Technische Produktbeschreibung

MU100

MU100.SW.TPB.0006

Release 1.1.x

Erstellt:	12.03.2026	Kanzur, Robert	Projekt:	MU100
Geprüft:	12.03.2026	Löber, Daniel	Kunde:	TQ-Automation
			Dokumenten-Nr.:	MU100.SW.TPB.0006
Firma:	TQ-Systems GmbH		Datei:	MU100.SW.TPB.0006.docx

© TQ-Systems GmbH. Sämtliche in diesem Dokument enthaltenen Informationen sind streng vertraulich zu behandeln. Eine Weitergabe der Darstellungen und Kenntnisse an Dritte bedarf der schriftlichen Zustimmung der TQ-Systems GmbH.

Inhaltsverzeichnis

Abbildungsverzeichnis **4**
Tabellenverzeichnis **5**
Änderungshistorie **6**
1 Umfang des Dokuments **7**
1.1 Zweck des Dokuments 7
1.2 Rechtlicher Hinweis 7
1.3 Referenzierte Dokumente 7
1.4 Verwendete Abkürzungen 8
2 Hardwarefunktionen **9**
2.1 LED-Zustände 9
2.1.1 LED „STATUS“ 9
2.1.2 LED „NETWORK“ 9
2.1.3 LED „SERIAL BUS“ 9
2.1.4 Identifikation des Gerätes 9
2.2 Funktionen der Reset-Taste 9
2.2.1 Neu starten 9
2.2.2 Zurücksetzen auf Werkseinstellung 9
3 Geräteeinstellung **10**
3.1 Einstellungen über Webserver 10
3.2 Werkseinstellung 10
4 Datenerfassung **11**
4.1 Messwerte 11
4.2 Fehlerspeicher 12
4.3 Ereignisspeicher 12
5 Modbus-Schnittstelle **13**
5.1 Modbus RTU 13
5.1.1 Terminierung 13
5.1.2 Idle-line Failsafe 13
5.2 Modbus TCP 14
5.3 Modbus TCP mit TLS 14
6 Netzwerk **15**
6.1 Netzwerkkonfiguration 15
6.2 mDNS 15
6.3 TCP Keepalive 16
6.4 IPv6 16
6.5 Auto IP 16
6.6 SNTP und Offline Timebasis 17
7 Webserver **18**
7.1 Autorisierung und Nutzerberechtigungen 18
7.2 Funktionen des Webserver Frontend 20
7.2.1 Dashboard 20
7.2.2 Manuelle Updatefunktionalität 22
7.2.3 OTA-Updatefunktionalität 23
7.2.4 Gerätekonfiguration 24
7.2.5 Logout 24

8 Update 25
8.1 Manuelles Update über Webserver Frontend 25
8.2 Manuelles Update über HTTPS Schnittstelle 25
8.2.1 Programmablaufplan 25
8.2.2 Beschreibung HTTP Update 25
8.2.3 Bereitgestellte REST Routen für Updatevorgang 26
8.3 Automatisches Remote Update 29
A. Anhang 30
8.4 Programmablaufplan Update über HTTP Rest Routen 31

Abbildungsverzeichnis

Abbildung 1: Modbus Anschluss 13
Abbildung 2: Anmeldebildschirm Webserver 18
Abbildung 3: Fehlgeschlagene Autorisierung Webserver 19
Abbildung 4: Dashboard des Webservers 20
Abbildung 5: Updateseite 22
Abbildung 6: Pop-Up Fenster während erfolgreichem Update 22
Abbildung 7: Fehlgeschlagenes Update über Webserver 23
Abbildung 8: Manuelle und OTA Updatefunktionalität 23
Abbildung 9: Gerätekonfiguration über Frontend des Webservers 24
Abbildung 10: Programmablaufplan manuelles Update 31

Tabellenverzeichnis

Tabelle 1: Änderungsverfolgung 6
Tabelle 2: Referenzierte Dokumente 7
Tabelle 3: Abkürzungen 8
Tabelle 4: Konfiguration Werkseinstellung 10
Tabelle 5: Parameter der Netzwerkkonfiguration 15
Tabelle 6: HTTP Response Codes für POST /authorize 26
Tabelle 7: HTTP Response Codes für POST /prepare 27
Tabelle 8: HTTP Response Codes für POST /upload 27
Tabelle 9: HTTP Response Codes für POST /retry 28
Tabelle 10: HTTP Response Codes für POST /restart 28
Tabelle 11: HTTP Response Codes für GET /verify 29
Tabelle 12: HTTP Response Codes für GET /status.json 29

Änderungshistorie

Revision	Datum	Bearbeiter	Kapitel	Änderungen
0001	25.04.2025	Römer, Leonhard	Alle	Erstellung
0002	12.05.2025	Römer, Leonhard	6.2	Anpassung mDNS TXT Felder
0003	26.05.2025	Kanzur, Robert	Alle	Anpassung Layout
0004	04.11.2025	Römer, Leonhard	Deckblatt	Änderung Release auf 1.1.x
			3.2	Erweiterung Konfigurationsdaten (RTU + OTA)
			5.2	Anpassung Anzahl Modbusverbindungen auf vier
			6.5	Anpassung Handhabung DHCP bei AutoIP
			7.1	Austausch Bilder Anmeldemaske Webserver
			8.3	Verallgemeinerung auf Remote Update
			7.2	Austausch Bilder und Restrukturierung Inhalt bzgl. Funktionalitäten des Frontends (Neue Funktionen: Aktivierung OTA, Mess- und Energiewerte)
0005	25.02.2026	Löber, Daniel	1.3	Setzen der Referenz auf Modbus Spezifikation 0003
			5	Detaillierung der Modbus Beschreibung
0006	12.03.2026	Kanzur, Robert	7.2.1	Anzahl an gleichzeitigen Websockets ergänzt. Aktualisierung der Dashboard-Grafik

Tabelle 1: Änderungsverfolgung

Behandlungs- und Archivierungshinweis

Dieses Dokument wird im Dokumentenmanagementsystem der TQ-Systems GmbH unter dem Namen MU100.SW.TPB.0006.docx im aktuellen Revisionsstand gespeichert.

1 Umfang des Dokuments

1.1 Zweck des Dokuments

Diese technische Produktbeschreibung spezifiziert die technischen und konfigurierbaren Eigenschaften, sowie die Produktvarianten der MU100.

1.2 Rechtlicher Hinweis

Alle innerhalb der Dokumentation genannten und ggf. durch Dritte geschützten Marken- und/oder Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind.

1.3 Referenzierte Dokumente

Referenz	Dokumententitel/-beschreibung Dokumentennummer / Dateibezeichnung	Version / Datum	Ersteller
/MBSpec/	Modbus Spezifikation der MU100 Datei: MU100.SW.SZ.Modbus.0003.pdf	0003	TQ Systems GmbH
/mDNSSpec/	Multicast DNS RFC6762 ISSN: 2070-1721	Februar 2013	S. Cheshire M. Krochmal Apple Inc.
/IPv6LinkLocalSpec/	IP Version 6 Adressing Architecture RFC 4291	Februar 2006	R. Hinden Nokia S. Deering Cisco Systems
/AutoIpSpec/	Dynamic Configuration of IPv4 Link Local Addresses	Mai 2005	S. Cheshire Apple Computer B. Aboba Microsoft Corporation
/FieldBusSpec/	DIN EN IEC 61158 Industrial communication networks – Fieldbus specification		International Electronical Comission

Tabelle 2: Referenzierte Dokumente

1.4 Verwendete Abkürzungen

Abkürzung	Benennung
CA	Certificate Authority
CSV	Comma-separated values
DDI	Direct Device Integration
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IC	Integrated Chip
MCU	Microcontroller Unit
mDNS	Multicast Domain Name System
NTP	Network Time Protocol
OTA	Over-the-Air
PRNG	Pseudorandom Number Generator
RMS	Root Mean Square
RTU	Remote Terminal Unit
SLAAC	Stateless Address Autoconfiguration
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UTC	Universal Time Coordinated

