Register (Dec)	Meaning	Data Type	Note
35000	Solis Inverter Model definition	U16	Explanation: 0000---no definition 1010---1phase grid-tied inverter 1020---3 phase grid-tied inverter 2030--- 1 phase LV Hybrid inverter 2031--- 1 phase LV AC Couple energy storage inverter 2040---1 phase HV Hybrid inverter 2050--- 3 phases LV Hybrid inverter 2060--- 3 phases HV Hybrid inverter 1070--- External EPM device 3010---OGI Off-grid inverter

Marc Haber
Dipl.-Inform.

Modbus
Die 80er haben angerufen

Agenda

- Was ist Modbus
- Wiederholung serielle Schnittstellen
- Protokollbeschreibung
  - Objekte
  - Datentypen
  - Frameformat
- Einbindung in moderne Systeme
- Sicherheit

Marc Haber, Dipl.-Inform.

- “Zugschlus”
- Wohnort St. Ilgen (bei Heidelberg)
- Freier IT-Berater
- Jahrgang 1969, verheiratet, 4 Katzen
- Arbeitet mit Linux und Netzwerken
- “alles was nichts mit Microsoft oder Apple zu tun hat”
- Würde gerne mal wieder mit Debian arbeiten

Was ist Modbus?

- Industrielles Kommunikationsprotokoll
- 1979 Modicon (heute Schneider Electric)
- Offenes Protokoll
  - weit verbreitet & lizenzfrei
- Verwendet für
  - SPS
  - Sensoren, Aktoren
  - SCADA, IoT
  - Hausautomatisierung, Heizung, Photovoltaik

Übertragungsmedien

- Serielle Schnittstellen
  - RS-232, V.24/V.28
  - RS-422
  - RS-485
- TCP

RS-232 / V.24/V.28

- kennen wir alle
- “serielle Schnittstelle”
- 115200 kbps “schnell”
- 15 Meter “weit”
- Punkt-zu-Punkt-Verbindung
- DB25-DE9-Stecker

Maximalwerte

Übertragungsrate (bit/s)	Länge (m)
2400	900
4800	300
9600	152
19200	15
57600	5
115200	< 2

Tabelle: de.wikipedia.org

Bild: start-e.net

RS-485

- Elektrische Übertragung differenziell
- robuster (“industrietauglich”)
- Schneller. (Höher.) Weiter.
- Multidropfähig (ein Master, mehrere Slaves)
- Kein V.xx Gegenstück
- Für die Software wie RS-232
- Kein genormter Stecker
  - nicht mal eine Konvention
  - Also: Lüsterklemmen und Widerstände

RS-485

- Elektrische Übertragung differenziell
- robuster (“indu
- Multidropfähig s)
- Kein V.xx Geg
- Low-Level-Pro ration
  wie RS-232
- Kein genormte
  - nicht mal e
  - Also: Lüste

