

LEGO

Small BalkonKwerk

LEGO

SolarbalkonKftwerke

Fails, Hacking, Security, - Security, Privacy

Design
61-9

Smiler Sacloker
Power Meter
Inventory Scanner

SolarbalkonKftwerke



Whoam... we!



- ▶ **Bastian Widmer**
- ▶ hello@bastianwidmer.ch
- ▶ bastianwidmer.ch
- ▶ [@dasrecht@chaos.social](https://twitter.com/dasrecht)



- ▶ **Roland Marx**
- ▶ solar@marxram-consulting.com
- ▶ <https://de.linkedin.com/in/marxram>
- ▶ <https://github.com/marxram/deye-esp-mqtt-bridge>

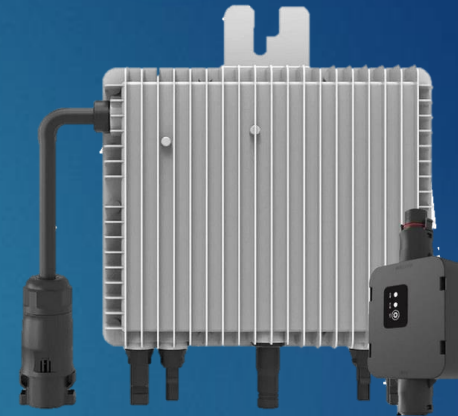
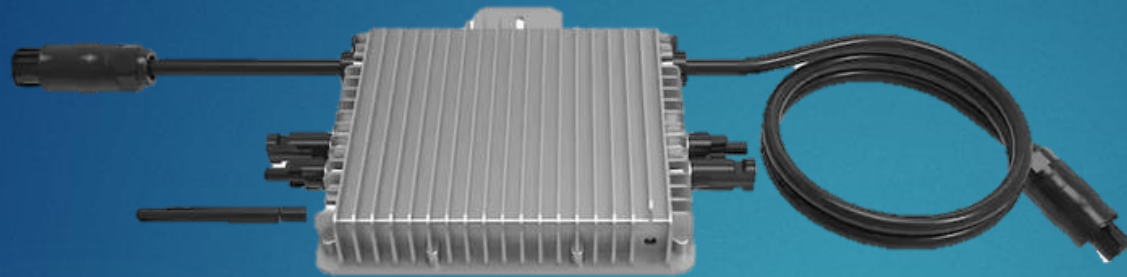
Agenda

- ▶ Einleitung Solarkraft
 - ▶ KEINE Zeit ;-)
- ▶ Firmware
- ▶ Whats in the box?
- ▶ Communication & Components
- ▶ Firmware Features
- ▶ Risk Assessment
- ▶ Status and Disclosure
- ▶ Discussion & Outlook

Message



- ✓ Solarenergie ist gut!
- ✓ Security wäre auch nicht schlecht
- ✓ Aktuell kochen leider viele nur mit Wasser
- ✓ Wir klären auf, worauf man achten sollte!



Firmware

Wie es dazu kam...



Firmware - Wie es dazu kam...



- ▶ Installations Wifi Passwort liess sich nicht ändern. [[Heise](#)]
- ▶ Standard Passwort ... 12345678
- ▶ Möglichkeit die Credentials des Heim Wifi auszulesen
- ▶ Firmware Updates nicht verfügbar
- ▶ Support nicht hilfreich
- ▶ Druck über Medien hilft

Balkonkraftwerke: Sicherheitslücke in Mikrowechselrichtern von Deye

Mikrowechselrichter von Deye werden mit unsicherer Firmware ausgeliefert. Helfen kann nur der chinesische Hersteller, doch das Update gibt es nur auf Anfrage.

Lesezeit: 4 Min.  In Pocket speichern

   308



Firmware - Wie es dazu kam...



- ▶ Nach dem Heise Artikel und der neuen Firmware
- ▶ Support sehr schnell und hilfreich:
 - ▶ [Hat ungefähr so in meiner Mailbox stattgefunden]
 - ▶ Ich: Gerne ein Update weil ein offenes Wifi mich stört
 - ▶ Support: Ihre Seriennummer bitte?
 - ▶ Ich: SN[REDACTED]
 - ▶ Support: Jep Update gemacht
 - ▶ Ich: Moment mal! 🤔
 - ▶ Support: Gerne doch und einen schönen Tag
 - ▶ Ich: 🤔

Firmware - Wie es dazu kam...



- ▶ Firmware Updates mal da mal nicht...
- ▶ Server Stabilität 😞
- ▶ Anfrage an den Support wiederum wenig hilfreich
- ▶ Photovoltaikforum

FW-Update offline! Deye SUN600G3-EU230 und baugleiche

astromeier · 11. Januar 2023

Antworten

< 1 2 3 4 5 6 >

Abonniert



astromeier
Stammmitglied

Reaktionen:	16
Beiträge:	38
Dateianhänge:	5
PV-Anlage in kWp:	0,6
Information:	Betreiber

11. Januar 2023

#1

So, nach einigen Stunden Recherche meine Zusammenfassung aus verschiedenen laaangen Threads: Im Web-Interface unter *Upgrade / Upgrade firmware* kann man eine Datei hochladen und upgraden... Diese .bin-Datei steht jedoch nicht zum Download bereit, also nicht Google-bar..... 😞

Es gibt hier aber eine [ZIP-Datei zum Download](#):

Mit der fwupdate.exe in diesem Archiv kann man ein Update versuchen, wenn man bzw. der Inverter eine Internet Verbindung hat.

Siehe dazu weiter im Thread des o.a. Links.

Klappt dies nicht oder will man so nicht vorgehen:

Man könnte ja die .exe-Datei mal in einem [HEX-Editor öffnen und nach AT+UPURL= suchen](#)

Mit dem Fund http://ipadressenfund:80/0_D0002_18/MW3_16U_5406_1.53.bin kann man die aktuelle Datei herunterladen 😊

Bei Bedarf den FW-Namen **MW3_16U_5406_1.53** durch die aktuelle oder gewünschte Version ersetzen.

Diese Datei kann dann im Inverter-Web-Interface unter *Upgrade / Upgrade firmware* hochgeladen und das Update offline gemacht werden.

In verschiedenen Threads gibt es Hinweise, dass beim per Mail beauftragten OTA-Update auch andere Teile des Inverters ein

Firmware - Wie es dazu kam...



- ▶ Alle reden über den Update Server aber keiner publiziert die IP oder details (Hackerparagraf oder Korrektheit?)
- ▶ fwupdate.exe - Deye Servicetechniker Tool
- ▶ notepad fwupdate.exe?

```
rent · map · read · and · map · writefindrunnable: · negative · nmspinningfreeing  
o · package · net: · using · cgo · DNS · resolver  
ime · executionAT+UPURL=http://47.254.36.66:80/0_D0002_18/gcBgMarkWor
```

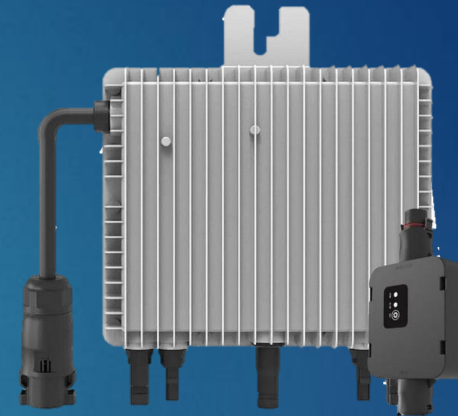
Firmware - Wie es dazu kam...



- ▶ <https://github.com/dasrecht/deye-firmware>
- ▶ Changelogs? Keine Antwort von Deye, Bosswerk, etc.
- ▶ Gewisse Changes sind bekannt (PW Change, Backend Server Changes)
- ▶ Aber keine Klarheit was wirklich geändert wird
- ▶ Aber was wenn der Hersteller sich an dem Repository stört?
 - ▶ Ja dann happy DMCA

