^MTXTUNNEL=TELEGRAM,SEND,tokenID,chatID,Nachricht**
- **Aktion:** Ermöglicht es Ihnen, eine Telegram-Textnachricht an einen bestimmten Telegram-Gruppenchat zu senden. Es ist notwendig, einen Bot mit der TokenID zu erstellen und die ChatID des Chats, an den die Nachricht gesendet werden soll, zu erhalten
- **Parameter:**

<tokenID>: token-Bezeichner

<chatID>: Chatkennzeichen

<message>: Telegrammanschrift

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. Nachricht gesendet.

ERROR:Befehl wurde mit Fehler ausgeführt

OK

- **Beispiel:** AT^MTXTUNNEL=TELEGRAM,SEND,5416419553:ZZHof6enVx-y7uFQrL15cpf3QCHqNHp7Dtg,-730297962,My message

E/A-bezogene AT-Befehle:

- **AT^MTXTUNNEL=GETIO,idIO**
- **Aktion:** Gibt den Wert eines digitalen Ein- oder Ausgangs zurück, wobei idIO der Identifikator des IO ist (0,1,2...)
- **Parameter:**

<idIO>: 0, ... X Anzahl der E/A

- **Ergebnis:**

OK: Befehl erfolgreich ausgeführt, wobei der Status des digitalen Eingangs oder Ausgangs zurückgegeben wird.

ERROR:Befehl wurde mit Fehler ausgeführt

Beispiel: Status des digitalen Eingangs E/A 0 lesen

AT^MTXTUNNEL=GETIO,0

1

OK

- **AT^MTXTUNNEL=SETIO,idIO,value**

- **Aktion:** Ermöglicht es, den Zustand eines digitalen Ausgangs zu ändern, wobei idIO der Identifikator des IO (0,1,2...) und Value der logische Wert des Ausgangs (0, 1) ist

- **Parameter:**

<idIO>: 0, ... X Anzahl der E/A

<value>: 0,1 Wert, der am digitalen Ausgang eingestellt werden soll

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. Verbesserter digitaler Ausgang.

ERROR:Befehl wurde mit Fehler ausgeführt

- **AT^MTXTUNNEL=GETCOUNTER,idIO**

- **Aktion:** Gibt den Wert des Impulszählers zurück, der einem digitalen Eingang zugeordnet ist, wobei idIO der Identifikator des IO ist (0,1,2...)

- **Parameter:**

<idIO>: 0, ... X Anzahl der E/A

- **Ergebnis:**

OK: Der Befehl wurde korrekt ausgeführt und gibt den Wert des Impulszählers zurück, der dem digitalen Eingang ERROR zugeordnet ist: Befehl wurde mit Fehler ausgeführt

1022

- **AT^MTXTUNNEL=SETCOUNTER,idIO,value**

- **Aktion:** Ermöglicht die Änderung des Wertes eines Impulszählers, der mit einem digitalen Eingang verbunden ist, wobei idIO der Identifikator des IO (0,1,2...) und Value der Wert des Zählers ist

- **Parameter:**

<idIO>: 0, ... X Anzahl der E/A

<value>: 0,1 Wert, der im mit dem Digitaleingang verbundenen Zähler gesetzt werden soll.

- **Ergebnis:**

OK: Befehl erfolgreich ausgeführt

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel:** AT^MTXTUNNEL=SETCOUNTER,3,1000

AT-Befehle im Zusammenhang mit OpenVPN:

- **AT^MTXTUNNEL=OVPNS,Minuten**

- **Aktion:** Wenn Sie den Bereich VPN > OpenVPN Server als On-Demand-OpenVPN konfiguriert haben, können Sie mit diesem AT-Befehl das OpenVPN im Servermodus für die angegebenen Minuten aktivieren.

- **Beispiel:** AT^MTXTUNNEL=OVPNS,5

(Dieses Beispiel würde das VPN für 5 Minuten aktivieren)

- **Parameter:**

<minutes>: 1 ... 525600 Minuten

- **Ergebnis:**

OK: Befehl wurde erfolgreich ausgeführt

ERROR:Befehl wurde mit Fehler ausgeführt

- **AT^MTXTUNNEL=OVPNC,Minuten**

- **Aktion:** Wenn Sie den Bereich VPN > OpenVPN Client als On-Demand-OpenVPN konfiguriert haben, können Sie mit diesem AT-Befehl das OpenVPN im Client-Modus für die angegebenen Minuten aktivieren.