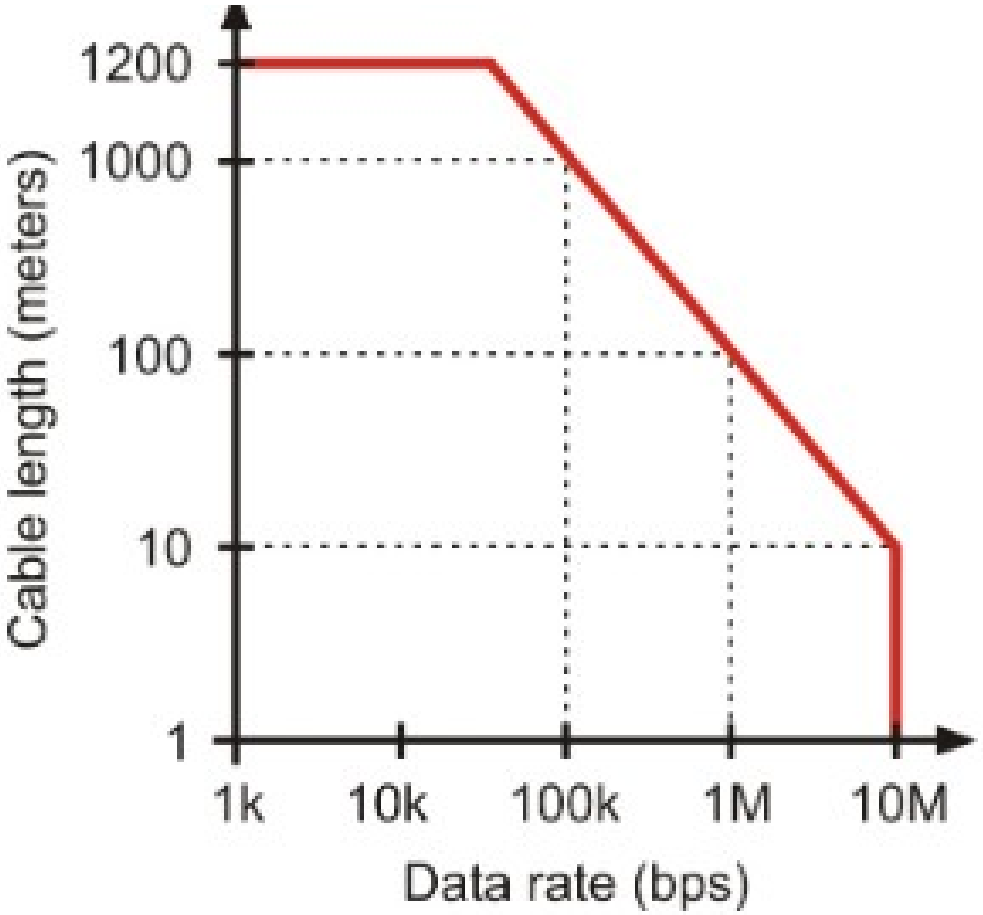


Bild: novusautomation.com

RS-485

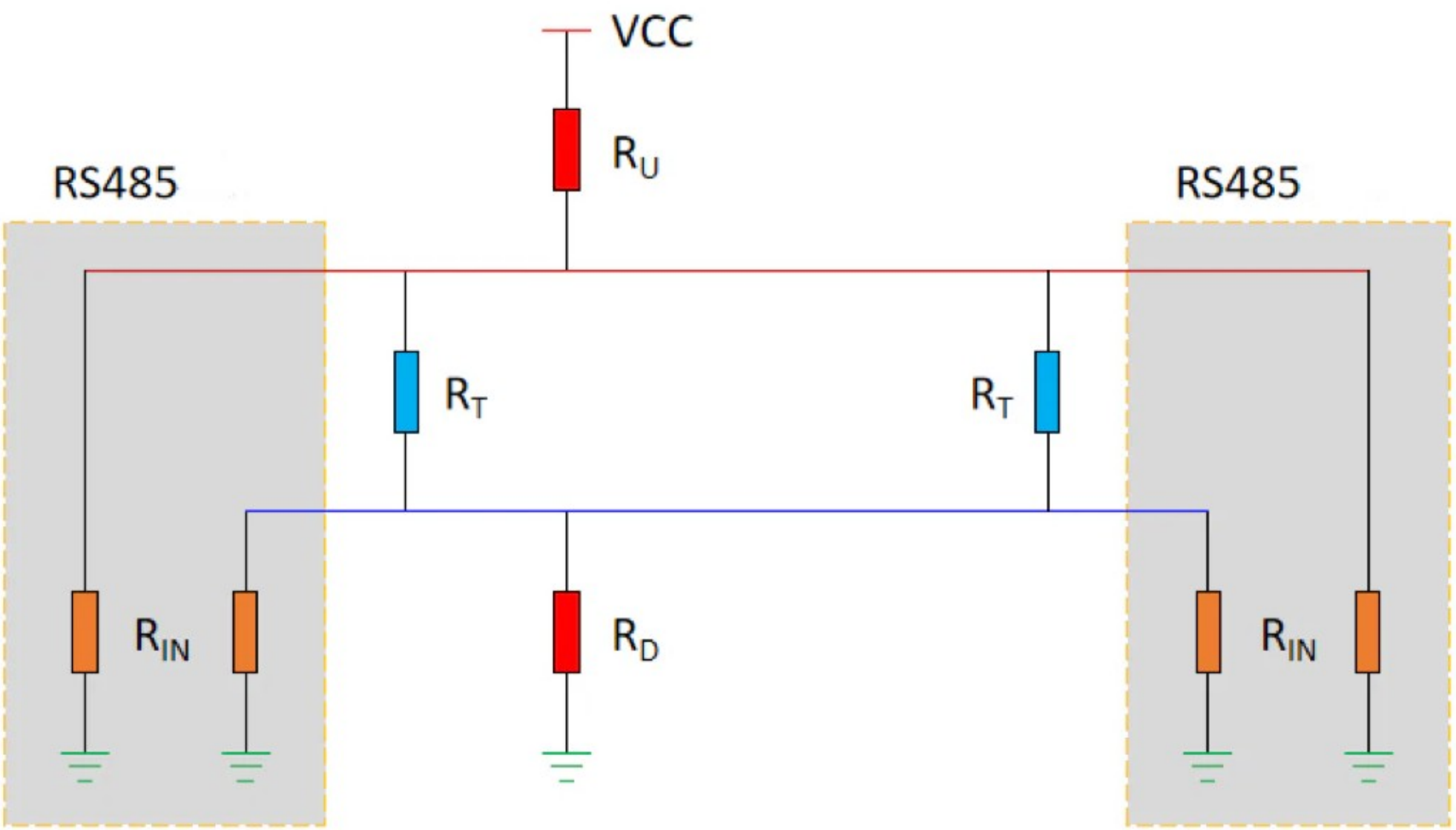


Bild: ebyteiot.com

Modbus-Kommunikationsmodell

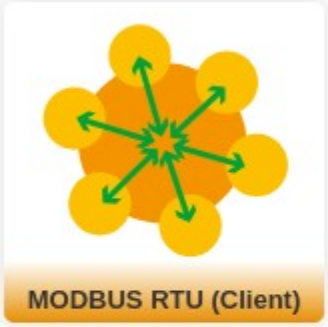
- Master-Slave bzw. Client-Server Prinzip
  - Master == Client, Slave == Server
- Master fragt, Slave antwortet
  - Andersherum eigentlich nur bei TCP
- 8 Bit Adressen (1-247 benutzbar)
- Adressierung bietet interessante Fehlerbilder

Modbus über serielle Schnittstelle

- Fast immer RS-485, RS-232 möglich
- Parametrierung notwendig
- Server antwortet nur auf Requests
  - Nur Polling möglich
  - Keine Alarmierung

Modbus über serielle Schnittstelle

- Fast imm
- Parame
- Server a
  - Nu
  - Kei



Modbus 1

Beschreibung	Modbus 1 ✓	
Typ	Eingebaute Schnittstelle	
Subsystem Manage subsystems	Name	Modbus 1
	Beschreibung	Modbus 1
	Präfix	MR1 Geräte Manager
RTU Einstellungen Erweiterte Einstellungen für die serielle Datenübertragung	Baudrate	9600
	Parität	gerade
	Stoppbits	1
	Datenbits	8
Statistik Letzte 60 Sekunden	Anforderungen gesamt	59
	Anforderungen mit Fehler	0
	Verbindungsversuche	0
	Verlauf anzeigen	