Tabelle 3: Abkürzungen

2 Hardwarefunktionen

2.1 LED-Zustände

2.1.1 LED „STATUS“

- Grün Dauerlicht: MU100 ist eingeschaltet
- Orange schnell blinkend: Firmware-Update läuft
- Rot Dauerlicht: Es ist ein kritischer Fehler aufgetreten
- Orange zweimaliges Blinken: Setzen der Werkseinstellungen via Reset-Button wurde erkannt

2.1.2 LED „NETWORK“

- Aus: Keine Verbindung
- Grün Dauerlicht: Ethernet Link ist aktiv
- Grün blinkend: Es findet eine Kommunikation über den Ethernet Link statt
- Rot blinkend: Es ist ein Fehler beim TLS-Handshake einer Modbus TLS Verbindung aufgrund der verwendeten Zertifikate aufgetreten

2.1.3 LED „SERIAL BUS“

- Aus: Es liegt keine Aktivität auf der Schnittstelle vor
- Grün blinkend: Es liegt eine reguläre Datenkommunikation vor
- Rot blinkend: Es ist ein Kommunikationsfehler bei Modbus RTU aufgetreten

2.1.4 Identifikation des Gerätes

Zur Identifikation eines Gerätes besteht die Möglichkeit dieses mittels der LEDs zu identifizieren. Alle verbauten LEDs blinken hierfür für 30 Sekunden mit einer Frequenz von 10 Hz. Diese Funktionalität kann über den Webserver angestoßen werden.

2.2 Funktionen der Reset-Taste

In den folgenden Kapiteln sind die Funktionen der Reset-Taste beschrieben.

2.2.1 Neu starten

Halten Sie die RESET-Taste mit einem spitzen Gegenstand etwas länger als 10 Sekunden gedrückt.

2.2.2 Zurücksetzen auf Werkseinstellung

Halten Sie die RESET-Taste mit einem spitzen Gegenstand kurz (<0,5 Sekunden) und innerhalb 1 Sekunde ein zweites Mal zwischen 3 und 5 Sekunden gedrückt, um das Gerät auf Werkseinstellung zurück zu setzen. Bei erfolgreicher Eingabe blinkt die Status LED zweimal orange. Bei einer falschen Eingabe muss 2 Sekunden gewartet werden, bevor ein neuer Eingabeversuch getätigt wird.

Für weitere Informationen bzgl. des Zurücksetzens auf Werkseinstellungen siehe Kapitel 3.2.

3 Geräteeinstellung

3.1 Einstellungen über Webserver

Voraussetzung für die Konfiguration über den Webserver ist dessen Aktivierung zum Produktionszeitpunkt. Die Einstellung des Gerätes über den Webserver wird in Kapitel 7.2.4 näher beschrieben.

3.2 Werkseinstellung

Nach einem erfolgreichen Zurücksetzen auf Werkseinstellung werden folgende Parameter auf den Auslieferungszustand zurückgesetzt:

Parameterfamilie	Parameter
Netzwerkeinstellungen	Statische IP
	Netzwerkmaske
	Default Gateway
	IPv6 aktiv
	DHCP aktiv
Messen	Messintervall
Modbus	Modbus RTU aktiv
	Modbus RTU Baudrate
	Modbus RTU Unit ID
	Modbus RTU Parität
	Modbus RTU Stopbits
	Modbus TLS aktiv
NTP	NTP-Serveradresse
OTA	OTA-Update aktiv

Tabelle 4: Konfiguration Werkseinstellung

Für das Messintervall wird dabei das kundenspezifische Messintervall (Default) verwendet.

Für die notwendige Tastenkombination für das Zurücksetzen auf Werkseinstellungen siehe Kapitel 2.2.2.

4 Datenerfassung

Nachdem das Gerät mit Spannung versorgt wird, sind die Messwerte spätestens nach 7 s verfügbar. Ein Neustart per Webserver oder Taster führt nicht zu dieser Verzögerung.

4.1 Messwerte

Für den Messvorgang werden die folgenden Messintervalle unterstützt:

- 100 ms
- 200 ms
- 500 ms
- 1000 ms

Folgende Daten werden von der MU100 berechnet und können über Modbus abgefragt werden. Die Energiewerte werden saldierend erfasst.

- Gesamt Wirkleistung | Total Active Power
- Gesamt Blindleistung | Total Reactive Power
- Gesamt Scheinleistung | Total Apparent Power
- Gesamt importierte Wirkarbeit | Total Imported Energy
- Gesamt exportierte Wirkarbeit | Total Exported Energy
- Gesamt induktive Blindarbeit | Total Inductive Energy
- Gesamt kapazitive Blindarbeit | Total Capacitive Energy
- Gesamt importierte Scheinarbeit | Total Imported Apparent Energy
- Gesamt exportierte Scheinarbeit | Total Exported Apparent Energy
- Leistungsfaktor | Total Power Factor
- Frequenz | Frequency
- Spannungen zwischen den Phasen | Voltages between phases

Für jede der drei Phasen werden folgende Messwerte ermittelt.

- Strom | RMS Current
- Spannung | RMS Voltage
- Wirkleistung | Active Power
- Blindleistung | Reactive Power
- Scheinleistung | Apparent Power
- Importierte Wirkarbeit | Imported Energy
- Exportierte Wirkarbeit | Exported Energy
- Induktive Blindarbeit | Inductive Energy
- Kapazitive Blindarbeit | Capacitive Energy
- Importierte Scheinarbeit | Imported Apparent Energy
- Exportierte Scheinarbeit | Exported Apparent Energy
- Leistungsfaktor | Power Factor

4.2 Fehlerspeicher

Für den Servicefall werden kritische Systemfehler und Warnungen persistent in der MU100 gesichert. Diese können in einem Servicefall von der TQ-Systems GmbH oder über das Webserver Frontend durch den Kunden ausgelesen werden.

4.3 Ereignisspeicher

Wie für den Fehlerspeicher werden im Ereignisspeicher wichtige Ereignisse im Systemablauf protokolliert. Diese können ebenfalls in einem Servicefall von der TQ-Systems GmbH oder über das Webserver Frontend durch den Kunden ausgelesen werden.

5 Modbus-Schnittstelle

Im Folgenden werden die Funktionalität, die Betriebsmodi, sowie die Modbus Registerspezifikation beschrieben. Eine detaillierte Beschreibung des Modbus Protokolls und seiner Funktionsweise ist in der Modbus-Spezifikation zu finden (siehe www.modbus.org). Modbus TCP ist Teil der IEC 61158 Norm (siehe /FieldBusSpec/).

Die Modbus Datenschnittstelle kann in folgenden Betriebsmodi verwendet werden:

- Modbus RTU Slave
- Modbus TCP Server
- Modbus TCP Server TLS gesichert

Für Informationen über das OBIS-Kennzahlen-System und einer Modbus Registerübersicht siehe /MBSpec/.

5.1 Modbus RTU

Die MU100 agiert als Modbus Slave.. Dafür verfügt die MU100 über eine RS-485 Schnittstelle, welche über eine einfache Buchse nach Außen geführt ist.

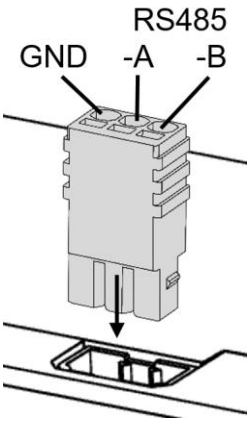

Abbildung 1: Modbus Anschluss

Details zum Anschluss an die RS-485 Buchse und der Verpolung der Schnittstelle finden Sie in der Installationsanleitung.