- **Beispiel:** AT^MTXTUNNEL=OVPNC,5

(Dieses Beispiel würde das VPN für 5 Minuten aktivieren)

- **Parameter:**

<minutes>: 1 ... 525600 Minuten

- **Ergebnis:**

OK: Befehl wurde erfolgreich ausgeführt

ERROR: Befehl wurde mit Fehler ausgeführt

AT-Befehle zum Testen der Konnektivität:

- **AT^MTXTUNNEL=COMMAND,timeout,command**

- **Aktion:** Ermöglicht die Ausführung bestimmter spezieller Befehle innerhalb des TITAN-basierten Geräts. Zurzeit sind nur die Befehle „ping“ und „traceroute“ verfügbar. Es ist erlaubt, einen Timeout (in Sekunden) sowie den auszuführenden Befehl anzugeben.

- **Parameter:**

<timeout>: 1 ... 60 Sekunden timeout

<command>: ping, traceroute

- **Beispiel:** AT^MTXTUNNEL=COMMAND,5,ping -c 3 8.8.8.8

(Dieses Beispiel würde 3 PINGS an IP 8.8.8.8 mit einem Timeout von 5 Sekunden ausführen)



AT-Befehle im Zusammenhang mit MODBUS:

- **AT^MTXTUNNEL=GETMODBUS** • ,<modbusAddress>;<addressFirstRegister>; Gibt den Wert eines oder mehrerer Modbus-Register eines Geräts zurück. Achtung: Modbus-bezogene Parameter werden durch „;“ und nicht durch „“,“ getrennt

- **Parameter:**

<modbusAddress>: Modbus-Geräteadresse (1 ... 255) oder IP-Adresse@dir:port

<addressFirstRegister>: Adresse des ersten zu lesenden Datensatzes (0 ... 65535)

<numWords>: Anzahl der zu lesenden Modbus-Register (1 ... 64)

<command>: Modbus-Schreibbefehl (5,6,15,16)

- **Ergebnis:**

OK: Befehl wurde korrekt ausgeführt. Gibt die gelesenen Wörter durch „“,“ getrennt zurück

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel:** **AT^MTXTUNNEL=GETMODBUS,192.168.1.200;502;1;1;3;3** , gesendet von der Web-Konfigurationsumgebung (obwohl es auch per SMS oder Remote-Konsole (Telnet) gesendet werden könnte), wobei die Werte 20, 21, 22 als Antwort erhalten werden



- **AT^MTXTUNNEL=SETMODBUS,dirModbus;dirFirstRegister;command;data1;data2; ...dataX**

Ergebnis:

OK: Befehl wurde erfolgreich ausgeführt

ERROR:Befehl wurde mit Fehler ausgeführt

Parameter:

<modbusAddress>: Modbus-Geräteadresse (1 ... 255) oder IP-Adresse@dir:port

<addressFirstRegister>: Adresse des ersten zu schreibenden Registers (0 ... 65535)

<command>: Modbus-Schreibbefehl (5,6,15,16)

-<data1>, .. <dataX>: Werte der zu schreibenden Modbus-Register (0 ... 65535)