“serielle” Datenformate

- Modbus RTU (Remote Terminal Unit)
  - Binäres Format
  - Weit verbreitet
- Modbus ASCII
  - Lesbares Format
  - Think Kombination aus CSV und SMTP
  - Exotisch

Modbus über TCP

- Bidirektionale Kommunikation möglich
  - Der Server kann sich unaufgefordert melden
- Standort- und netzwerkübergreifend
- Ausfall des Servers kann detektiert werden
- Signalverarbeitung in Virtualisierung
  - Ohne Hardwareklimmzüge
- Protokoll sehr ähnlich
  - dass Konvertierung trivial

Modbus-Frame-Aufbau

Modbus RTU Frame Format

Start	Address	Function	Data	CRC	End
≥3.5 char	8 bit	8 bit	N * 8 bit	16 bits	≥3.5 char

- 01: Read Coils
- 02: Read Discrete Inputs
- 03: Read Holding Registers
- 04: Read Input Registers
- 05: Write Single Coil
- 06: Write Single Holding Register
- 15: Write Multiple Coils
- 16: Write Multiple Holding Registers

Bild: Research Gate

Kommunikationsobjekte: Arten

- Coils
  - Boolean-Wert
  - “Spule” (wie in einem Relais)
- Register
  - Menge von Bits
  - Bedeutung bedarf Definition
    - float/integer – signed/unsigned - Länge
- Read-Only / Read-Write
  - Read-Write nicht notwendigerweise richtig!