Die Baudrate, Parität, die Anzahl der Stoppbits und die Modbus Slave ID lässt sich geräteabhängig während der Produktion vorkonfigurieren. Während des Betriebes ist eine Einsicht und Anpassung der genannten Parameter über die Webschnittstelle (siehe Kapitel 7.2.4) und durch Zugriff auf die Konfigurationsregister über Modbus RTU (siehe /MBSpec/) möglich.

5.1.1 Terminierung

In Abhängigkeit der Leitungslänge und der Anzahl an Teilnehmern auf dem Bus, ist es empfehlenswert den Bus an beiden Enden mit einem 120 Ohm Widerstand zu terminieren. Durch die Terminierung werden Reflexionen in der Verbindung reduziert. Dies kann unter Umständen für die Zuverlässigkeit der Anwendung zwingend erforderlich sein und Übertragungsfehler vermeiden.

5.1.2 Idle-line Failsafe

Die Gegenstelle des RS-485 Buses muss sicherstellen, dass jederzeit ein definierter Pegel auf dem Bus anliegt, auch wenn sich alle Treiber im passiven Zustand befinden.

Für den Betrieb der MU100 an einem Bus muss die Idle-line Failsafe durch die Gegenstelle oder extern sichergestellt werden.

5.2 Modbus TCP

Der Modbus TCP Server wird über Port 502 zur Verfügung gestellt. Der Client muss zwingend die Unit ID der MU100 bei Lesebefehlen mitschicken. Die Unit ID ist für die MU100 immer 1. Der Zugriff über Modbus TCP erfolgt ausschließlich lesend mittels Function Code 0x03 Read Holding Registers.

Es werden maximal vier gleichzeitige Modbus TCP Verbindungen unterstützt. Bei Verwendung von IPv6 kann Modbus TCP auch über die IPv6 Adresse angesprochen werden.

5.3 Modbus TCP mit TLS

Optional kann die Verbindung mit dem Modbus TCP Server mittels TLS gesichert werden. Dies kann während der Produktion vorkonfiguriert werden. Bei aktiviertem TLS startet der Server auf Port 802 und erwartet einen TLS-Handshake bevor eine Modbus TCP Kommunikation möglich ist. Port 502 für ungesichertes Modbus TCP lehnt alle Verbindungsversuche ab.

Zur Verwendung von Modbus TLS ist ein gültiges Zertifikat für den Client notwendig, um Daten über Modbus auslesen zu können. Ist das Zertifikat ungültig, wird die Verbindung während des TLS-Handshakes abgebrochen und das Gerät quittiert einen solchen Versuch mit einer rot blinkenden Ethernet LED. Ein Auslesen über die unverschlüsselte Schnittstelle an Port 502, wenn gleichzeitig TLS aktiv ist, führt ebenfalls zu einer rot blinkenden Ethernet LED.

Durch die Verwendung von Zertifikaten ist es möglich die Gegenstelle zu verifizieren.

Folgende Funktionen lassen sich zum Produktionszeitpunkt aktivieren:

- Verifikation des Clients mittels Zertifikats einer vertrauenswürdigen CA. Dafür muss das Zertifikat der CA im Gerät hinterlegt werden. Falls die Verifikation deaktiviert ist, werden Clients ohne Zertifikat akzeptiert. Sollten diese dennoch ein Zertifikat übermitteln wird dieses nicht gegen eine CA geprüft, wenn es die übrigen Validierungsschritte besteht.
- Validierung der zeitlichen Gültigkeit des Zertifikats des Clients. Der Gerätebetreiber muss sicherstellen, dass in diesem Fall das Gerät Zugriff zu einem synchronisierten NTP-Server hat, damit die Geräteuhr der tatsächlichen Zeit entspricht.

6 Netzwerk

Neben der Netzwerkkonfiguration unterstützt die MU100 verschiedene Protokolle und Mechanismen, die in diesem Kapitel näher beschrieben werden. Sofern nicht anders angegeben, bezieht sich die IP-Adresse auf IPv4. IPv6 wird als optionales Feature gesondert behandelt.

6.1 Netzwerkkonfiguration

Die Netzwerkkonfiguration erfolgt über den Webserver. Dabei können folgende Parameter eingestellt werden:

Parameter	Werte	Bemerkungen
Statische IP-Adresse	Vier Bytes (0-255), ein Byte für jedes Oktett der IP-Adresse	wird verwendet, wenn DHCP ausgeschaltet ist
Subnetzmaske	Vier Bytes (0-255), ein Byte für jedes Oktett der Subnetzmaske	wird verwendet, wenn DHCP ausgeschaltet ist
Default Gateway	Vier Bytes (0-255), ein Byte für jedes Oktett der IP-Adresse	wird verwendet, wenn DHCP ausgeschaltet ist
IPv6	IPv6 aktiv/nicht aktiv 0: IPv6 nicht aktiv 1: IPv6 aktiv	kann mit IPv4 gleichzeitig im Dual Mode betrieben werden
DHCP	DHCP aktiv/nicht aktiv 0: DHCP nicht aktiv 1: DHCP aktiv	

Tabelle 5: Parameter der Netzwerkkonfiguration

Die Einstellungen werden erst nach Neustart des Gerätes aktiv. Dies geschieht entweder nach erfolgreicher Konfiguration am Webserver oder durch einen manuellen Neustart des Gerätes in der "Device Information" Webpage des Webservers.

Die Default-Werte für die Netzwerkkonfiguration können OEM spezifisch parametriert werden.

6.2 mDNS

Für das Auffinden im Netzwerk unterstützt jede MU100LR und MU100LR+ mDNS. Für die mDNS Spezifikation siehe /mDNSSpec/

Die MU100 bietet die Service Typen `_mbap._tcp` und `_http._tcp` in der Applikation an. *_http._tcp* ist dabei nur aktiv, wenn der Webserver eingeschaltet ist. Beide mDNS Dienste finden sich unter dem Instanznamen *Produktname-Seriennummer*. Des Weiteren bieten beide Service Typen im Textfeld einen generischen Teil zur eindeutigen Identifikation des Gerätes.

Der Aufbau stellt sich wie folgt dar:

```
manufacturer=<Hersteller>
type="Metering Unit"
model=<Produktname>
mac=<MAC>
software=<SW Version>
serial=<Seriennummer>
txtvers=1
```

Als zusätzliche Information ist dem `_mbap._tcp` die Unit ID in folgender Form angehangen:

```
unitid=1
```

6.3 TCP Keepalive

Es ist ein TCP Keepalive Mechanismus implementiert, der dazu dient, nicht ordnungsgemäß geschlossene Verbindungen zu erkennen und zu schließen.

Der Mechanismus wird dabei OEM spezifisch implementiert und wird durch drei Parameter konfiguriert:

- Idle Intervall
- Intervall zwischen zwei Anfragen
- Anzahl an Anfragen

Der erste Parameter bezeichnet dabei die Zeitperiode wie lange eine Verbindung inaktiv sein darf, bevor ein erstes TCP Keepalive Paket an die Gegenstelle verschickt wird. Falls die Verbindung inaktiv ist und die Gegenstelle erreichbar ist, wird das Paket quittiert und der Timer zurückgesetzt. Sollte die Gegenstelle nicht erreichbar sein oder die Verbindung inaktiv werden, wird entsprechend dem dritten Parameter eine bestimmte Anzahl von TCP Keepalive Paketen versendet. Hierbei ist zu beachten, dass bereits das erste Paket bei der Anzahl berücksichtigt wird. Der Zeitabstand zwischen den Paketen wird durch den zweiten Parameter konfiguriert. Antwortet die Gegenstelle auf keines der Pakete, wird die Verbindung seitens der MU100 geschlossen.

6.4 IPv6

Neben der IPv4 Schnittstelle bietet die MU100 IPv6 als optionale Schnittstelle an. Diese kann in der Konfiguration aktiviert werden. IPv4 und IPv6 können nebeneinander betrieben werden. Anders als IPv4 kann IPv6 nur in Zusammenhang mit DHCPv6 betrieben werden. Die Verwendung von SLAAC wird derzeit nicht unterstützt.