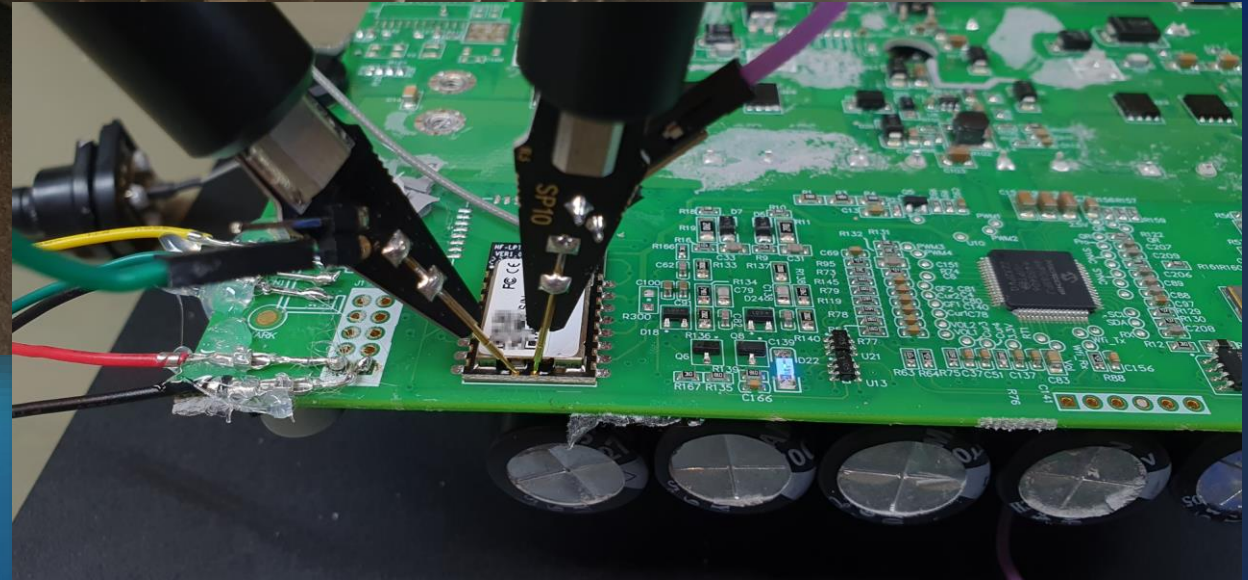
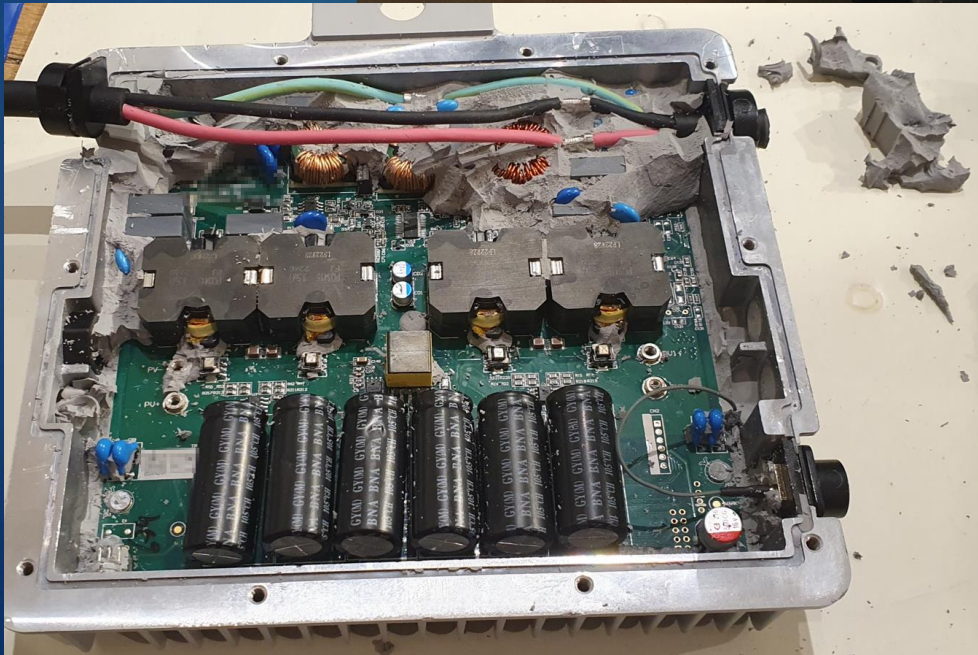
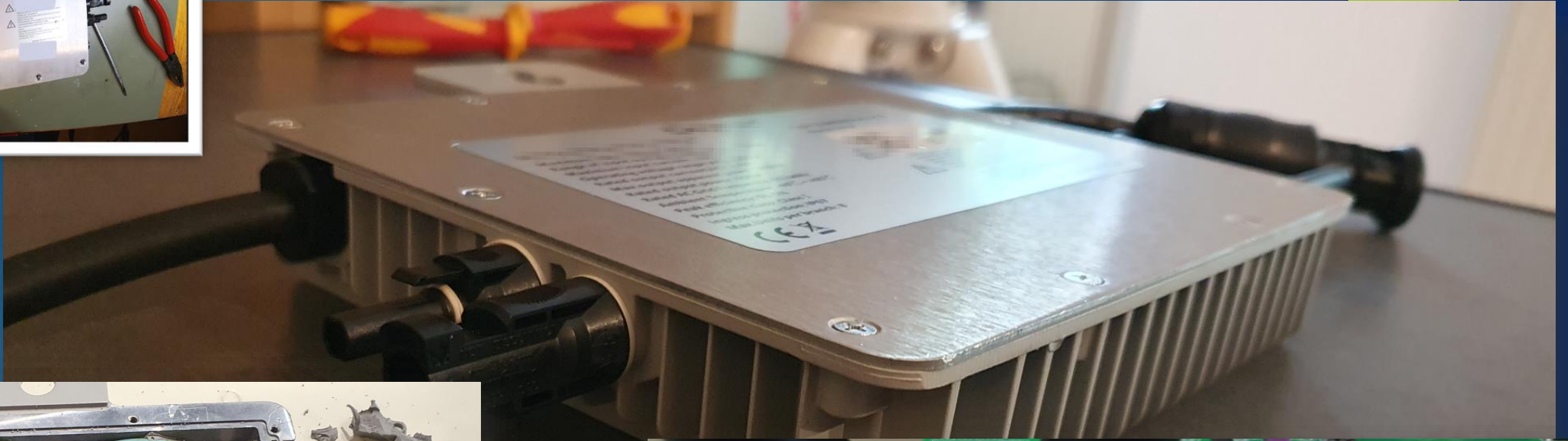
The screenshot shows the GitHub repository page for 'deye-firmware' by user 'dasrecht'. The repository is public and has 13 forks, 124 stars, and 31 watchers. The main branch is 'main' with 2 branches and 0 tags. The commit history shows a merge pull request #25 from 'palto42/MW3_16U_5406_2.32-D1' 3 months ago, and several other commits including 'Adding 0_5407_1 versions trough enumeration', 'Added firmware version MW3_16U_5406_2.32-D1.bin', 'Adding the deye inverter reset apk', and 'initial commit'.

Commit	Description	Time
dasrecht Merge pull request #25 from palto42/MW3_16U_5406_2.32-D1		75a77ab · 3 months ago · 34 Commits
0_5407_1	Adding 0_5407_1 versions trough enumeration	5 months ago
0_D0002_18	Added firmware version MW3_16U_5406_2.32-D1.bin	4 months ago
Deye-Inverter-Reset-Apk	Adding the deye inverter reset apk	5 months ago
fwupdate	initial commit	last year
README.md	Merge pull request #18 from dasrecht/2023-08-new-firm	5 months ago



What's in the box

YOU DON'T OWN IT IF YOU DON'T OPEN IT



Wifi Modul Firmware



MW3_15_0501_1.15.bin 17.09.2023 15:37 BIN-Datei 424 KB

```

1 HF-LPBX300 Image™žACKNULmQ^p
2 NUL$mr
3 "HqαŸ;ÚJ→4' DC1h...ôBEL `
4 N×ëzIi}ÁEOTgçUŽÉûcè»Ô;ÔRSISO
5 EŸ¹GSµªECÛ°f`gõĐ àìuBELiDêóé
6 ttÃ4USMep
    
```

HF 物联·改变生活

Home IOT Module IOT Device

Home > ★HF-LPT130A

★HF-LPT130A

Product Code: UART to Wi-Fi [LPT130A]

Description	Specification	Downloads
Production Data	2017/Q4	
Key Feature	Low Power SDK Support SmartLink Config Tiny Size Lowest Price	
Processor	Cortex-M4 SOC	
Basic Frequency	160MHz	
Operating System	mbed	
Wi-Fi Standard	802.11bgn	
Certification	CE/FCC/SRRC/RoHS	
Temp. Range	-40°C- 125°C	
Internal Antenna	√	
I-PEX Connector	√	
Size (mm)	22×14.3×8	
Package Type	DIP10	
Work Voltage	2.9-4.2V	
Current @No data	~25mA	
Current @Tx Peak	~260mA	
Resource-Flash	1MB/2MB/4MB	
Resource-RAM	352KB /384KB/448KB	

Software Parameters	Network Type	STA/AP/AP+STA
	Security Mechanisms	WEP/WPA-PSK/WPA2-PSK
	Encryption	WEP64/WEP128/TKIP/AES
	Update Firmware	Local Wireless, Remote OTA
	Customization	Support SDK for application develop
	Network Protocol	IPv4, TCP/UDP/HTTP/TLS(SDK)
	User Configuration	AT+instruction set. Android/ IOS Smart Link APP tools

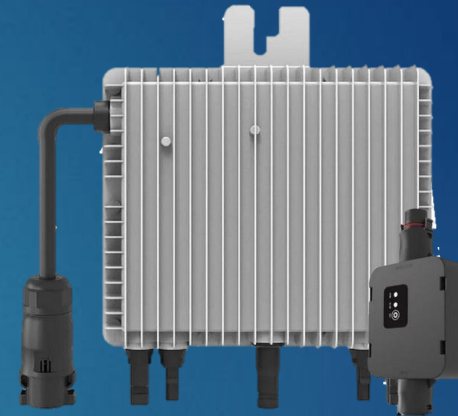
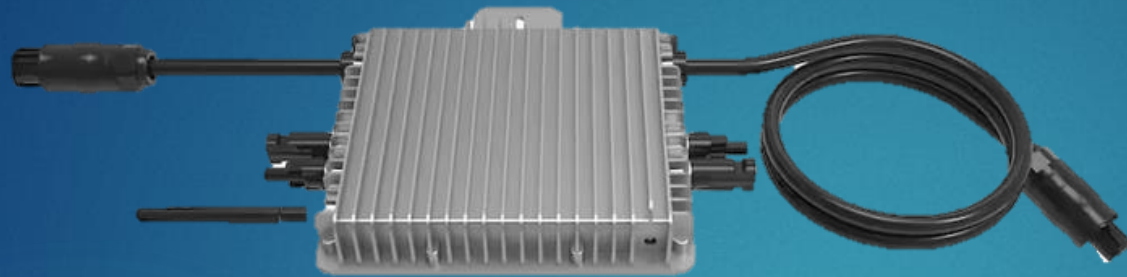
HF-LPT130A-XX (XM)