Kommunikationsobjekte

- Objekte sind durchnummeriert
  - 1-9999: read-write output coils
  - 10001-19999: read-only input coils
  - 30001-39999: read-only input registers
  - 40001-49999: read-write output registers
  - Aber: Register 1 Adresse 0?
  - Oder: Register 1 Adresse 1?
  - Hexadezimal? Dezimal?
- Jedes Register-Objekt hat 16 bit
  - 32-bit-Objekt? Nächstes Objekt mit belegt!

Kommunikationsobjekte

33029-33030	Total energy generation	U32	1kWh
33031-33032	Current month energy generation	U32	1kWh
33033-33034	Last month energy generation	U32	1kWh
33035	Today energy generation	U16	0.1kWh
33036	Yesterday energy generation	U16	0.1kWh
33037-33038	This year energy generation	U32	1kWh
33039-33040	Last year energy generation	U32	1kWh

33251	Meter ac voltage A	U16	0.1V
33252	Meter ac current A	U16	0.01A
33253	Meter ac voltage B	U16	0.1V
33254	Meter ac current B	U16	0.01A
33255	Meter ac voltage C	U16	0.1V
33256	Meter ac current C	U16	0.01A
33257	Meter active power A	S32	0.001kW
33259	Meter active power B	S32	0.001kW
33261	Meter active power C	S32	0.001kW
33263	Meter total active power	S32	0.001kW

Quelle: Solis

Und die Praxis?

Modbus RTU im CLI

```
1 [1/4986]mh@lapis:~ $ mbrtu --help
This is mbrtu version 0.3.3 - GPL 2.1 (c) 2015 Lars Täuber
gitaeuber@users.noreply.github.com

mbrtu -d DEVICE [-b BAUDRATE] [-p PARITY] [-s STOPPBITS] [-D]
     [-a ADDR] [-f FUNC] [-t TYPE] [-n #] -r REG
    [[-a ADDR] [-f FUNC] [-t TYPE] [-n #] -r REG ...]


The following options need to be specified first:
        -h                      Print this help message.
        -d serial device        /dev/ttyUSB?
        -b baud rate                    default: 9600
        -p parity               E|O|N   default: even
        -s number of stop bits  [1|2]   default: 1 for odd and even parity, 2 for no parity

        -a address of slave to ask 1-255
           0 for broadcast
           default: last one called or 1

        -f function to send     [h|i|w|3|4|6|16]
           h = 3 = read holding registers
           i = 4 = read input registers         (default)
           w = 6 = write single register
              16 = write multiple 16 bit registers
          default: last one called or 4

        -n
           either: number of 16 bit registers to read
```

Modbus RTU im GUI

MODBUS RTU

MR1 Modbus 1

Modbus 1

Status: OK

Schnittstelle: Modbus 1 Typ: Eingebaute Schnittstelle

Anzeigefilter

Durch Intervall ausgelöst: Ein

Durch Bedingung ausgelöst: Ein

Live Check: Ein

Anzeige Optionen

Basis 0: Ein

HEX: Aus

Millisekunden: Aus

Aktualisierung: Ein

Quelle	Date Zeit	Gerät ID	Adresse Datenlänge	Zugriff	Ergebnis Daten
	02.04.2025 10:21:21	DVH4013 privat 72	4 16384 32 Bits	R (03) →	ok 89 ms 0x0017 C810
	02.04.2025 10:21:21	DVH4013 privat 72	4 00000 32 Bits	R (03) →	ok 127 ms 0x0000 0919
	02.04.2025 10:21:21	DVH4013 privat 72	4 16640 32 Bits	R (03) →	ok 131 ms 0x0000 0000
	02.04.2025 10:21:20	DVH4013 privat 72	4 00002 32 Bits	R (03) →	ok 89 ms 0x0000 0000