Bei Verwendung von IPv6 erhält das Gerät sowohl eine globale als auch eine lokale Adresse. Diese haben unterschiedliche Gültigkeitsbereiche, für weitere Informationen siehe/IPv6LinkLocalSpec/. Damit lässt sich das Gerät über IPv6 mit verschiedenen Adressen ansprechen.

Aufgrund der Dual Stack Unterstützung können alle Netzwerkschnittstellen des Gerätes auch mit IPv6 verwendet werden.

6.5 Auto IP

Wenn DHCP-Anfragen innerhalb von 10 Sekunden unbeantwortet bleiben, vergibt die MU100 automatisch eine lokal gültige IP-Adresse aus dem Adressbereich 169.254.0.0/16. Währenddessen sendet die MU100 alle 60 Sekunden eine weitere DHCP-Anfrage. Erhält das Gerät infolge einer solchen Anfrage eine gültige DHCP-Adresse, wird die verwendete Auto IP Adresse durch die DHCP-Adresse ersetzt.

Die IP wird mithilfe eines Pseudozufallszahlengenerators (PRNG) erzeugt und basiert nicht auf gerätespezifischen Parametern.

Weitere Informationen zu AutoIP finden sich in der Spezifikation /AutoIpSpec/.

6.6 SNTP und Offline Timebasis

SNTP wird in der MU100 einerseits zur Echtzeiterfassung des Ereignisspeichers und andererseits zur Zertifikatsvalidierung für Modbus TLS und des Remoteupdates verwendet.

Die MU100 schickt alle zwölf Stunden SNTP-Anfragen an den hinterlegten NTP-Server in der Gerätekonfiguration. Anhand der Systemzeit und dem letzten NTP-Zeitstempel kann der aktuelle Zeitpunkt errechnet werden. Wird eine SNTP Anfrage durch den Server nicht beantwortet, wird der zuletzt empfangene Zeitstempel verwendet. Ist der NTP-Server seit Systemstart nicht verfügbar, wird die Offline Timebasis des Systems verwendet. Dabei wird sowohl der Kompilierungszeitpunkt der Software als auch das Produktionsdatum des Gerätes berücksichtigt und der aktuellere Zeitpunkt zusammen mit der Systemlaufzeit verwendet.

7 Webserver

Zum Produktionszeitpunkt kann der Webserver im Gerät aktiviert werden. Eine nachträgliche Aktivierung, bzw. Deaktivierung im Feld ist nicht möglich.

Der Zugang zum Webserver erfolgt über HTTPS an Port 443. Anfragen über HTTP an Port 80 werden umgeleitet als HTTPS Anfragen an Port 443.

Nachfolgend wird primär die Bedienung des Frontend betrachtet. Aktionen aus dem Frontend werden dabei über REST API Routen im Backend abgebildet, die Dokumentation der REST API Routen erfolgt in Kapitel 8.2.

Die in diesem Kapitel beschriebenen Funktionen wurden mit folgenden Browsern getestet:

- Google Chrome - Version 134.0.6998.89
- Microsoft Edge - Version 134.0.3124.72

7.1 Autorisierung und Nutzerberechtigungen

Bevor ein Update oder eine Konfiguration des Gerätes durchgeführt werden kann, muss sich der Benutzer am Webserver autorisieren. Dabei benötigt dieser neben einem Nutzernamen auch ein Passwort. Initial wird die MU100 mit einem generierten Passwort (siehe Beilagenetikett) für den Benutzer „admin“ geliefert.

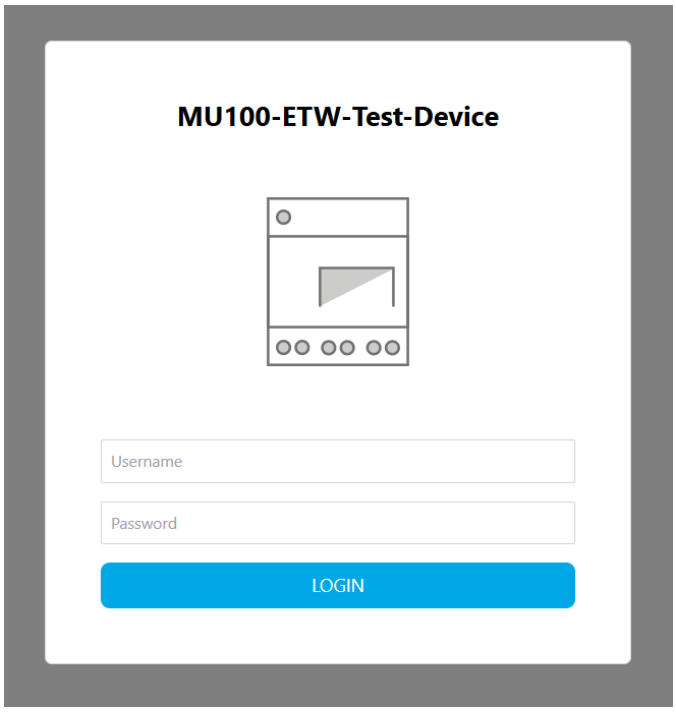

Abbildung 2: Anmeldebildschirm Webserver

Nach Eingabe der IP-Adresse des Gerätes im Browser öffnet sich die Anmeldeoberfläche des Gerätes (siehe hierzu Abbildung 2). Auf dieser muss der Nutzername und das Passwort eingegeben werden, bei erfolgreicher Anmeldung wird der Nutzer auf die Webpage der Gerätekonfiguration umgeleitet. Im Falle eines fehlerhaften Anmeldeversuches erfolgt die Ausgabe einer Fehlermeldung (siehe Abbildung 3).

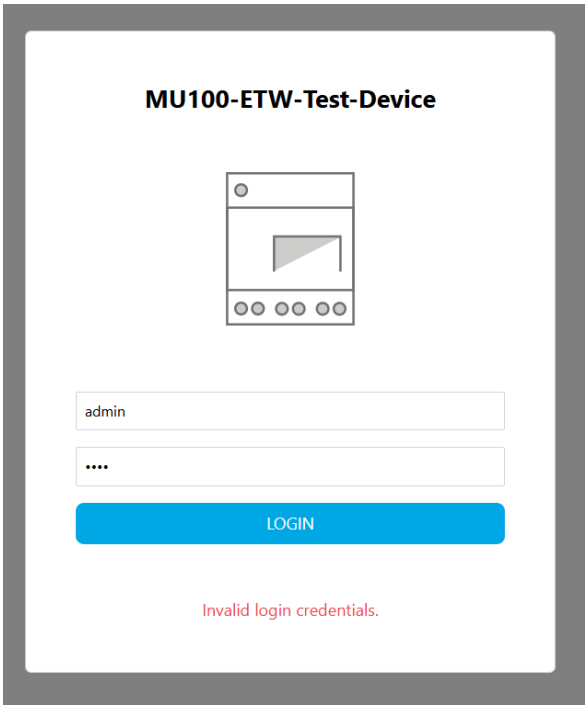

Abbildung 3: Fehlgeschlagene Autorisierung Webserver

Im Falle einer erfolgreichen Anmeldung wird im Backend eine Session für den autorisierten Nutzer erstellt. Diese Session wird durch den Cookie *mu100* gekennzeichnet, welcher an das Frontend zurückgemeldet wird. Dieser muss in allen nachfolgenden Anfragen verwendet werden. Ohne gültigen Cookie werden alle Anfragen, ausgenommen hiervon sind Anfragen zur Anmeldung und Abfrage einer gültigen Session, mit HTTP Status Code 401 (Unauthorized) beantwortet. Eine gültige Session ist zeitlich durch ein Timeout begrenzt, erfolgt innerhalb dieser Zeitdauer keine weitere Interaktion mit dem Backend wird die Session als ungültig erkannt und Zugriffe auf das Backend als unautorisiert gekennzeichnet. Die maximale Zeitdauer einer Session kann OEM spezifisch parametriert werden.