Blank: 1MB Flash
(2M): 2MB Flash

Connector:
0-180 Straight
2- 90 Bend

Antenna Type
1- Internal Copper Line
0- External IPEX Interface

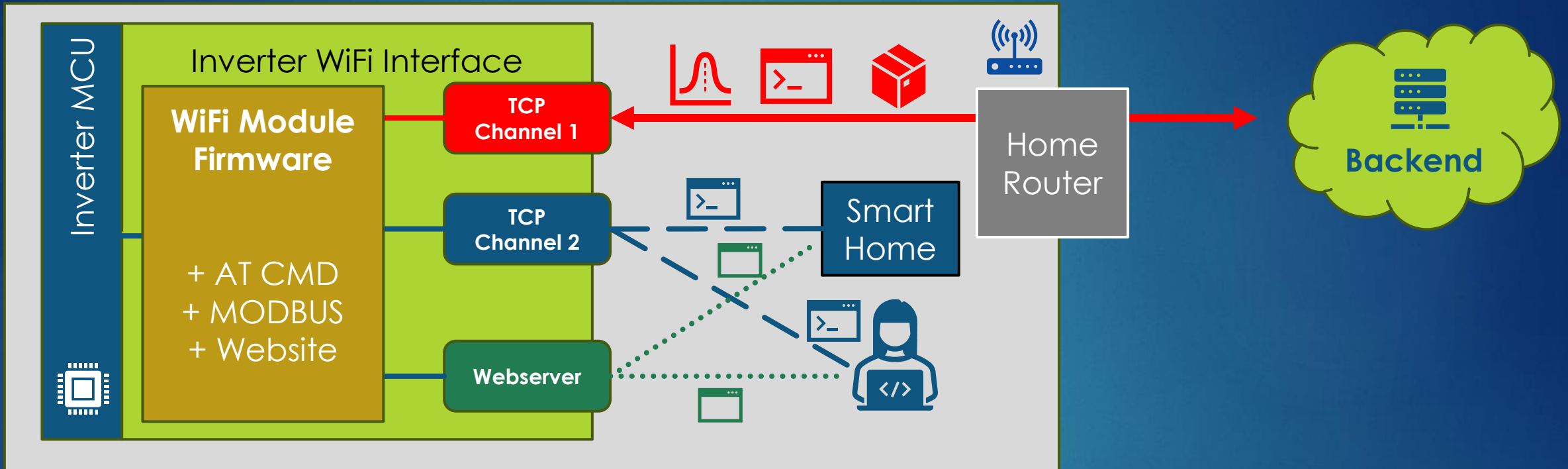
Product: LPT130A
Company: HF



Communication?

WHO? WHAT? WHY?

Communication & Components



Webserver

- ▶ Configuration, reduced data read out, lightweight smart-home integration

TCP Channel 1

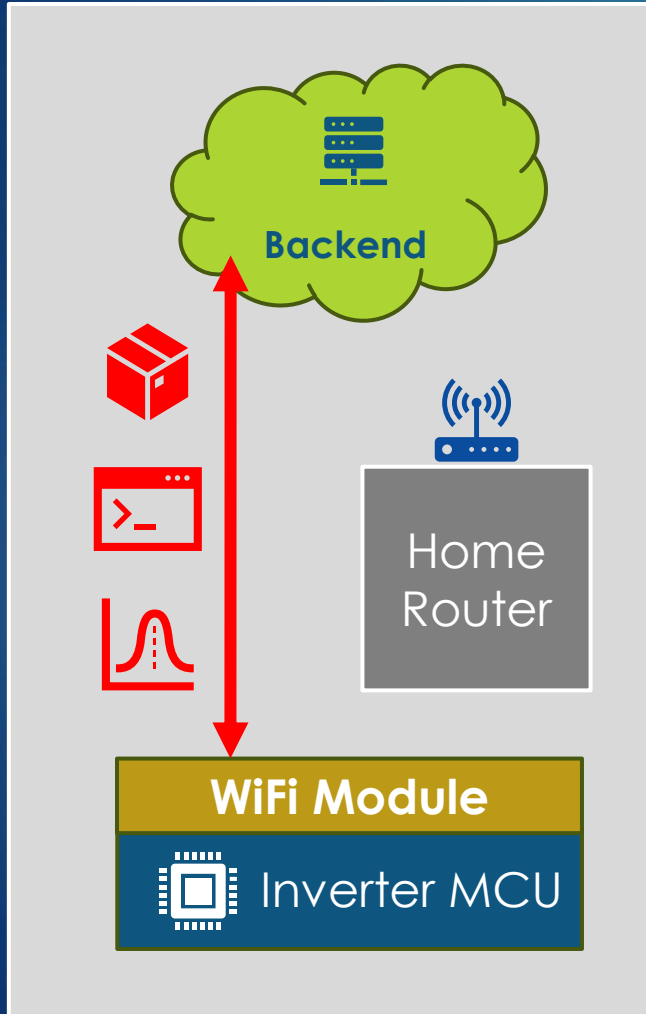
- ▶ TCP#1: Backend communication, data delivery, remote management, firmware update, time sync

TCP Channel 2

- ▶ TCP#2: Local Management Port, detailed data readout, time setting, SmartHome Integration

Packet Capture for Dummies

fritz.box/html/capture.html



FRITZ!Box 7590

Paketmitschnitt

Die FRITZ!Box kann zur Diagnose alle Datenpakete im [Wireshark](#)-Format mitschneiden, wenn die FRITZ!Box als Router eingestellt ist. Es können mehrere Mitschnitte gleichzeitig gestartet werden. Sie helfen dem AVM-Support bei einer genauen Analyse komplexerer Probleme mit dem Internetzugang. Beachten Sie, dass Mitschnitte eventuell Ihre persönlichen Kennwörter enthalten.

Starten Sie den Mitschnitt über die entsprechende Schaltfläche "Start" und speichern Sie die Datei auf der Festplatte. Beenden Sie den Mitschnitt mit der Schaltfläche "Stopp" bzw. "Alle Mitschnitte stoppen".
Wichtig: Brechen Sie nicht das Speichern der Datei auf die Festplatte im Internet Browser ab, wenn Sie den Mitschnitt beenden wollen, sondern drücken Sie die entsprechende "Stopp"-Schaltfläche.
Klicken Sie auf die Schaltfläche "Aktualisieren", wenn die Schaltflächen zum Stoppen des Mitschnitts nicht angezeigt werden.

Internet

1. Internetverbindung	Start	Stopp
Routing-Schnittstelle	Start	Stopp
Schnittstelle 0 ('internet')	Start	Stopp

Netzwerkschnittstellen

Längenlimitierung pro Paket: 1600 Bytes

Paketfilter: ip host 10.2.2.11

ath0	Start	Stopp
cpunet0	Start	Stopp
eoam	Start	Stopp
eth0	Start	Stopp
eth1	Start	Stopp
eth2	Start	Stopp
eth3	Start	Stopp
ing0	Start	Stopp