- **Beispiel:** **AT^MTXTUNNEL=SETMODBUS,1;3;16;10;11;12;13;14;15** schreibt in das Modbus-RTU-Gerät mit der Adresse 1, beginnend bei Register 3 und mit dem Modbus-Schreibbefehl 16, die Werte 10,11,12,13,14 und 15.
- **Beispiel:** **AT^MTXTUNNEL=SETMODBUS,192.168.1.202@1;502;3;16;10;11;12;13;14;15** schreibt an das Modbus-TCP-Gerät mit der IP-Adresse 192.168.1.202 unter Verwendung der RTU-Adresse @1 und des TCP-Anschlusses 502, beginnend bei Register 3 und unter Verwendung des Modbus-Schreibbefehls 16, die Werte 10,11,12,13,14 und 15.
- **Beispiel:** **AT^MTXTUNNEL=SETMODBUS,1;3;6;10** schreibt in das Modbus-RTU-Gerät mit der Adresse 1, in Register 3 und mit dem Modbus-Schreibbefehl 6 den Wert 10
- **Beispiel:** **AT^MTXTUNNEL=SETMODBUS,1;18;5;1** schreibt an das Modbus-RTU-Gerät mit der Adresse 1, an der Spule 18 und mit dem Modbus-Schreibbefehl 5, den Wert 1
- **Beispiel:** **AT^MTXTUNNEL=SETMODBUS,1;25;15;1;0;1;0;1** schreibt an das Modbus-RTU-Gerät mit der Adresse 1, beginnend bei Spule 25 und unter Verwendung des Modbus-Schreibbefehls 15, den Wert der Spulen 1,0,1,0 und 1

AT-Befehle in Zusammenhang mit der Systemzeit:

- **AT^MTXTUNNEL=GETTIME**

Aktion: Gibt die aktuelle Zeit zurück Gibt die aktuelle Systemzeit im Format JJJJ-MM-TTTHH:NN:SSZ (UTC) zurück

- **Ergebnis:**

OK: Befehl wurde erfolgreich ausgeführt

ERROR:Befehl wurde mit Fehler ausgeführt

- **Beispiel:**

AT^MTXTUNNEL=GETTIME

2016-21-05T10:56:52Z

OK

- **AT^MTXTUNNEL=SETTIME,<dateAndHour>**

Handlung: Stellt die aktuelle Uhrzeit ein.

Parameter:

<dateAndHour> Datum/Uhrzeit im UTC-Format JJJJ-MM-TTTHH:NN:SSZ

Ergebnis:

OK: Befehl wurde erfolgreich ausgeführt

ERROR: Befehl wurde mit Fehler ausgeführt

Beispiel:

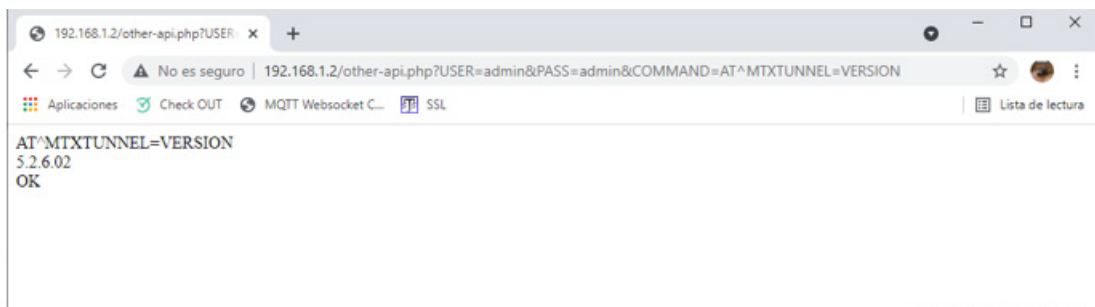
AT^MTXTUNNEL=SETTIME,2023-01-10T14:42:23Z

OK

AT-Befehle in Zusammenhang mit der Konfiguration des Titan-Geräts:

- **AT^MTXTUNNEL=GETPARAM,<paramName>**

Aktion: So können Sie beispielsweise die Konfiguration jeder Geräteparameter über eine Webplattform oder über ein an den Ethernet- oder WLAN-Anschluss angeschlossenes Gerät TITAN sehen. Wenn Sie mit der Maus auf ein beliebiges Feld einer beliebigen Konfigurationsseite des TITAN-basierten Geräts doppelklicken, erhalten Sie den Namen des Feldes.