Datentypdefinition heutzutage

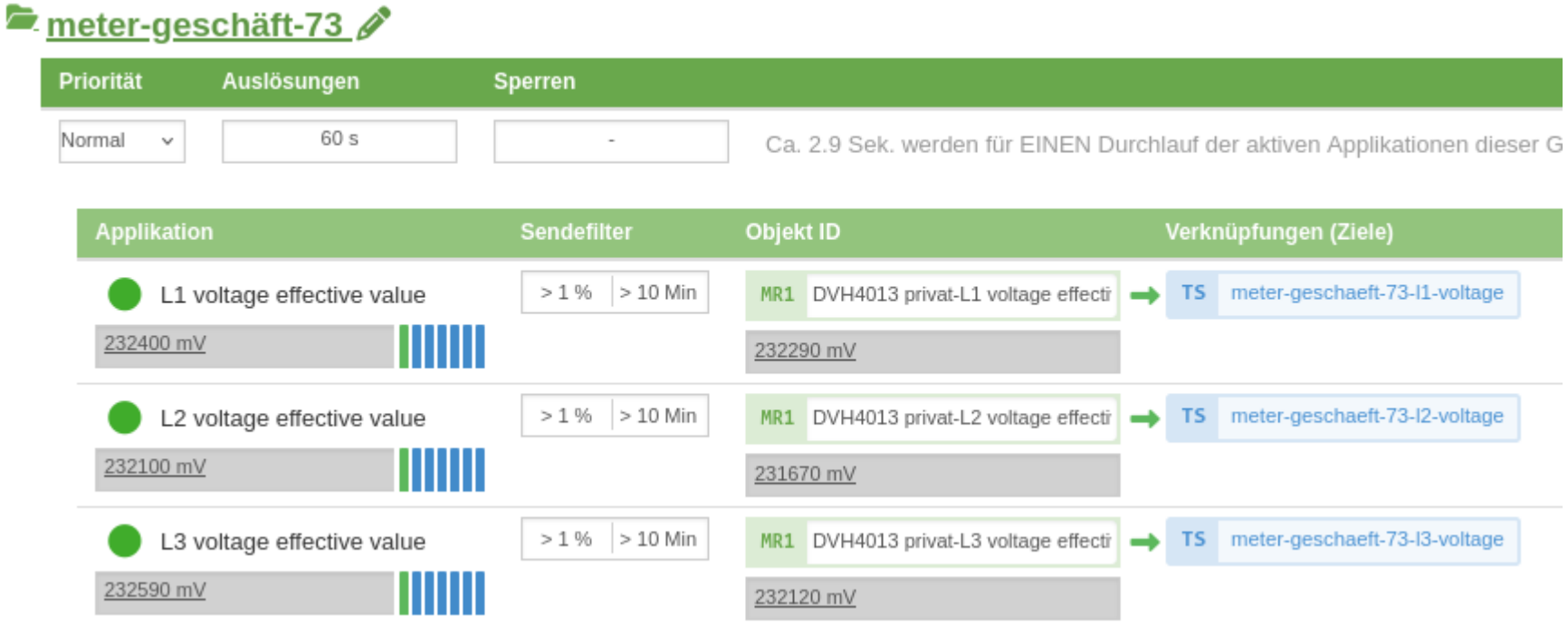
Register und Applikationen

Auswahl Registersets: Alle Registersets

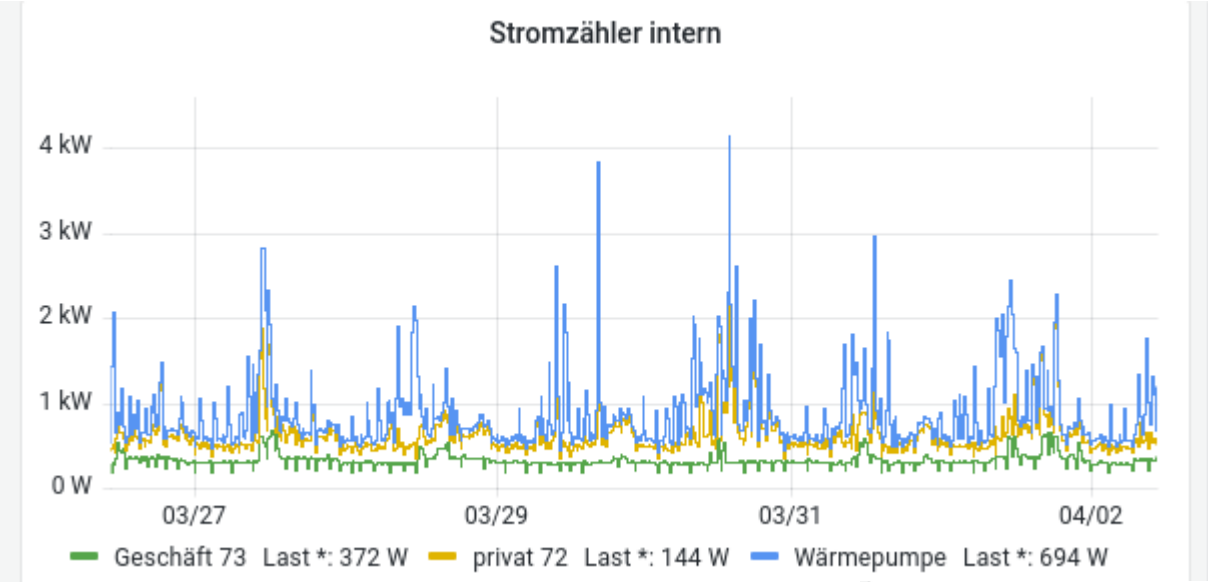
Register in HEX: Aus | Register zur Basis 0: Ein | Schreiben in Live-Checks: Aus | Experten Modus: Ein