Alle stoppen Aktualisieren Zurück



Unencrypted TCP Plain Text

4773	20:36:52,419854	47.102.152.71	10.2.2.11	ICMP	74 Echo (ping) reply id=0xafaf, seq=2833/4363, ttl=4
4774	20:36:53,164019	10.2.2.11	47.254.132.226	SOLARMANV5	369 27168 → 10000 [PSH, ACK] Seq=1 Ack=1 Win=4380 Len=315
4775	20:36:53,187018	47.254.132.226	10.2.2.11	TCP	54 10000 → 27168 [ACK] Seq=1 Ack=316 Win=30016 Len=0
4776	20:36:53,187280	47.254.132.226	10.2.2.11	SOLARMANV5	77 10000 → 27168 [PSH, ACK] Seq=1 Ack=316 Win=30016 Len=
4777	20:36:53,221338	10.2.2.11	47.254.132.226	TCP	60 27168 → 10000 [ACK] Seq=316 Ack=24 Win=4357 Len=0
4778	20:36:53,301934	10.2.2.11	47.254.132.226	SOLARMANV5	397 27168 → 10000 [PSH, ACK] Seq=316 Ack=24 Win=4357 Len=


```

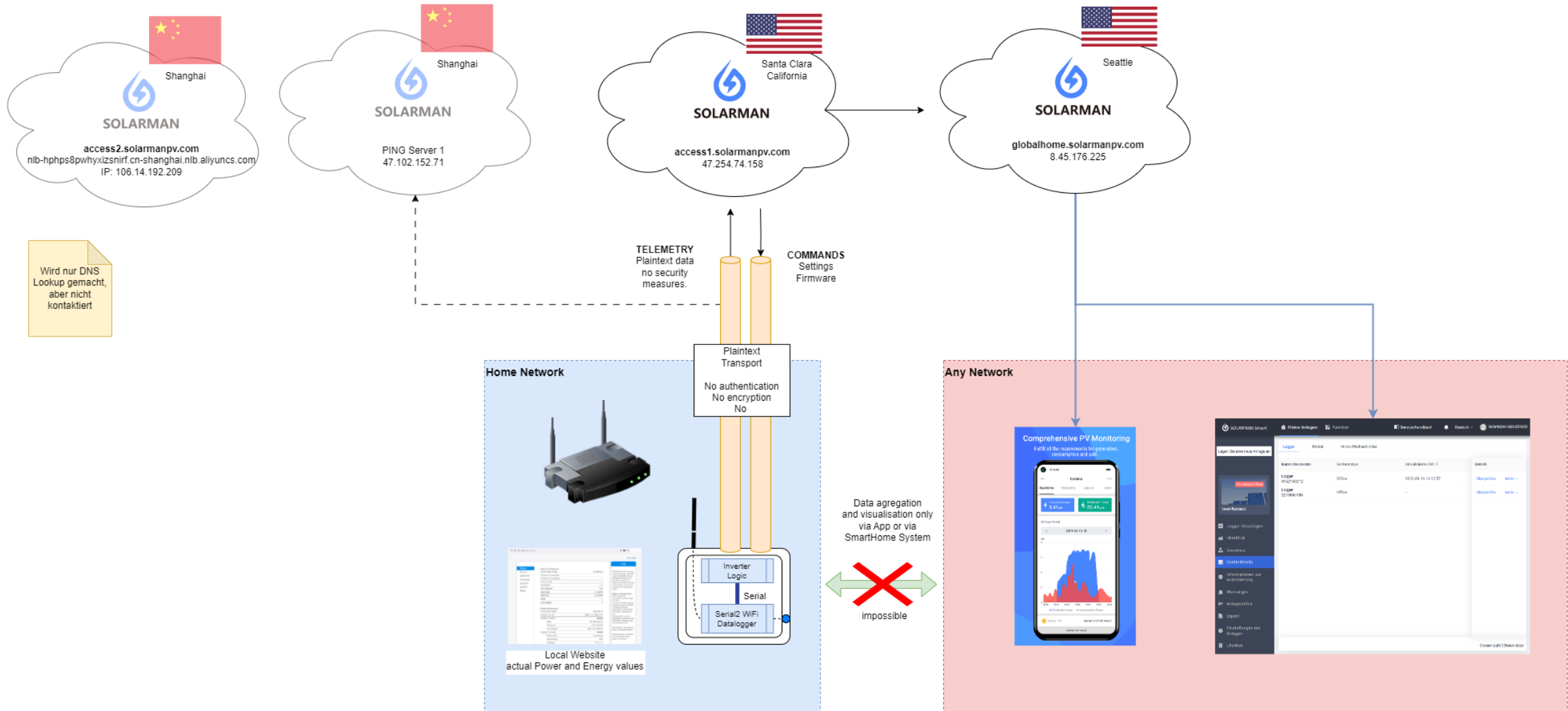
> Frame 4774: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface unknown, id 0
> Ethernet II, Src: HighFlyingE1_37:c9:b0 (40:2a:8f:37:c9:b0), Dst: AVMAudiovisu_56:f6:9d (44:4e:6d:56:f6:9d)
> Internet Protocol Version 4, Src: 10.2.2.11, Dst: 47.254.132.226
> Transmission Control Protocol, Src Port: 27168, Dst Port: 10000, Seq: 1, Ack: 1, Len: 315
v SolarmanV5 Protocol
  Start: 0xa5
  Length: 302
  Message Type: 0x4110 (Hello message, unit to cloud)
  Serial (Cloud): 0x00
  Serial (Unit): 0x01
  Logger Serial: 
  Frame Type: 0x02 (Solar Inverter)
  Delivery Time: 13272 s
  Power On Time: 3220 s
  Upload Period: 5 min
  Data Acquisition Period: 60 s
  Heart Rate: 120 s
  Signal Strength: 100
  Module Version: MW3_16U_5406_2.27
  MAC Address: 402a8f37c9b0 (HighFlyingE1_37:c9:b0)
  Local IP Number: 10.2.2.11
  AT+ Update Command Supported (?): 0xff
  Extended System Version: V1.1.00.11
  Protocol Upgrade Method (?): 0xfe
  
```

```

0000 44 4e 6d 56 f6 9d 40 2a 8f 37 c9 b0 08 00 45 00  DnmV-@* 7...E-
0010 01 63 1e a0 00 00 ff 06 db 07 0a 02 02 0b 2f fe  c......./-
0020 84 e2 6a 20 27 10 00 30 d1 03 fb fe 10 09 50 18  .j'..0.....P-
0030 11 1c 59 10 00 00 a5 2e 01 10 41 00 01  3.....<
0040 02 d8 33 00 00 94 0c 00 00 00 00 00 05 3c  .3.....<
0050 78 01 64 01 4d 57 33 5f 31 36 55 5f 35 34 30 36  x.d.MW3_16U_5406
0060 5f 32 2e 32 37 00 00 00 00 00 00 00 00 00 00  Serial 2.27...
0070 00 00 00 00 00 00 00 00 00 00 00 00 40 2a 8f 37  WiFi Name
0080 c9 b0 31 30 2e 32 2e 32 2e 31 31 00 00 00 00 00  -10.2.2.11...
0090 00 00 31 00 01 06 54 0f 00 ff 56 31 2e 31 2e 30  -1...T...V1.1.0
00a0 30 2e 31 31 00 00 00 00 00 00 00 00 00 00 00  0.11...
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00c0 00 00 fe fe 00 00 00 00 00 00 00 00 00 00 00  .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00f0 4c 61 62 4e 65 74 00 00 00 00 00 00 00 00 00  LabNet .....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  WiFi Name .....
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a7  .....
0170 15
  
```

- ▶ All messages are sent via Plain TCP
- ▶ Neither the Backend, nor the Device can be sure it's talking to the real counterpart
- ▶ Binary Data format also mainly public ally available
<https://github.com/0xb1ff/solarman-dissector/tree/main>

Meta Data Analysis



Privacy?



Before (2023)

Working mode
Working mode ▼

Save

Server A Setting
IP address
Domain name
Port
Connection ▼

Save

Optional Server Setting
IP address
Domain name
Port

After (2024)