Werden fünf Fehlversuche bei der Anmeldung unternommen, wird der Nutzer für 10 Sekunden gesperrt, bei weiteren Fehlversuchen erhöht sich die Sperrdauer. In dieser Zeit werden alle Anmeldeversuche für diesen Nutzer abgeblockt.

7.2 Funktionen des Webserver Frontend

Im Nachfolgenden werden die einzelnen Funktionalitäten des Frontend des Webservers beschrieben.

7.2.1 Dashboard

Nach erfolgreicher Autorisierung am Gerät wird die Startseite bzw. das Dashboard des Gerätes dargestellt. Eine beispielhafte Darstellung findet sich in Abbildung 4.

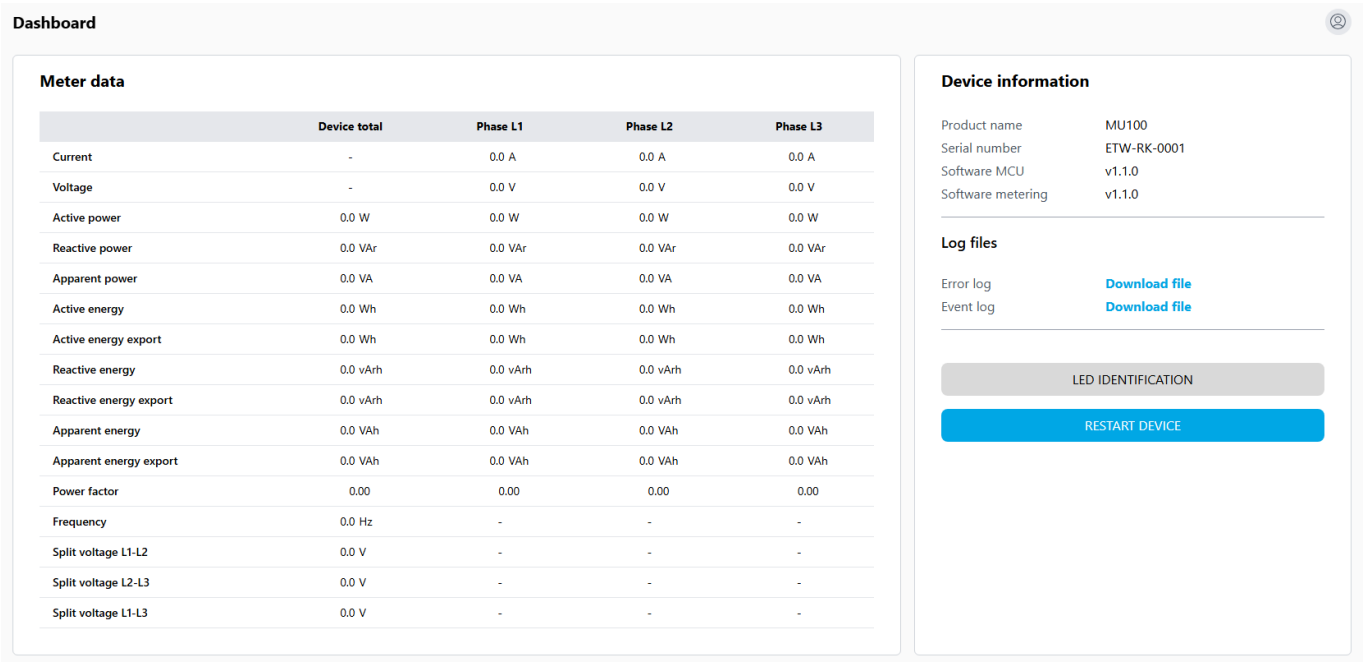

Abbildung 4: Dashboard des Webservers

Mess- und Energiewerte

Auf der linken Seite werden die aktuellen Mess- und Energiewerte des Geräts ausgegeben. Diese teilen sich dabei auf in allgemeine und phasenspezifische Werte. Ihre Ausgabe erfolgt normiert auf die geläufigen Strom-, Spannungs-, Leistungs- oder Energieeinheiten. Die Daten werden fortlaufend mittels Websocket ausgelesen und im Frontend alle zwei Sekunden aktualisiert.

Es werden maximal zwei gleichzeitige Websocket-Verbindungen unterstützt. Bei einer weiteren Verbindung wird die älteste Verbindung automatisch geschlossen.

Geräteinformationen

Auf der rechten Seite werden bestimmte gerätespezifische Informationen im Abschnitt „Device information“ dargestellt. Neben dem Produktnamen und der Seriennummer des Geräts werden auch die aktuellen Versionen der MCU und des Metering ICs angezeigt.

Logging

Unter dem Abschnitt „Log files“ ist es möglich, das Log des bereits in Kapitel 4.2 beschriebene Fehlerspeichers oder des Eventspeichers aus Kapitel 4.3 auszulesen. Eine Logdatei wird dabei als CSV-Datei (Semikolon als Trennzeichen) bereitgestellt.

LED Identifikation

Der Button "LED Identification" dient zum Anstoßen der gleichnamigen Aktion auf dem Gerät. Für die Beschreibung des Verhaltens siehe Kapitel 2.1.4.

Geräteneustart

Der Button "Restart Device" dient zum Ausführen eines Geräteneustartes. Durch den Neustart des Gerätes erlischt auch die gültige Session des Nutzers und dieser wird auf die Login Page des Webservers weitergeleitet.

7.2.2 Manuelle Updatefunktionalität

Nach Auswahl der Seite "Update" in der Sidebar öffnet sich die Webpage wie in Abbildung 5 zu sehen.

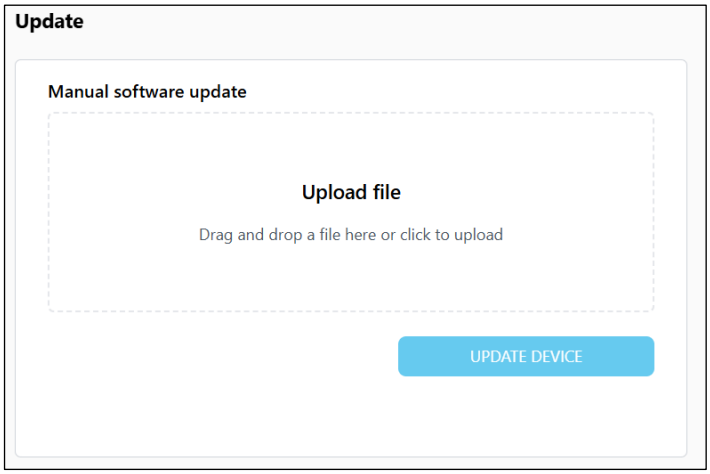

Abbildung 5: Updateseite

Über Drag-and-Drop auf die Schaltfläche "Upload File" oder das Klicken auf die Schaltfläche kann eine Updatedatei geladen werden. Nach erfolgreicher Auswahl einer Updatedatei, wird der Button "Update Device" verfügbar. Nach Betätigung des Buttons öffnet sich ein Pop-Up Fenster wie im linken Bild in Abbildung 6.