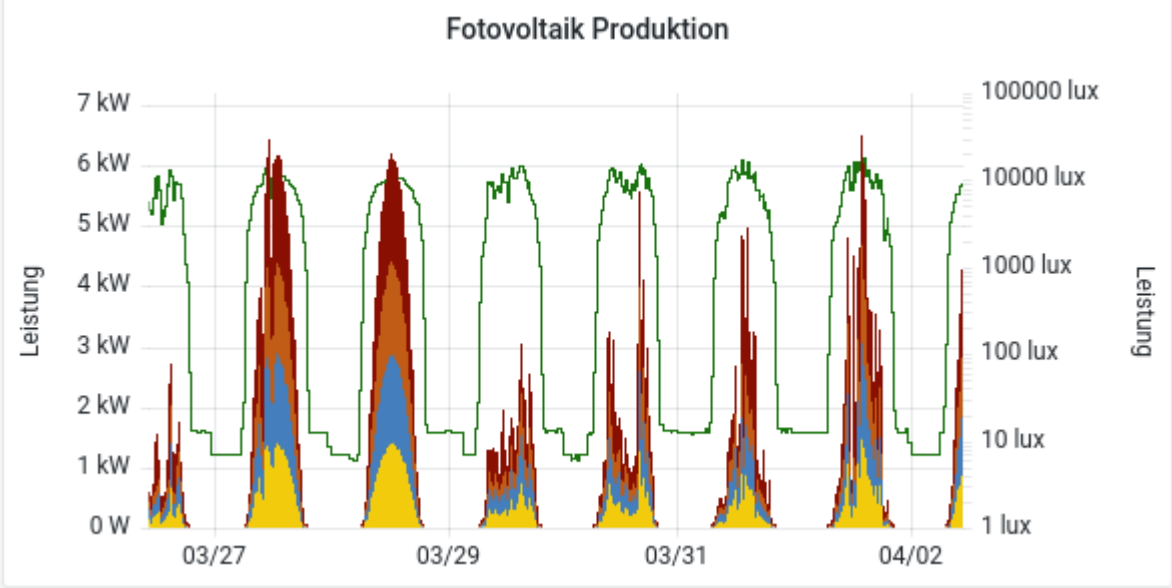
Register	Breite	Applikation	Beschreibung	Zugriff	Format	Wert	Wertprüfung / Wertanpassung / Objekt-Typ / Einheit	Objektwert	Flags
Address	Filter	Name	Description	Filter	Filter	Filter	Filter	(max 20)	Flags
4 00000	32 Bit (2 Word	total import activ		R (03)	UINT	···	- x / 10 int W	···	----
4 00002	32 Bit (2 Word	total export activ		R (03)	UINT	···	- x / 10 int W	···	----
4 00004	32 Bit (2 Word	L1 voltage effect		R (03)	UINT	···	- x * 10 int mV	···	----
4 00006	32 Bit (2 Word	L2 voltage effect		R (03)	UINT	···	- x * 10 int mV	···	----
4 00008	32 Bit (2 Word	L3 voltage effect		R (03)	UINT	···	- x * 10 int mV	···	----
4 00010	32 Bit (2 Word	L1 current effecti		R (03)	UINT	···	- - int mA	···	----
4 00012	32 Bit (2 Word	L2 current effecti		R (03)	UINT	···	- - int mA	···	----
4 00014	32 Bit (2 Word	L3 current effecti		R (03)	UINT	···	- - int mA	···	----

Weiterverteilung der Daten



Grafana


Stromzähler intern
4 kW
3 kW
2 kW
1 kW
0 W
03/27
03/29
03/31
04/02
Geschäft 73 Last *: 372 W
privat 72 Last *: 144 W
Wärmepumpe Last *: 694 W