Working mode
Working mode ▼

Save

Server A Setting
IP address
Domain name
Port
Connection ▼

Save

Optional Server Setting
IP address
Domain name
Port
Connection ▼

Changing the Management Server



65383	21:39:35,769825	10.1.1.62	8.211.53.112	TCP	397	1655 → 10000 [PSH, ACK] Seq=7444 Ack=714 Win=3667 Len=343
65384	21:39:35,790380	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=714 Ack=7787 Win=31088 Len=23
65385	21:39:35,856017	10.1.1.62	8.211.53.112	TCP	397	1655 → 10000 [PSH, ACK] Seq=7787 Ack=737 Win=3644 Len=343
65386	21:39:35,876638	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=737 Ack=8130 Win=31088 Len=23
65387	21:39:35,931065	10.1.1.62	8.211.53.112	TCP	60	1655 → 10000 [ACK] Seq=8130 Ack=760 Win=3621 Len=0
65388	21:39:35,953478	10.1.1.62	8.211.53.112	TCP	397	1655 → 10000 [PSH, ACK] Seq=8130 Ack=760 Win=3621 Len=343
65389	21:39:35,973877	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=760 Ack=8473 Win=31088 Len=23
65390	21:39:36,026511	10.1.1.62	8.211.53.112	TCP	114	1655 → 10000 [PSH, ACK] Seq=8473 Ack=783 Win=3598 Len=60
65391	21:39:36,046867	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=783 Ack=8533 Win=31088 Len=23
65395	21:39:36,111685	10.1.1.62	8.211.53.112	TCP	98	1655 → 10000 [PSH, ACK] Seq=8533 Ack=806 Win=3575 Len=44
65396	21:39:36,132165	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=806 Ack=8577 Win=31088 Len=23
65397	21:39:36,183689	10.1.1.62	8.211.53.112	TCP	60	1655 → 10000 [ACK] Seq=8577 Ack=829 Win=3552 Len=0
65398	21:39:36,193332	10.1.1.62	8.211.53.112	TCP	365	1655 → 10000 [PSH, ACK] Seq=8577 Ack=829 Win=3552 Len=311
65400	21:39:36,213615	8.211.53.112	10.1.1.62	TCP	77	10000 → 1655 [PSH, ACK] Seq=829 Ack=8888 Win=31088 Len=23
65402	21:39:36,434732	10.1.1.62	8.211.53.112	TCP	60	1655 → 10000 [ACK] Seq=8888 Ack=852 Win=3529 Len=0
65420	21:39:41,492068	8.211.53.112	10.1.1.62	TCP	139	10000 → 1655 [PSH, ACK] Seq=852 Ack=8888 Win=31088 Len=85
65421	21:39:41,540343	10.1.1.62	8.211.53.112	TCP	84	1655 → 10000 [PSH, ACK] Seq=8888 Ack=937 Win=3444 Len=30
65422	21:39:41,599820	8.211.53.112	10.1.1.62	TCP	60	10000 → 1655 [ACK] Seq=937 Ack=8918 Win=31088 Len=0
65689	21:40:22,403633	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	58892 → 40000 [FIN, ACK] Seq=193 Ack=1583 Win=2097664 Len=0
65690	21:40:22,403757	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	[TCP Retransmission] 58892 → 40000 [FIN, ACK] Seq=193 Ack=1583 Win=2097664 Len=0
65691	21:40:22,404875	fe80::36b8:4def:256...	fe80::84f2:46a9:463...	TCP	74	40000 → 58892 [FIN, ACK] Seq=1583 Ack=194 Win=64256 Len=0
65692	21:40:22,404911	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	58892 → 40000 [ACK] Seq=194 Ack=1584 Win=2097664 Len=0
65693	21:40:22,405115	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	[TCP Dup ACK 65692#1] 58892 → 40000 [ACK] Seq=194 Ack=1584 Win=2097664 Len=0
65808	21:40:41,946987	10.1.1.62	8.211.53.112	TCP	60	[TCP Keep-Alive] 1655 → 10000 [ACK] Seq=8917 Ack=937 Win=3444 Len=0
65809	21:40:41,968554	8.211.53.112	10.1.1.62	TCP	60	[TCP Keep-Alive ACK] 10000 → 1655 [ACK] Seq=937 Ack=8918 Win=31088 Len=0
65890	21:40:52,646404	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	86	58941 → 40000 [SYN] Seq=0 Win=64440 Len=0 MSS=1432 WS=256 SACK_PERM
65891	21:40:52,646513	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	86	[TCP Retransmission] 58941 → 40000 [SYN] Seq=0 Win=64440 Len=0 MSS=1432 WS=256 SACK_PERM
65892	21:40:52,647073	fe80::36b8:4def:256...	fe80::84f2:46a9:463...	TCP	86	40000 → 58941 [SYN, ACK] Seq=0 Ack=1 Win=64440 Len=0 MSS=1432 SACK_PERM WS=128
65893	21:40:52,647118	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	58941 → 40000 [ACK] Seq=1 Ack=1 Win=2097664 Len=0
65894	21:40:52,647202	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	[TCP Dup ACK 65893#1] 58941 → 40000 [ACK] Seq=1 Ack=1 Win=2097664 Len=0
65895	21:40:52,647205	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	266	58941 → 40000 [PSH, ACK] Seq=1 Ack=1 Win=2097664 Len=192 [TCP segment of a reassembled PDU]
65896	21:40:52,647287	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	266	[TCP Retransmission] 58941 → 40000 [PSH, ACK] Seq=1 Ack=1 Win=2097664 Len=192
65897	21:40:52,647538	fe80::36b8:4def:256...	fe80::84f2:46a9:463...	TCP	74	40000 → 58941 [ACK] Seq=1 Ack=193 Win=64256 Len=0
65898	21:40:52,652054	fe80::36b8:4def:256...	fe80::84f2:46a9:463...	TCP	226	40000 → 58941 [PSH, ACK] Seq=1 Ack=193 Win=64256 Len=152 [TCP segment of a reassembled PDU]
65899	21:40:52,652176	fe80::36b8:4def:256...	fe80::84f2:46a9:463...	TCP	1504	40000 → 58941 [PSH, ACK] Seq=153 Ack=193 Win=64256 Len=1430 [TCP segment of a reassembled PDU]
65900	21:40:52,652194	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	58941 → 40000 [ACK] Seq=193 Ack=1583 Win=2097664 Len=0
65901	21:40:52,652280	fe80::84f2:46a9:463...	fe80::36b8:4def:256...	TCP	74	[TCP Dup ACK 65900#1] 58941 → 40000 [ACK] Seq=193 Ack=1583 Win=2097664 Len=0
65911	21:40:55,858467	10.1.1.62	8.211.53.112	TCP	68	1655 → 10000 [PSH, ACK] Seq=8918 Ack=937 Win=3444 Len=14

Source Port: 10000
Destination Port: 1655
[Stream index: 85]

> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 85]
Sequence Number: 852 (relative sequence number)
Sequence Number (raw): 2970229659
[Next Sequence Number: 937 (relative sequence number)]
Acknowledgment Number: 8888 (relative ack number)
Acknowledgment number (raw): 15488
0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Flags (12 bits) (tcp.flags), 2 Bytes

```

0000 44 4e 6d 56 f6 9a 1c ed 6f 7a 42 5a 08 00 45 00  DNmV... ozBZ..E.
0010 00 7d 0d 54 00 00 34 06 ef a5 08 d3 35 70 0a 01  .}T@ 4. ....Sp.
0020 01 3e 27 10 06 77 b1 0a 1b 9b 00 00 3c 80 50 18  ->...w.....<P.
0030 79 70 60 f5 00 00 a5 48 00 10 45 c9 01 02 a5 32  yp'...H ..E...Z
0040 ee 01 08 54 00 00 00 00 00 00 00 00 8b 46 a4 65  T...
0050 41 54 2b 43 4e 4d 4f 53 41 56 45 3d 32 31 34 30  AT+CNMOS AVE=2140
0060 32 38 2c 30 2c 32 2c 32 30 2c 30 2c 35 34 30 36  28,0,2,2 0,0,5406
0070 2e 64 65 76 69 63 65 61 63 63 65 73 73 2e 68 6f  .devicea ccess.ho
0080 73 74 2c 31 30 30 30 30 0d b4 15  st,10000 ...

```

Pakete: 67732 · Angezeigt: 34765 (51.3%)



Remote Software Update

5267	20:37:00,086596	10.2.2.11	10.2.2.50	TCP	60 80 → 58875 [ACK] Seq=2 Ack=350 Win=4031 Len=0
5268	20:37:00,516535	47.254.132.226	10.2.2.11	SOLARMANV5	150 10000 → 27168 [PSH, ACK] Seq=599 Ack=5130 Win=31088 Len=96
5269	20:37:00,538863	10.2.2.11	47.254.132.226	SOLARMANV5	104 27168 → 10000 [PSH, ACK] Seq=5130 Ack=695 Win=3686 Len=96
5270	20:37:00,601274	47.254.132.226	10.2.2.11	TCP	54 10000 → 27168 [ACK] Seq=695 Ack=5180 Win=31088 Len=0
5271	20:37:00,605286	10.2.2.11	47.254.132.226	SOLARMANV5	104 27168 → 10000 [PSH, ACK] Seq=5180 Ack=695 Win=3686 Len=96
5272	20:37:00,628252	47.254.132.226	10.2.2.11	TCP	54 10000 → 27168 [ACK] Seq=695 Ack=5230 Win=31088 Len=0

> Packet comments

- > Frame 5268: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface unknown, id 0
- > Ethernet II, Src: AVMAudiovisu_56:f6:9d (44:4e:6d:56:f6:9d), Dst: HighFlyingEl_37:c9:b0 (40:2a:8f:37:c9:b0)
- > Internet Protocol Version 4, Src: 47.254.132.226, Dst: 10.2.2.11
- > Transmission Control Protocol, Src Port: 10000, Dst Port: 27168, Seq: 599, Ack: 5130, Len: 96
- > SolarmanV5 Protocol
 - Start: 0xa5
 - Length: 83
 - Message Type: 0x4510 (Unknown)
 - Serial (Cloud): 0xc8
 - Serial (Unit): 0x01
 - Logger Serial: 3996296450
 - Frame Type: 0x01 (Data Logging Stick)

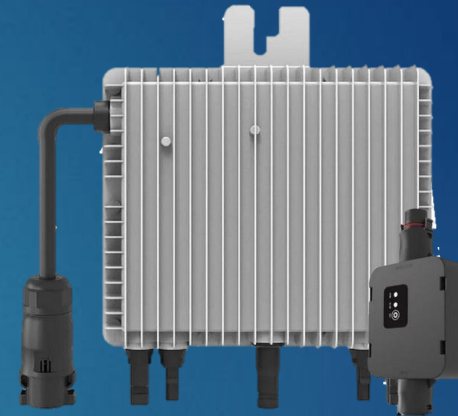
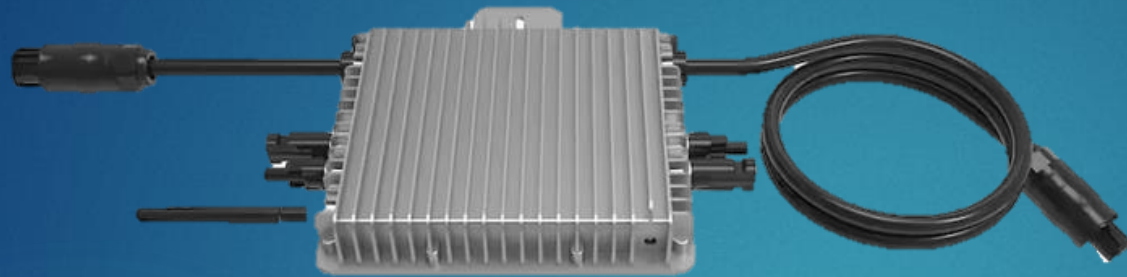

```

0000 40 2a 8f 37 c9 b0 44 4e 6d 56 f6 9d 08 00 45 00  @*.7..DN mV....E.
0010 00 88 7f 6b 40 00 33 06 07 18 2f fe 84 e2 0a 02  ...k@.3.../.....
0020 02 0b 27 10 6a 20 fb fe 12 5f 00 30 e5 0c 50 18  ...j..._0..P.
0030 79 70 6c 31 00 00 a5 53 00 10 45 c8 01 02 a5 32  yp11...S ..E....2
0040 ee 01 13 54 00 00 00 00 00 00 00 00 eb 45 a4 65  ...T....E.e
0050 41 54 2b 55 50 55 52 4c 3d 68 74 74 70 3a 2f 2f  AT+UPURL =http://
0060 34 37 2e 32 35 34 2e 33 36 2e 36 36 3a 38 30 2f  47.254.3 6.66:80/
0070 30 5f 44 30 30 30 32 5f 31 38 2f 4d 57 33 5f 31  0_D0002_18/MW3_1
0080 36 55 5f 35 34 30 36 5f 32 2e 33 32 2d 44 31 2e  6U_5406_2.32-D1.
0090 62 69 6e 0d e2 15  bin...
    
```

- ▶ Server not uses Server name and no TLS → Server not authenticated
- ▶ **RISK: Device could fetch Firmware also from untrusted origin!**
- ▶ Server not in the EU
- ▶ ...
- ▶ **Currently no downgrade protection**

Geolocation data from IP2Location (Product: DB6, 2024-1-1)

IP ADDRESS: 47.254.36.66	ISP: AliCloud
COUNTRY: United States	ORGANIZATION: Not available
REGION: California	LATITUDE: 34.0526
CITY: Los Angeles	LONGITUDE: -118.2439



Firmware Features

WHAT ELSE CAN WE DO?