- **Parameter:**

<paramName> Name des zu lesenden Konfigurationsparameters

Ergebnis:

OK: Lesen des richtigen Konfigurationsparameters

ERROR: Fehler beim Lesen des richtigen Konfigurationsparameters

- **Beispiel:**

AT^MTXTUNNEL=GETPARAM,WAN_APN

m2m.movistar.es

OK

- **AT^MTXTUNNEL=SETPARAM,paramName,paramWert**

Aktion: Ermöglicht es Ihnen, den Wert eines beliebigen Konfigurationsparameters des TITAN-basierten Geräts zu ändern. So können Sie beispielsweise die Konfiguration fast aller Parameter des TITAN-basierten Geräts über eine Web-Plattform oder über ein Gerät ändern, das mit dem Ethernet- oder Wifi-Anschluss des TITAN-basierten Geräts verbunden ist. Wenn Sie mit der Maus auf ein beliebiges Feld einer beliebigen Konfigurationsseite des TITAN-basierten Geräts doppelklicken, erhalten Sie den Namen des Feldes. Um den Namen des Feldes mit „Doppelklick“ sehen zu können, müssen Sie zuerst den AT-Befehl senden: AT^MTXTUNNEL=SETPARAM,MTX_SHOWNAMES,1

- **Parameter:**

<paramName> Name des zu ändernden Konfigurationsparameters

<paramValue> Neuer Wert des Konfigurationsparameters

- **Ergebnis:**

OK: Der Wert des Konfigurationsparameters wurde korrekt geändert

ERROR:Fehler beim Ändern des Wertes des Konfigurationsparameters.

- **Beispiel:**

^MTXTUNNEL=SETPARAM,WAN_APN,m2m.movistar.es OK



- **AT^MTXTUNNEL=SETFILE,<fileName>,<length>,<{data_base64}>**

Handlung: so wie der Befehl AT^MTXTUNNEL=SETPARAM die Änderung des Wertes eines Konfigurationsparameters durch einen AT-Befehl ermöglicht, erlaubt dieser Parameter die Änderung der Konfiguration von Parametern vom Typ Datei (Skripte, Zertifikate, Operatoren, ...). Der Name der Datei erscheint neben den entsprechenden Konfigurationsfeldern.

- **Parameter:**

<fileName> Dateiname

<length> Datenlänge des data_base64-Feldes, ohne Berücksichtigung von { }

<{data_base64}>: dateidaten in base64 kodiert. Der Text muss in { } angegeben werden

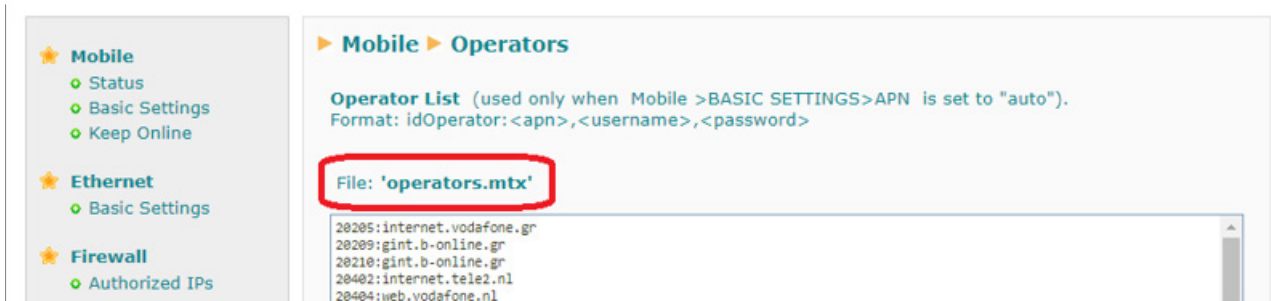
- **Ergebnis:**

OK: Die Datei wurde erfolgreich hochgeladen

ERROR:Fehler bei der Ausführung des Befehls.

- **Beispiel:**

Wenn Sie z. B. die Datei „operators.mtx“ im Abschnitt „Mobile“ ändern möchten > Basic Settings > Operators



Der zu sendende AT-Befehl würde lauten

AT*MTXTUNNEL=SETFILE,operators.mtx,220,{MjE0MDY6YWlydGVsbmV0LmVzCjlxNDA3Om1vdmldzGFyLmVzLE1PVkIWEFSLE1PVkIWEFSCjlxNDA4OmludGVybWV0LmV1c2thbHRlbC5tb2JpCjlxNDE2OmludGVybWV0LmV1c2thbGJvJWJsZS5lcwoyMTQxNzppbnRlcm5ldC5tdW5kby1yLmVnbG9yMTQxODppbnRlcm5ldC5vbW8uY29tCg==}

Hinweis: nachfolgend finden Sie einige nützliche Links für Ihre Tests:

<https://www.base64encode.org/>

<https://wordcounter.net/character-count>

- **AT^MTXTUNNEL=GETFILEHASH,<fileName>**

Handlung: gibt den HASH-Wert einer im Gerät gespeicherten Datei zurück.