Fotovoltaik Produktion
7 kW
6 kW
5 kW
4 kW
3 kW
2 kW
1 kW
0 W
Leistung
100000 lux
10000 lux
1000 lux
100 lux
10 lux
1 lux
Leistung
03/27
03/29
03/31
04/02

Umsetzung Modbus RTU auf TCP

Logout Chinese

Device Information

Device Name	WSDEV0001	Firmware Version	V1. 452	Device MAC	28-72-78-55-D6-A5

Network Settings

Device IP	192.168.196.90	Device Port	502	Device Web Port	80
Work Mode	TCP Server	Subnet Mask	255.255.255.0	Gateway	192.168.196.254
Destination IP/DNS	192.168.1.3	Destination Port	502	IP mode	DHCP

Serial Settings

Baud Rate	9600	Databits	8	Parity	None
Stopbits	1	Flow control	None		

Advanced Settings

No-Data-Restart	Disable	No Data Restart Time	300 5~1270 second	Reconnect-time	12 1~255 second

Sicherheit?

- Hamwernich!

- Keine Verschlüsselung
- Keine Authentifizierung
- Besonders problematisch bei Modbus TCP

- Besser:
  - Wegfiltern, ortsnah verarbeiten
  - Transport mit moderneren Protokollen

Modbus in der Praxis

Bild: DZG

Modbus in der Praxis

Bild: Waveshare Electronics

Modbus in der Praxis

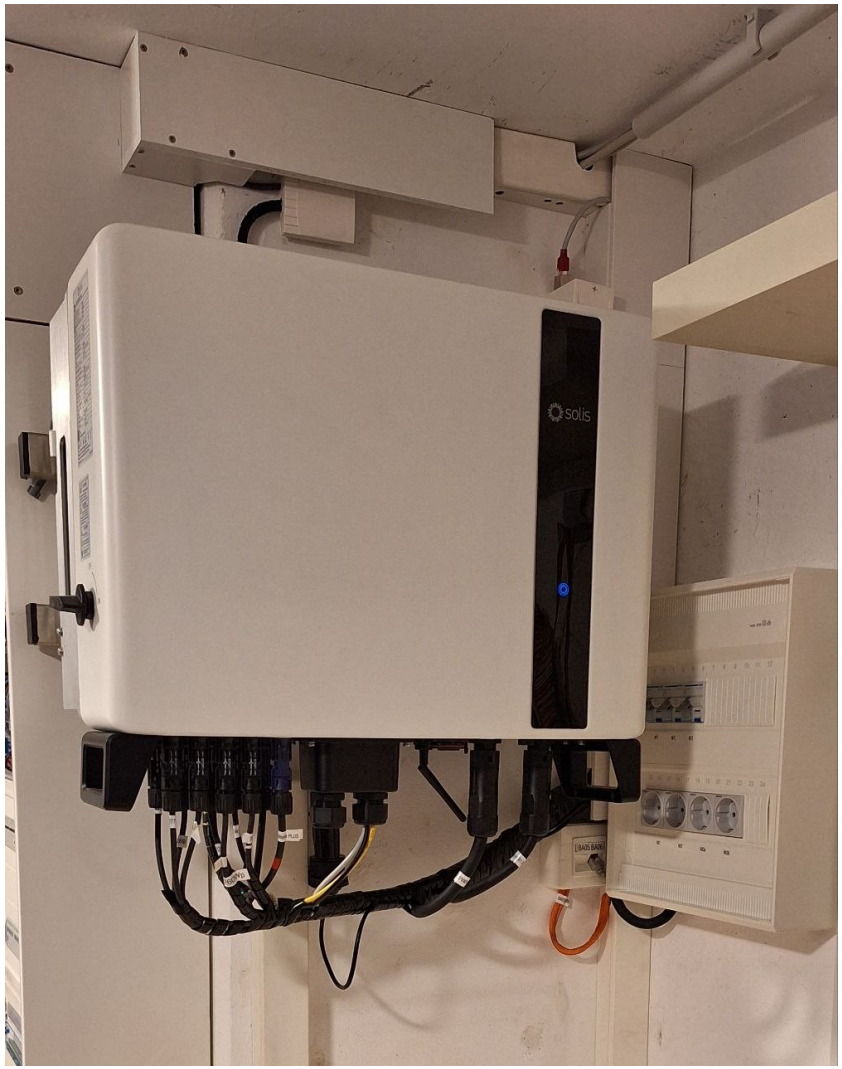
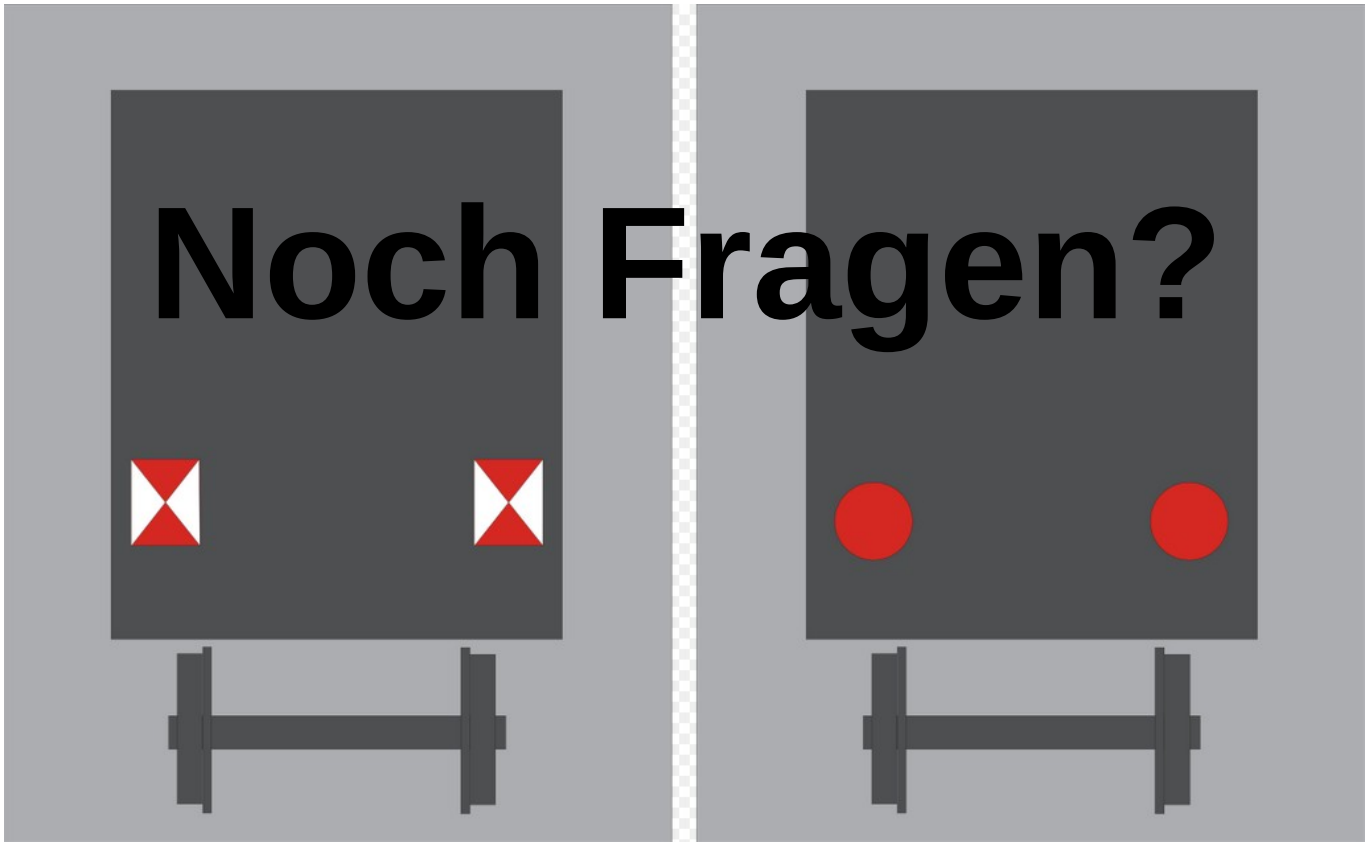


Bild oben: Waveshare Electronics
Bild rechts: eigene Aufnahme

Vielen Dank für Eure Geduld

Noch Fragen?

Vielen Dank für Eure Geduld



Marc Haber mh+flarp@zugschlus.de
Fediverse: @Zugschlus@zug.network https://blog.zugschlus.de/