TCP Channel 2

TCP Channel 1

AT Commands



- ▶ Web Page User and Password
- ▶ Wi-Fi Settings can be read out from TCP1 and TCP2

```

micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd/build main ./main -t 10.2.2.11:48899
2024/01/17 08:31:28 * Connecting :0 -> 10.2.2.11:48899...
2024/01/17 08:31:36 AP settings
2024/01/17 08:31:36 Mode, SSID and Chanel: 11BGN,AP_3996296450,AUTO
2024/01/17 08:31:36 Encryption: WPA2PSK,AES,81084a86
2024/01/17 08:31:36 Station settings
2024/01/17 08:31:36 SSID: solarLabNet
2024/01/17 08:31:36 Key: WPA2PSK,AES,2024!Solar!Hacking!
2024/01/17 08:31:36 IP: DHCP,10.2.2.11,255.255.255.0,10.2.2.1
2024/01/17 08:31:36 Web settings
2024/01/17 08:31:36 Login: admin,admin
2024/01/17 08:31:37
micro@micro-Latitude-7490 ~/GIT/deye-logg

```

```

$ ./main.exe -t 10.10.100.254:48899
2023/09/22 15:05:25 * Connecting :0 -> 10.10.100.254:48899...
2023/09/22 15:05:33 AP settings
2023/09/22 15:05:33 Mode, SSID and Chanel: 11BGN,AP_416700017001,AUTO
2023/09/22 15:05:33 Encryption: WPA2PSK,AES,12345678
2023/09/22 15:05:33 Station settings
2023/09/22 15:05:33 SSID: FRITZ!Box 6490 Cable
2023/09/22 15:05:33 Key: WPA2PSK,AES,1374
2023/09/22 15:05:33 IP: DHCP,0.0.0.0,0.0.0.0,0.0.0.0
2023/09/22 15:05:33 Web settings
2023/09/22 15:05:33 Login: admin,admin
2023/09/22 15:05:34

```

Id	Id	Id	Id	Id
1	At+key	Set/get Device Password	AT+KEY	+OK:216428
2	At+time	Set/get Device Time	AT+TIME	+OK:60,320
3	At+time	Set/get Device Time	AT+TIME	+OK:60,320
4	At+time	Set/get Device Time	AT+TIME	+OK:60,320
5	At+time	Set/get Device Time	AT+TIME	+OK:60,320
6	At+time	Set/get Device Time	AT+TIME	+OK:60,320
7	At+time	Set/get Device Time	AT+TIME	+OK:60,320
8	At+time	Set/get Device Time	AT+TIME	+OK:60,320
9	At+time	Set/get Device Time	AT+TIME	+OK:60,320
10	At+time	Set/get Device Time	AT+TIME	+OK:60,320
11	At+time	Set/get Device Time	AT+TIME	+OK:60,320
12	At+time	Set/get Device Time	AT+TIME	+OK:60,320
13	At+time	Set/get Device Time	AT+TIME	+OK:60,320
14	At+time	Set/get Device Time	AT+TIME	+OK:60,320
15	At+time	Set/get Device Time	AT+TIME	+OK:60,320
16	At+time	Set/get Device Time	AT+TIME	+OK:60,320
17	At+time	Set/get Device Time	AT+TIME	+OK:60,320
18	At+time	Set/get Device Time	AT+TIME	+OK:60,320
19	At+time	Set/get Device Time	AT+TIME	+OK:60,320
20	At+time	Set/get Device Time	AT+TIME	+OK:60,320
21	At+time	Set/get Device Time	AT+TIME	+OK:60,320
22	At+time	Set/get Device Time	AT+TIME	+OK:60,320
23	At+time	Set/get Device Time	AT+TIME	+OK:60,320
24	At+time	Set/get Device Time	AT+TIME	+OK:60,320
25	At+time	Set/get Device Time	AT+TIME	+OK:60,320
26	At+time	Set/get Device Time	AT+TIME	+OK:60,320
27	At+time	Set/get Device Time	AT+TIME	+OK:60,320
28	At+time	Set/get Device Time	AT+TIME	+OK:60,320
29	At+time	Set/get Device Time	AT+TIME	+OK:60,320
30	At+time	Set/get Device Time	AT+TIME	+OK:60,320
31	At+time	Set/get Device Time	AT+TIME	+OK:60,320
32	At+time	Set/get Device Time	AT+TIME	+OK:60,320
33	At+time	Set/get Device Time	AT+TIME	+OK:60,320
34	At+time	Set/get Device Time	AT+TIME	+OK:60,320
35	At+time	Set/get Device Time	AT+TIME	+OK:60,320
36	At+time	Set/get Device Time	AT+TIME	+OK:60,320
37	At+time	Set/get Device Time	AT+TIME	+OK:60,320
38	At+time	Set/get Device Time	AT+TIME	+OK:60,320
39	At+time	Set/get Device Time	AT+TIME	+OK:60,320
40	At+time	Set/get Device Time	AT+TIME	+OK:60,320
41	At+time	Set/get Device Time	AT+TIME	+OK:60,320
42	At+time	Set/get Device Time	AT+TIME	+OK:60,320
43	At+time	Set/get Device Time	AT+TIME	+OK:60,320
44	At+time	Set/get Device Time	AT+TIME	+OK:60,320
45	At+time	Set/get Device Time	AT+TIME	+OK:60,320
46	At+time	Set/get Device Time	AT+TIME	+OK:60,320
47	At+time	Set/get Device Time	AT+TIME	+OK:60,320
48	At+time	Set/get Device Time	AT+TIME	+OK:60,320
49	At+time	Set/get Device Time	AT+TIME	+OK:60,320
50	At+time	Set/get Device Time	AT+TIME	+OK:60,320
51	At+time	Set/get Device Time	AT+TIME	+OK:60,320
52	At+time	Set/get Device Time	AT+TIME	+OK:60,320
53	At+time	Set/get Device Time	AT+TIME	+OK:60,320
54	At+time	Set/get Device Time	AT+TIME	+OK:60,320
55	At+time	Set/get Device Time	AT+TIME	+OK:60,320
56	At+time	Set/get Device Time	AT+TIME	+OK:60,320
57	At+time	Set/get Device Time	AT+TIME	+OK:60,320
58	At+time	Set/get Device Time	AT+TIME	+OK:60,320
59	At+time	Set/get Device Time	AT+TIME	+OK:60,320
60	At+time	Set/get Device Time	AT+TIME	+OK:60,320
61	At+time	Set/get Device Time	AT+TIME	+OK:60,320
62	At+time	Set/get Device Time	AT+TIME	+OK:60,320
63	At+time	Set/get Device Time	AT+TIME	+OK:60,320
64	At+time	Set/get Device Time	AT+TIME	+OK:60,320
65	At+time	Set/get Device Time	AT+TIME	+OK:60,320
66	At+time	Set/get Device Time	AT+TIME	+OK:60,320
67	At+time	Set/get Device Time	AT+TIME	+OK:60,320
68	At+time	Set/get Device Time	AT+TIME	+OK:60,320
69	At+time	Set/get Device Time	AT+TIME	+OK:60,320
70	At+time	Set/get Device Time	AT+TIME	+OK:60,320
71	At+time	Set/get Device Time	AT+TIME	+OK:60,320
72	At+time	Set/get Device Time	AT+TIME	+OK:60,320
73	At+time	Set/get Device Time	AT+TIME	+OK:60,320
74	At+time	Set/get Device Time	AT+TIME	+OK:60,320
75	At+time	Set/get Device Time	AT+TIME	+OK:60,320
76	At+time	Set/get Device Time	AT+TIME	+OK:60,320
77	At+time	Set/get Device Time	AT+TIME	+OK:60,320
78	At+time	Set/get Device Time	AT+TIME	+OK:60,320
79	At+time	Set/get Device Time	AT+TIME	+OK:60,320
80	At+time	Set/get Device Time	AT+TIME	+OK:60,320
81	At+time	Set/get Device Time	AT+TIME	+OK:60,320
82	At+time	Set/get Device Time	AT+TIME	+OK:60,320
83	At+time	Set/get Device Time	AT+TIME	+OK:60,320
84	At+time	Set/get Device Time	AT+TIME	+OK:60,320
85	At+time	Set/get Device Time	AT+TIME	+OK:60,320
86	At+time	Set/get Device Time	AT+TIME	+OK:60,320
87	At+time	Set/get Device Time	AT+TIME	+OK:60,320
88	At+time	Set/get Device Time	AT+TIME	+OK:60,320
89	At+time	Set/get Device Time	AT+TIME	+OK:60,320
90	At+time	Set/get Device Time	AT+TIME	+OK:60,320
91	At+time	Set/get Device Time	AT+TIME	+OK:60,320
92	At+time	Set/get Device Time	AT+TIME	+OK:60,320
93	At+time	Set/get Device Time	AT+TIME	+OK:60,320
94	At+time	Set/get Device Time	AT+TIME	+OK:60,320
95	At+time	Set/get Device Time	AT+TIME	+OK:60,320
96	At+time	Set/get Device Time	AT+TIME	+OK:60,320
97	At+time	Set/get Device Time	AT+TIME	+OK:60,320
98	At+time	Set/get Device Time	AT+TIME	+OK:60,320
99	At+time	Set/get Device Time	AT+TIME	+OK:60,320
100	At+time	Set/get Device Time	AT+TIME	+OK:60,320