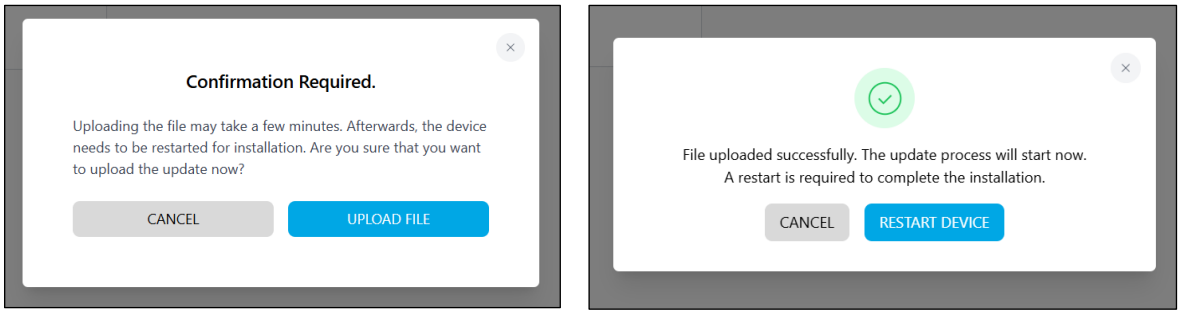

Abbildung 6: Pop-Up Fenster während erfolgreichem Update

Mit dem Button "Upload File" wird der Updateprozess gestartet. Während des Updates blinkt die Status LED der MU100 orange und der Webserver zeigt einen Ladebildschirm an. Nach erfolgreichem Update zeigt der Webserver ein Pop-Up Fenster wie im rechten Bild von Abbildung 6. Nach Betätigung des Buttons "Restart Device", startet das Gerät neu und der Anwender wird auf den Login weitergeleitet.

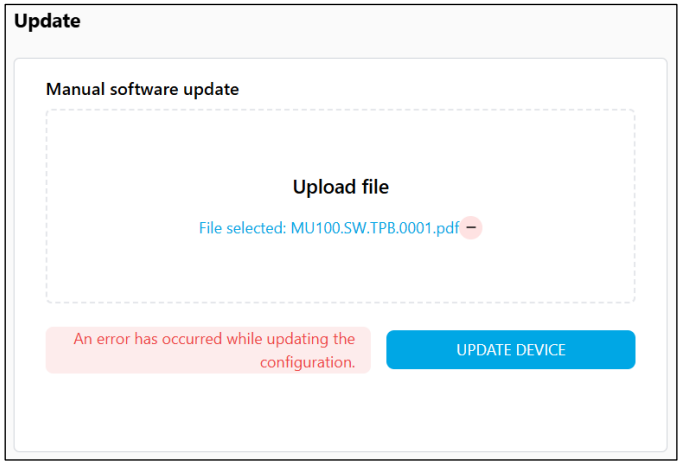

Abbildung 7: Fehlgeschlagenes Update über Webserver

Sollte das Update fehlschlagen, wird eine Fehlernachricht entsprechend Abbildung 7 angezeigt. Das Gerät befindet sich hierbei wieder im Ausgangszustand. Der Updateprozess kann erneut gestartet werden.

7.2.3 OTA-Updatefunktionalität

Nach Auswahl der Seite "Update" in der Sidebar des Webservers kann neben dem manuellen Update auch Informationen bezüglich der OTA-Updatefunktionalität ausgelesen werden bzw. diese aktiviert werden. Voraussetzung hierfür ist, dass diese in den Produktionsdaten aktiviert wurde

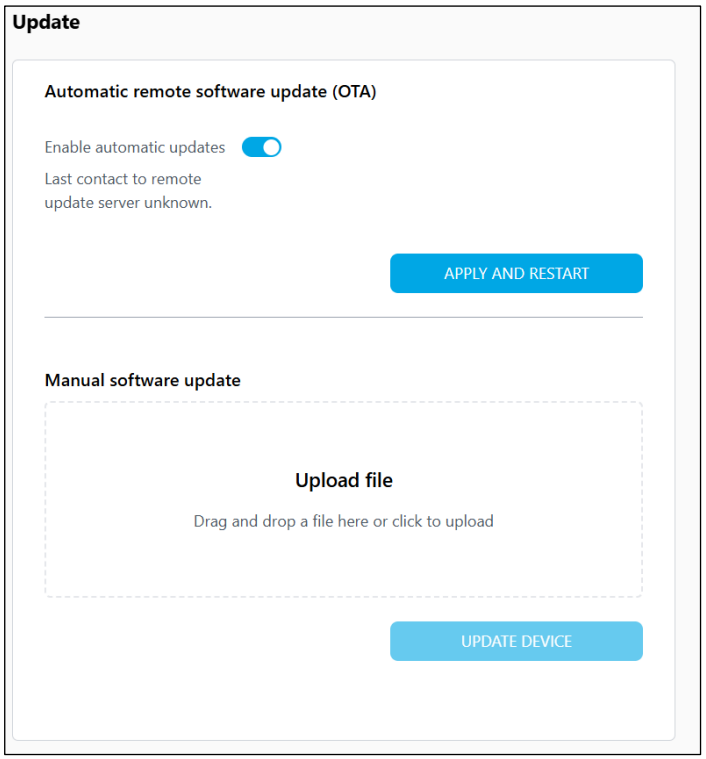

Abbildung 8: Manuelle und OTA Updatefunktionalität

Wie in Abbildung 8 zu sehen, kann die OTA-Funktionalität über einen Button aktiviert oder deaktiviert werden. Damit die Anpassung auf dem Gerät wirksam wird, muss der in der Abbildung gezeigte Button "Apply and Restart" betätigt werden, dieser startet das Gerät nach erfolgreicher Konfiguration neu. Der Nutzer wird aus der Weboberfläche ausgeloggt.

Bei aktivierter OTA-Funktionalität wird zusätzlich der Zeitstempel des letzten Kontakts zum OTA-Server angezeigt. Liegt kein gültiger Zeitstempel vor, erfolgt die Meldung „Last contact to remote update server unknown“. Beim Zeitstempel ist zu beachten, dass dieser als UTC-Zeitstempel bereitgestellt wird.

7.2.4 Gerätekonfiguration

Nach erfolgreicher Autorisierung am Gerät, kann in der Sidebar der Reiter „Settings“ ausgewählt werden. Auf dieser Seite können verschiedene Parameter des Gerätes angepasst werden, siehe hierzu Abbildung 9. Für Informationen zu der Netzwerkkonfiguration siehe Kapitel 6.1. Bestimmte Parameter wie IPv6 und TLS sind nur sichtbar, wenn diese in den Produktionsdaten als konfigurierbar gesetzt wurden.

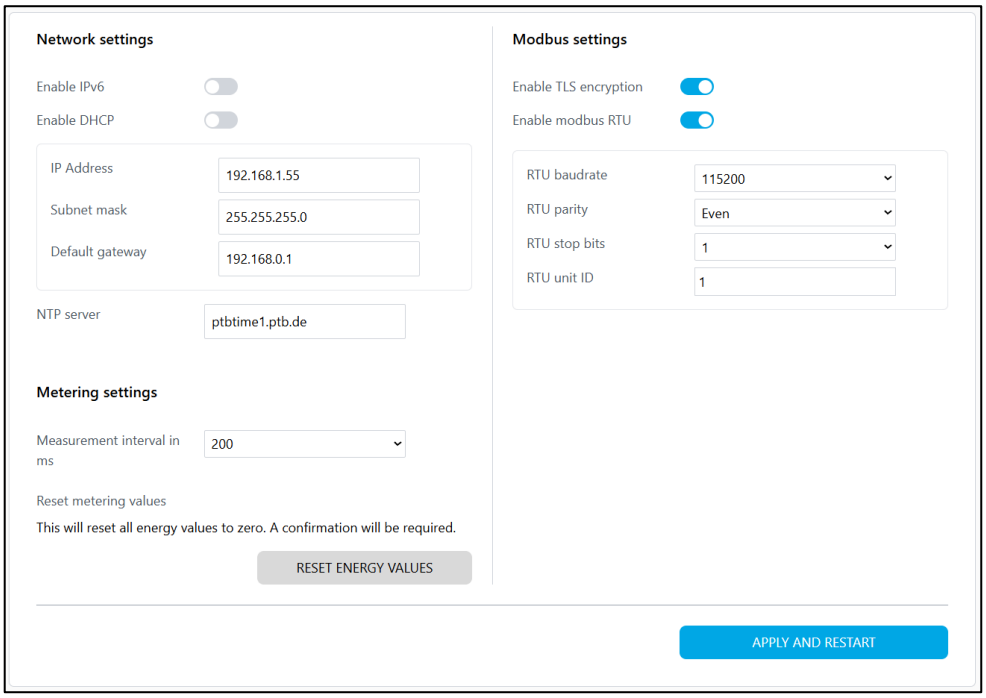

Abbildung 9: Gerätekonfiguration über Frontend des Webservers

Bei Aktivierung von DHCP werden die Felder für IP-Adresse, Subnetzmaske und Default Gateway ausgegraut und es wird die stattdessen die aktuelle Konfiguration der Netzwerkschnittstelle angezeigt. Wird Modbus RTU deaktiviert, werden auch hier die Felder für die Baudrate, die Parität, die Anzahl der Stopbits sowie der Unit ID ausgegraut und können nicht mehr angepasst werden.