Parameter:

<fileName> Dateiname

- **Ergebnis:**

{<HASH>}OK: HASH der Datei.

ERROR:Fehler bei der Ausführung des Befehls.

- **Beispiel:**

Wenn Sie zum Beispiel den HASH-Wert der Datei „operators.mtx“ nachschlagen wollen

AT^MTXTUNNEL=GETFILEHASH,operators.mtx

```
{06FD031D0CE8B58EA41A4E282047818E0EB74EFEEF3097F719968571DD7D8BC3}
```

OK

AT-Befehle im Zusammenhang mit Zählern IEC-60870-5-102

- **AT^MTXTUNNEL=SETIEC102,<IDMETER>**

Handlung: durch die Ausführung dieses Befehls ist es möglich, den Start der Auslesung der Echtzeitwerte eines Zählers mit IEC-60870-5-102-Protokoll zu erzwingen. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtX konfigurierter Tag. iec102AddMeter

- Ergebnis:**
 OK: Der Prozess wurde eingeleitet.
 ERROR:Fehler beim Start des BUSY-Prozesses
 BUSY: Serieller Bus belegt durch einen CSD-Anruf, IP-RS232-Gateway
- Beispiel:**
 AT^MTXTUNNEL=SETIEC102,ID0001
 OK
- AT^MTXTUNNEL=GETIEC102,<IDMETER>**

Handlung: Lesen des Ergebnisses der Ausführung des Befehls AT^MTXTUNNEL=SETIEC102,<IDMETER>. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: Zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtX konfigurierter Tag. iec102AddMeter

Ergebnis:

OK: Richtig gelesen
 ERROR:Fehler beim Lesen oder der Lesevorgang ist noch nicht abgeschlossen.

Beispiel:

```
AT^MTXTUNNEL=GETIEC102,ID0001
{"IMEI":"869101054255506","TYPE":"IEC102","TS":"2023-01-26T09:22:37Z","P":"MTX1","ID":"ID0001","VABA":0,"VABRI":0,"VABRC":0,"PAT":0,"PRT":0,"FPT":1000,"PAF1":0,"PRF1":0,"FPF1":1000,"PAF2":0,"PRF2":0,"FPF2":1000,"PAF3":0,"PRF3":0,"FPF3":1000,"IF1":0,"TF1":1156,"IF2":0,"TF2":1141,"IF3":0,"TF3":1}
```

OK

- AT^MTXTUNNEL=SETIEC102_CTAVM2, <IDMETER>, <hourIni>, <minuteIni>, <dayIni>, <monthIni>, <yearIni>, <hourEnd>, <minuteEnd>, <dayEnd>, <monthEnd>, <yearEnd>

Handlung: durch die Ausführung dieses Befehls ist es möglich, einen Auslesestart der Fiskalabschlüsse (Vertrag I) eines Zählers mit IEC-60870-5-102-Protokoll zu erzwingen. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: Zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtX konfigurierter Tag. iec102AddMeter

<hourIni>: Startstunde des Intervalls (0 ... 23)

<minuteIni>: Startminute des Intervalls (0 ... 59)
<dayIni>: erster Tag des Intervalls (1 ... 31)
<monthIni>: Anfangsmonat des Intervalls (1 ... 12)
<yearIni>: Anfangsjahr des Intervalls (20 ... 99)
<hourEnd>: Endstunde des Intervalls (0 ... 23)
<minuteEnd>: Endminute des Intervalls (0 ... 59)
<dayEnd>: Endtag des Intervalls (1 ... 31)
<monthEnd>: Endmonat des Intervalls (1 ... 12)
<yearEnd>: Endjahr des Intervalls (20 ... 99)

Ergebnis:

OK: Der Prozess wurde eingeleitet.