109 AT Commands

This could happen if you just threw things away

Reference: <https://github.com/s10l/deye-logger-at-cmd/tree/main>

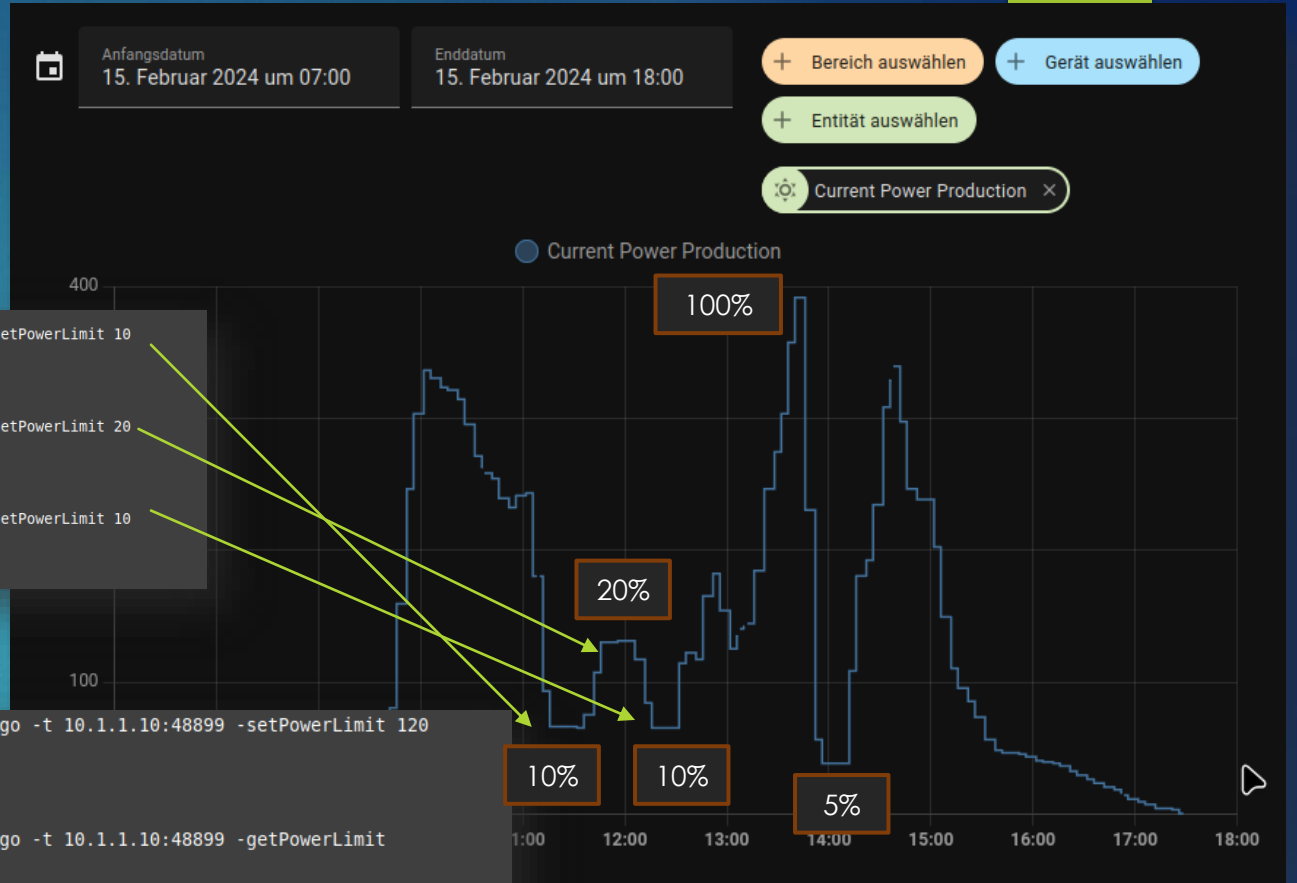
TCP Channel 2

TCP Channel 1

Unlimited Power?

```
2024/02/15 10:59:31
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -setPowerLimit 10
2024/02/15 11:00:40 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 11:00:43 +ok=01100028000181C1
2024/02/15 11:00:43 The PowerLimit is set to 10%
2024/02/15 11:00:44
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -setPowerLimit 20
2024/02/15 11:32:38 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 11:32:41 +ok=01100028000181C1
2024/02/15 11:32:41 The PowerLimit is set to 20%
2024/02/15 11:32:42
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -setPowerLimit 10
2024/02/15 12:02:05 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 12:02:08 +ok=01100028000181C1
2024/02/15 12:02:08 The PowerLimit is set to 10%
```

```
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -setPowerLimit 120
2024/02/15 12:29:32 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 12:29:35 +ok=01100028000181C1
2024/02/15 12:29:35 The PowerLimit is set to 120%
2024/02/15 12:29:36
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -getPowerLimit
2024/02/15 12:29:39 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 12:29:42 Raw Modbus read response: +ok=0103020078B866
2024/02/15 12:29:42 Cleaned Modbus read response: +ok=0103020078B866
2024/02/15 12:29:42 The PowerLimit is 120%
2024/02/15 12:29:42 Extracted Hex Value: 0078 (interpreted as 120%)
2024/02/15 12:29:43
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -setPowerLimit 100
2024/02/15 12:29:47 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 12:29:50 +ok=01100028000181C1
2024/02/15 12:29:50 The PowerLimit is set to 100%
2024/02/15 12:29:51
micro@micro-Latitude-7490 ~/GIT/deye-logger-at-cmd  feature power-throttle ± go run src/main.go -t 10.1.1.10:48899 -getPowerLimit
2024/02/15 12:29:53 * Connecting :0 -> 10.1.1.10:48899...
2024/02/15 12:29:56 Raw Modbus read response: +ok=0103020064B9AF
2024/02/15 12:29:56 Cleaned Modbus read response: +ok=0103020064B9AF
2024/02/15 12:29:56 The PowerLimit is 100%
2024/02/15 12:29:56 Extracted Hex Value: 0064 (interpreted as 100%)
```



<https://github.com/s10l/deye-logger-at-cmd> (own branch ;-)



Risk Assessment

AT A GLANCE

Attacker



- BE: Remote attacker with access to data backend
- SUPL: Supplier with access to remote management functions
- ATM: Adversary in the middle, communication interceptions
- LAT: Local adjacent attacker - not the owner, but in Wi-Fi Range
- OW: Owner and user of the system, in the same Wi-Fi network

Assets



- ▶ Energy Production (Av)
- ▶ Inverter Hardware (I, Safety)
- ▶ Energy Grid (Av)
- ▶ Customer WiFi Network (Av, C)
- ▶ Customer Privacy (C)
- ▶ Backend Database (C, I, Av)

Damage Scenarios

- ▶ Device Damaged by unsafe electrical parameters
- ▶ Destabilizing power grid
- ▶ Loss of personal data like credentials to home routers
- ▶ Solar Inverter Bot-Net