Der NTP-Server dient zur Abfrage des aktuellen Zeitpunktes durch Verwendung des SNTP-Protokolls. Hierbei kann sowohl eine IP-Adresse als auch eine Domain verwendet werden. Für weitere Informationen siehe Kapitel 6.6.
Damit eine Konfiguration auf dem Gerät wirksam wird, muss der in der Abbildung gezeigte Button "Apply and Restart" betätigt werden, dieser startet das Gerät nach erfolgreicher Konfiguration neu. Der Nutzer wird aus der Weboberfläche ausgeloggt. Neben dem „Apply and Restart“ Button wird auch ein zweiter Button namens „Reset Energy Values“ bereitgestellt. Mithilfe dieses Buttons können die Energiewerte des Gerätes auf null zurückgesetzt werden.

7.2.5 Logout

Über den Button "Logout" in der oberen rechten Ecke kann der aktuelle Nutzer am Webserver abgemeldet werden. Die aktuelle Session wird als invalide gekennzeichnet.

8 Update

Abhängig von der Modelvariante wird ein manuelles Update über das Webserver Frontend bzw. HTTPS und optional eine automatische Remote Updatefunktionalität unterstützt.

Die OTA-Updatefunktionalität kann mittels Webserver aktiviert werden.

8.1 Manuelles Update über Webserver Frontend

Die Updatefunktionalität im Webserver-Frontend ist nur verfügbar, wenn der Webserver zum Produktionszeitpunkt aktiviert wurde. Die Vorgehensweise bei Durchführung eines Updates ist in Kapitel 7.2.1 beschrieben.

8.2 Manuelles Update über HTTPS Schnittstelle

Die HTTPS Schnittstelle ist nur verfügbar, wenn der Webserver aktiviert ist.

8.2.1 Programmablaufplan

Abbildung 10 zeigt den Ablauf des Updatevorgangs.

8.2.2 Beschreibung HTTP Update

Im Folgenden wird der Updateprozess stichpunktartig beschrieben:

- Ist eine valide Applikation vorhanden, wird diese gestartet nachdem die MU100 mit Strom versorgt wird.
- Falls keine valide Applikation vorhanden ist, gilt das Gerät als defekt. Es sind keine Schnittstellen verfügbar und die LEDs sind inaktiv.
- Um sicherzustellen, dass der Webserver erreichbar ist, kann jederzeit ein GET-Request auf */status.json* ausgeführt werden. Dieser wird bei fehlender Autorisierung mit HTTP Status Code 401 beantwortet.
- Um sich am Webserver zu autorisieren, muss eine Anmeldung mittels POST auf /authorize mit dem Usernamen und Passwort als Payload durchgeführt werden. Ohne gültige Autorisierung werden die Updaterouten */prepare, /upload, /verify, /retry and /status.json* mit HTTP Status Code 401 beantwortet.
- Bei einer erfolgreichen Autorisierung wird ein Cookie für die valide Session generiert, welcher bei allen nachfolgenden Anfragen zwingend verwendet werden muss, um sich erfolgreich am Webserver zu authentifizieren.
- Vor dem Übertragen der Updatedatei muss ein POST Request auf /prepare ausgeführt werden. Dieser Request dient dazu, das Gerät in den Updatemodus zu versetzen und den internen Speicher vorzubereiten. In diesem Fall können andere autorisierte Nutzer nicht auf REST Routen des Webservers zurückgreifen; Anfragen werden mit HTTP Status Code 403 Forbidden beantwortet. Der aktuelle User kann in diesem Zustand ausschließlich auf */prepare, /upload, /verify, /retry, /getAuth* und */status.json* zugreifen. Alle anderen Anfragen werden mit HTTP Status Code 403 Forbidden beantwortet.
- Wird der POST Request auf /prepare mit HTTP Status Code 403 beantwortet, besitzt der Nutzer keine Berechtigungen zum Durchführen eines Updates oder es wird bereits ein Update durchgeführt.
- Das Übertragen der Updatedatei erfolgt mit dem POST-Request auf /update. Die Datei muss mit dem FormData Interface übertragen werden.
- Sollte die Übertragung erfolgreich sein, kann mit einem GET Request auf /verify die Korrektheit des Updates überprüft werden. Liefert der GET Request auf /verify HTTP Status

Code 403 trotz durchgeführtem Update besitzt die neue Firmware eine ältere Version als die aktuelle Firmware. Dies ist für die MU100 nicht erlaubt.

- Bei einem fehlgeschlagenen Update muss ein POST Request auf /retry ausgeführt werden, bevor der Updatevorgang erneut gestartet werden kann.
- Erfolgt kein POST Request auf /retry bei einem laufenden bzw. gescheiterten Update verbleibt der Webserver im Updatemodus bis zum Ablauf der Session des Nutzers, welcher ein Update angestoßen hat.

8.2.3 Bereitgestellte REST Routen für Updatevorgang

Die nachfolgenden Abschnitte beschreiben die verfügbaren URLs, welche für den Updatevorgang notwendig sind.
Eine Beschreibung der HTML-Dateien, welche der Webserver zur Verfügung stellt, wird nicht beschrieben, da diese für die Erstellung eines Clients nicht relevant sind.

Sollte eine nicht verfügbare URL aufgerufen werden wird der HTTP Status Code 404 zurückgegeben.

POST /authorize

Die Anfrage dient zum Login des Nutzers und erzeugt eine valide Sitzung für den Nutzer. Diese ist notwendig für die Interaktion mit anderen REST Routen. Die JSON im Anfragebody enthält den Nutzername ("user") und das Passwort ("pwd"). Die MU100 liefert bei einer erfolgreichen Autorisierung den Cookie *mu100* zurück.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Autorisierung an der MU100 wurde erfolgreich durchgeführt. Es wird eine gültige Session mit dazugehörigem Cookie *mu100* erzeugt.
	HTTP Code 400 - Bad Request	Autorisierung ist fehlgeschlagen
	HTTP Code 403 - Forbidden	Autorisierung an der MU100 ist derzeit nicht möglich

Tabelle 6: HTTP Response Codes für POST /authorize

POST /prepare

Mit der /prepare Methode wird die MU100 auf ein Update vorbereitet. Die MU100 wechselt in den Zustand "Prepare" nachdem der Request empfangen wurde. In diesem Zustand werden alle Anfragen an den Webserver, die nicht Teil des Updateprozesses sind mit HTTP Status Code 403 Forbidden beantwortet.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	MU100 wurde auf Update vorbereitet und wechselt in den Zustand "Prepared"
	HTTP Code 400 - Bad Request	Start des Updatevorganges auf der MU100 ist derzeit nicht möglich
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät
	HTTP Code 403 - Forbidden	Nutzer besitzt nicht die ausreichenden Berechtigungen um ein Update zu starten

Tabelle 7: HTTP Response Codes für POST /prepare

POST /upload

Mit der /upload Methode werden die Daten der Updatedatei übertragen. Es wird empfohlen das FormData Interface dafür zu verwenden. Für ein erfolgreiches Update muss sich das Gerät im Zustand "Prepare" befinden.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Updatefile wurde hochgeladen, Gerät befindet sich im Zustand "In Progress"
	HTTP Code 400 - Bad Request	Folgende Möglichkeiten bestehen: ▪ Die MU100 befindet sich nicht im Zustand "Prepared" ▪ Es wurde keine Updatedatei übertragen ▪ Die übertragene Updatedatei hat während des Transfers zu einem Fehler geführt
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät
	HTTP Code 403 - Forbidden	Das Gerät befindet sich entweder nicht im Updatezustand und/oder User besitzt keine ausreichenden Rechte ein Update durchzuführen