ERROR:Fehler beim Start des BUSY-Prozesses

BUSY: Serieller Bus belegt durch einen CSD-Anruf, IP-RS232-Gateway

Beispiel:

AT^MTXTUNNEL=SETIEC102_CTAVM2,ID001,0,0,22,12,22,0,0,24,1,23

OK

- **AT^MTXTUNNEL=GETIEC102_CTAVM2,<IDMETER>**

Handlung: Lesen des Ergebnisses der Ausführung des Befehls AT^MTXTUNNEL=SETIEC102_CTAVM2,<IDMETER>. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtz konfigurierter Tag. iec102AddMeter

Ergebnis:

OK: Richtig gelesen

ERROR:Fehler beim Lesen oder der Lesevorgang ist noch nicht abgeschlossen.

Beispiel:

```

AT^MTXTUNNEL=GETIEC102_CTAVM2,ID001
{"IMEI":"869101054255506","TYPE":"IEC102_CTAVM2","TS":"2023-01-
26T09:41:29Z","P":"MTX1","ID":"ID001","CTAVM2":{"DO":20,"EaA":0,"EiA":0,"CA":2,"EaRi":
0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"CRc":2,"R7":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMP
A":"2023-01-09T12:58-0","CMA":2,"EPA":0,"CE":128,"DINI":"2022-12-01T00:00-
0","DEND":"2023-01-09T12:58-
0"},"DO":21,"EaA":0,"EiA":0,"CA":2,"EaRi":0,"EiRi":0,"CRi":2,"EaRc":0,"EiRc":0,"CRc":2,"R7
":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":2,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-
0"},"DO":22,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7
":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-
0"},"DO":23,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7
":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-
0"},"DO":24,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7
":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-
0"},"DO":25,"EaA":0,"EiA":0,"CA":0,"EaRi":0,"EiRi":0,"CRi":0,"EaRc":0,"EiRc":0,"CRc":0,"R7
":0,"C7":128,"R8":0,"C8":128,"MPA":0,"FMPA":"2023-01-09T12:58-
0","CMA":0,"EPA":0,"CE":0,"DINI":"2022-12-01T00:00-0","DEND":"2023-01-09T12:58-

```

- **AT^MTXTUNNEL=SETIEC102_CCINX2,<IDMETER>,<hourIni>,<minuteIni>,<dayIni>,<monthIni>,<yearIni>,<hourEnd>,<minuteEnd>,<dayEnd>,<monthEnd>,<yearEnd>,<absoluteIncremental>,<period>**

Handlung: durch die Ausführung dieses Befehls ist es möglich, den Start der Auslesung der integrierten Summen (Lastkurve) eines Zählers mit IEC-60870-5-102-Protokoll zu erzwingen. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtX konfigurierter Tag. iec102AddMeter

<hourIni>: Startstunde des Intervalls (0 ... 23)

<minuteIni>: Startminute des Intervalls (0 ... 59)

<dayIni>: erster Tag des Intervalls (1 ... 31)

<monthIni>: Anfangsmonat des Intervalls (1 ... 12)

<yearIni>: Anfangsjahr des Intervalls (20 ... 99)

<hourEnd>: Endstunde des Intervalls (0 ... 23)

<minuteEnd>: Endminute des Intervalls (0 ... 59)

<dayEnd>: Endtag des Intervalls (1 ... 31)

<monthEnd>: Endmonat des Intervalls (1 ... 12)

<yearEnd>: Endjahr des Intervalls (20 ... 99)

<absoluteIncremental>: 0=absolut, 1=inkrementell <period>: 0=stündlich, 1=viertelstündlich

Ergebnis:

OK: Der Prozess wurde eingeleitet.

ERROR:Fehler beim Start des BUSY-Prozesses

BUSY: Serieller Bus belegt durch einen CSD-Anruf, IP-RS232-Gateway

Beispiel:

```
AT^MTXTUNNEL=SETIEC102_CCINX2,ID001,15,0,19,1,23,20,0,19,1,23,1,0
```

OK

- **AT^MTXTUNNEL=GETIEC102_CCINX2,<IDMETER>**

Handlung: Lesen des Ergebnisses der Ausführung des Befehls AT^MTXTUNNEL=SETIEC102_CCINX2,<IDMETER>. Der Dienst im Abschnitt „Externe Geräte >IEC102 Zähler“ muss aktiv und korrekt konfiguriert sein.

Parameter:

<IDMETER>: zählerkennzeichen. Im Abschnitt „Externe Geräte >IEC102 Zähler“ oder im Code eines Skripts mit der Funktion mtz konfigurierter Tag. iec102AddMeter

Ergebnis:

OK: Richtig gelesen

ERROR:Fehler beim Lesen oder der Lesevorgang ist noch nicht abgeschlossen.

Beispiel:

```
AT^MTXTUNNEL=GETIEC102_CCINX2,ID001
```

```
{["IMEI":"869101054255506","TYPE":"IEC102_CCINX2","TS":"2023-01-26T09:54:10Z","P":"MTX1","ID":"ID001","CCINX2":[{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T15:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T16:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T17:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T18:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T19:00-00"},{"DO":11,"TI1":0,"TI2":0,"TI3":0,"TI4":0,"TI5":0,"TI6":0,"TI7":0,"TI8":0,"Q1":128,"Q2":128,"Q3":128,"Q4":128,"Q5":128,"Q6":128,"Q7":128,"Q8":128,"DATE":"2023-01-19T20:00-00"}]}
```

OK

6.- Neuigkeiten in den Firmwareversionen

6.17 - Möglichkeit der autonomen Ablesung von Lastkurven für IEC-60870-5-102 Zähler aus einem Skript. Neue SCRIPT-Funktionen `mtx.iec102SetIntegratedTotal` und `mtx.iec102GetIntegratedTotal...`

- Neues SCRIPT-Beispiel 52, das zeigt, wie man die Lastkurven eines IEC-60870-5-102-Zählers ausliest.

- Neue Befehle `AT^MTXTUNNEL=SETIEC102_CCINX2` und `AT^MTXTUNNEL = GETIEC102_CCINX2` zum Auslesen von Lastkurven für IEC-60870-5-102-Zähler

6.18 - Verbesserungen bei der Behandlung von TCP-Client-Verbindungen im Falle eines Kontextverlustes.

6.19.- MAC-Filterung aus dem Abschnitt "Firewall > Mac Filter"

- IEC60870-5.102. Es wurden Parameter (`patDir`, `paf1Dir`, `paf2Dir`, `paf3Dir`) hinzugefügt, um importierte/exportierte Energie im JSON der momentanen Energiewerte anzugeben.

- IEC60870-5.102. Neuer Konfigurationsparameter im Abschnitt „Externe Geräte > Zähler 102“, der es erlaubt, den Parametern `pat/fpt`, `paf1/fpf1`, `paf2/fpf2`, `paf3/fpf3` Vorzeichen zuzuweisen

- Ästhetische Verbesserungen am Programmierbildschirm von Titan Scripts

- Hinzufügen der Methoden HTTP PUT und HTTPS PUT zu den Sendeoptionen LOGGER und SCRIPTS.

- Änderung des SCRIPT-Beispiels 39 einschließlich der HTTP PUT-Methode.

- Neue Funktion `mtx.loggerSendingEnabled` für den Abschnitt SCRIPTS. Mit dieser Funktion kann der Dienst zum Senden der im LOGGER gespeicherten Daten aktiviert/deaktiviert werden.

- Neues SCRIPT von Beispiel 7b. Lesen eines TCP-Modbus-Registers.

- Neues SCRIPT-Beispiel 14b. Lesen von Modbus-RTU-Registern, Anpassung des Sende-JSON, Speicherung im LOGGER und Zeitplanung des Sendens innerhalb eines bestimmten Zeitplans.

- Neuer Befehl `AT^MTXTUNNEL=GETFILEHASH,<filename>`, der es ermöglicht, den HASH-Wert einer internen Konfigurationsdatei zu lesen.