Tabelle 8: HTTP Response Codes für POST /upload

POST /retry

Diese Anfrage veranlasst die MU100 den Updatezustand zu verlassen. Um diesen verlassen zu können, muss der User vorher selbstständig das Gerät in den Updatezustand versetzen und muss eine gültige Session besitzen. Zudem muss der Nutzer mindestens Rechte als Servicepersonal besitzen. Das Gerät muss sich entweder im Zustand "Prepared", "In Progress" oder „Error“ befinden.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Updatezustand wurde verlassen. Das Gerät befindet sich nun im Updatezustand „Idle“
	HTTP Code 400 - Bad Request	Folgende Möglichkeiten bestehen: ▪ Die MU100 befindet sich nicht im Zustand "Prepared", „In Progress“ oder „Error“ ▪ Das Update konnte trotz Abbruchbefehl nicht abgebrochen werden
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät
	HTTP Code 403 - Forbidden	Das Gerät befindet sich entweder nicht im Updatezustand und/oder User besitzt keine ausreichenden Rechte ein Update durchzuführen

Tabelle 9: HTTP Response Codes für POST /retry

POST /restart

Diese Anfrage veranlasst die MU100 zu einem Neustart

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Updatezustand wurde verlassen. Das Gerät befindet sich nun im Updatezustand „Idle“
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät
	HTTP Code 403 - Forbidden	Es wird gegenwärtig ein Update durchgeführt

Tabelle 10: HTTP Response Codes für POST /restart

GET /verify

Mit der /verify Methode kann der Erfolgsstatus eines durchgeführten Updates abgefragt werden. Zu Beginn der Anfrage ist der Updatezustand entweder „In Progress“ oder „Success“.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Update ist erfolgreich durchgelaufen. Updatezustand ist nun „Idle"
	HTTP Code 400 - Bad Request	Das Update ist entweder fehlgeschlagen oder noch nicht durchgelaufen
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät
	HTTP Code 403 - Forbidden	Folgende Möglichkeiten bestehen: ▪ Gerät befindet sich nicht im Updatezustand ▪ Nutzer besitzt keine ausreichenden Berechtigungen ▪ Übertragene Firmware besitzt eine niedrigere Version als die aktuelle Firmware

Tabelle 11: HTTP Response Codes für GET /verify

GET /status.json

Die Methode /status.json wird verwendet, um den internen Status des Updatehandlers abzufragen. Im Falle einer erfolgreichen Abfrage des Zustandes, enthält die Response den Json Key „status“, welcher die Zustandsinformation enthält.

Format	Rückgabewert	Beschreibung
HTTP Response Code	HTTP Code 200 - Status OK	Status konnte erfolgreich abgefragt werden
	HTTP Code 401 - Unauthorized	Zugriff erfolgte ohne vorherige Autorisierung am Gerät

Tabelle 12: HTTP Response Codes für GET /status.json

8.3 Automatisches Remote Update

Die MU100 bietet die Funktionalität eines Remoteupdates an.
Die Aktivierung der Funktion erfolgt mittels Webserver, das Hinterlegen der Serveradresse erfolgt jedoch bereits zum Produktionszeitpunkt. Um die Funktionalität sicherzustellen, muss ein Zugang zum Internet für das Gerät bereitgestellt werden, da regelmäßiger Datenaustausch mit dem Server notwendig ist, um Informationen hinsichtlich eines bereitgestellten Updates zu erhalten. Wird das Gerät am Server für ein Update ausgewählt, erfolgt die Abfrage des Updatefiles und Rückmeldung des Updatestatus durch das Gerät selbst. Die Authentifizierung des Servers gegenüber dem Gerät wird durch eine eigene Root-of-Trust gewährleistet, um sicherzustellen, dass die bezogene Updatedatei nur aus einer vertrauenswürdigen Quelle stammt. Außerdem wird sichergestellt, dass jedes Gerät eindeutig am Server identifiziert werden kann.

A. Anhang

Diese Seite wurde absichtlich leer gelassen.

8.4 Programmablaufplan Update über HTTP Rest Routen

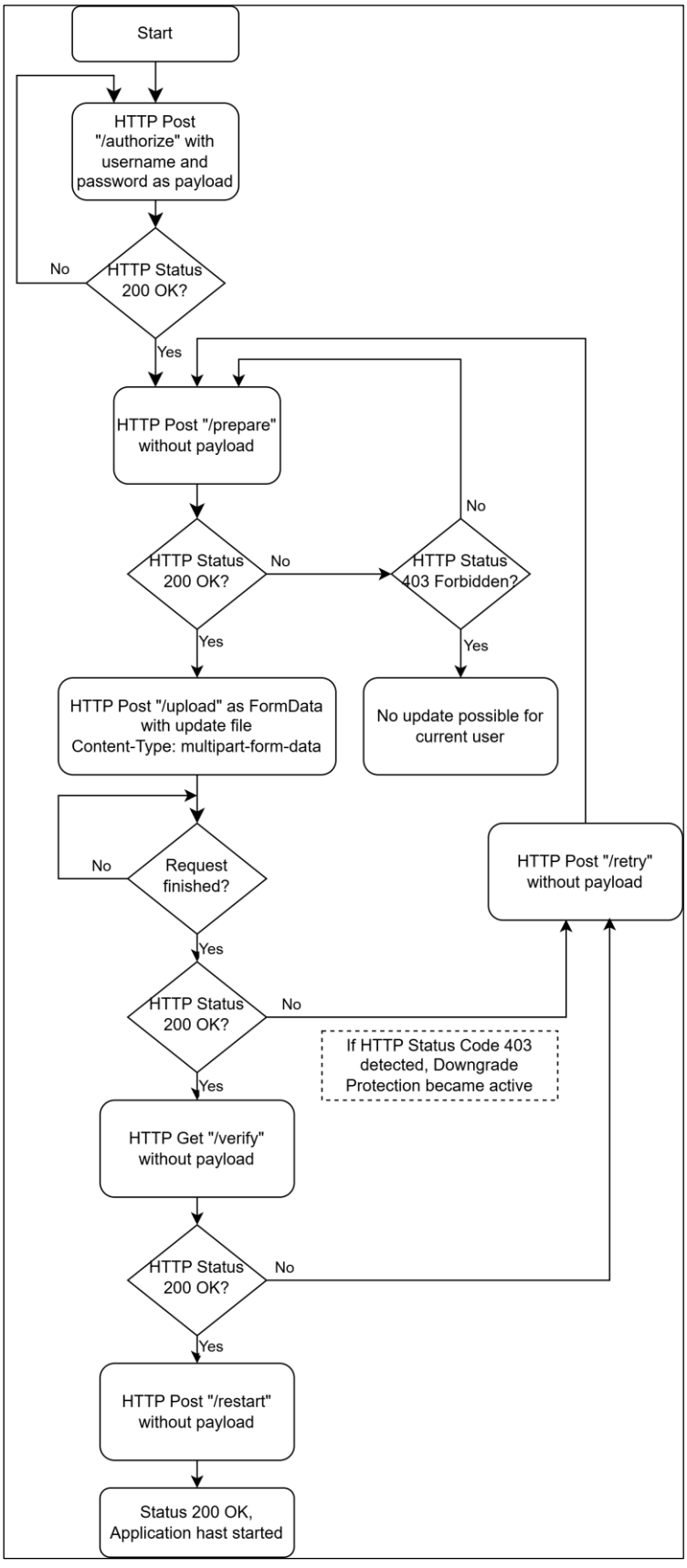

Abbildung 10: Programmablaufplan manuelles Update