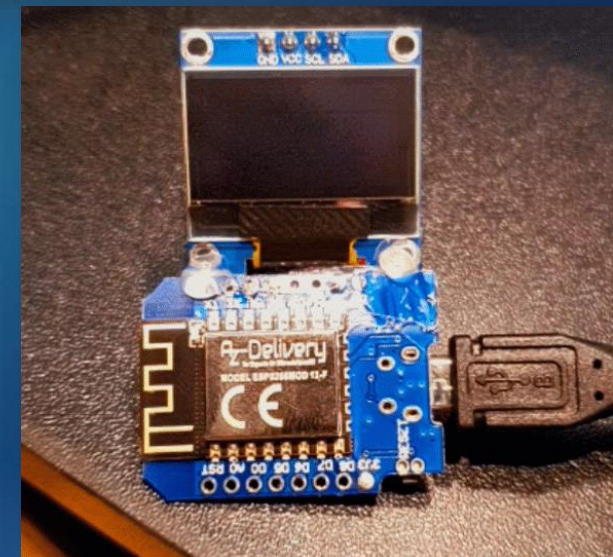
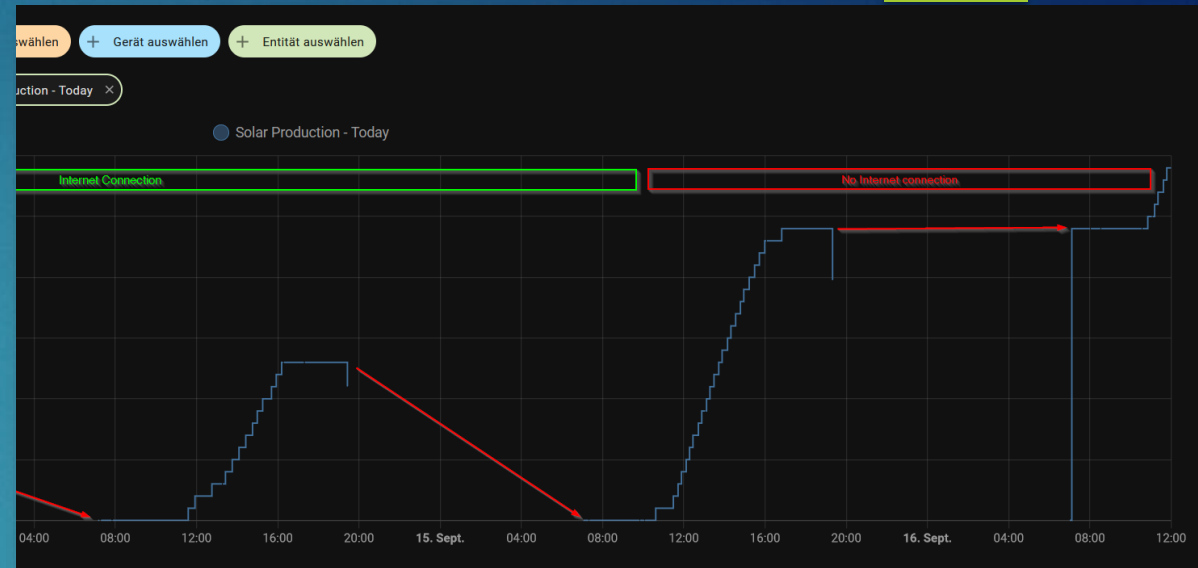
Mitigations?

HOW TO PROTECT AND MITIGATE RISK

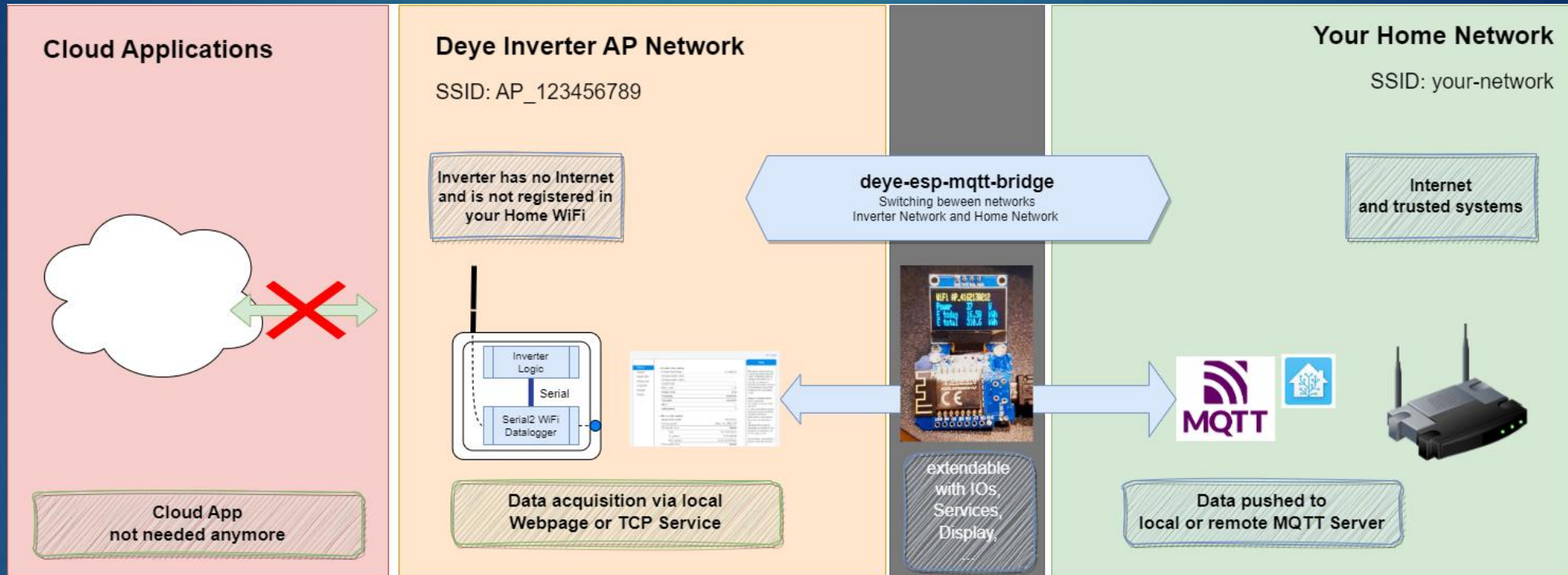
Mitigation Options



- ▶ No WiFi at all
 - ▶ WiFi Power Meter
 - ▶ z.B. Tasmota
- ▶ Kindersicherung
 - ▶ No Internet / 5 Minutes Internet
 - ▶ Server Settings or own-backend
- ▶ Firmware Sanitation
- ▶ WiFi „Bridge“



Maker Projects



Screen Scraping

MODBUS

MQTT

DISPLAY

Security

Contributors welcome!

<https://github.com/marxram/deye-esp-mqtt-bridge>

Improvements

- ▶ **Earlier**
 - ▶ Backend Servers **hosted in the USA**
- ▶ Servers (now) seem to be in **Europe**
 - ▶ Have been US before



- ▶ **Earlier**
 - ▶ Wi-Fi SSID: AP_SERIALNUMBER
 - ▶ Wi-Fi PSWD: **12345678**

- ▶ **Now**
 - ▶ Wi-Fi SSID: AP_SERIALNUMBER
 - ▶ PSWD: **Random with QR Tag**



Disclosure



- ▶ All points were brought to IGEN-Tech (Backend Provider)
- ▶ We made Quick Fix Proposal
- ▶ Product Management is working on solution
- ▶ Some things cannot fixed
- ▶ New devices likely better security
- ▶ **Next fix release planned for March 2024**

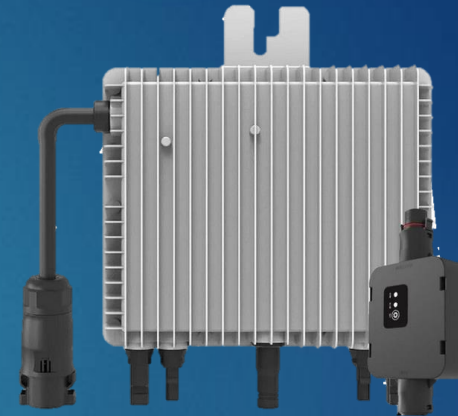
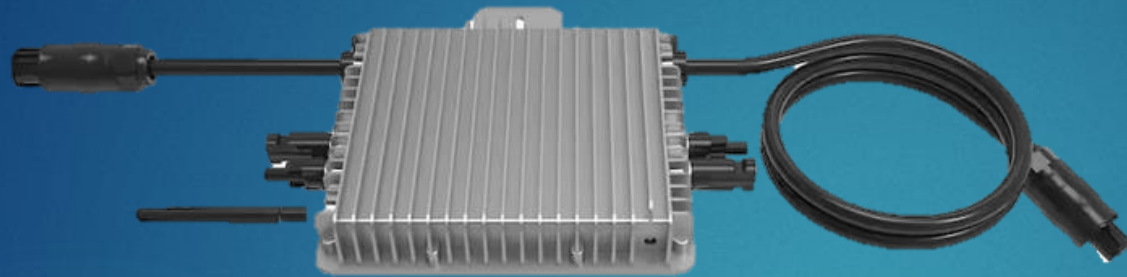
Quick Fixes

Short Term doable

- ▶ Get rid of special AT commands
 - ▶ Get PWD
 - ▶ Get WiFi PWD
- ▶ Let the user set a local PSWD
 - ▶ Power reduction only with customer in the loop
- ▶ Security and Privacy by design
 - ▶ Opt-In to data transmission → TCP1 not on by default

Mid Term doable

- ▶ Community Connectivity
- ▶ Extra Edge devices / bridges



Can we do it better?

General Security Requirements



- ▶ **Local Authentication**
 - ▶ **Individual Password to protect important functionalities (*ETSI 303645 P5.1)**
- ▶ **Authenticated and Encrypted Communication (*ETSI 303645 P5.5)**
 - ▶ **mTLS**
- ▶ **Vulnerability Management / Secure Software Updates (*ETSI 303645 P5.2)**
 - ▶ **Only recent and authentic OEM firmware to be installed**
- ▶ **Securely Store Credentials (*ETSI 303645 P5.4)**
 - ▶ **User and Password, WiFi Credentials**
- ▶ **Potential new concepts / Mitigation**
 - ▶ **Network Island Mode (*ETSI 303645 P5.5)**
 - ▶ Interfaces to use in smart-home only (read telemetry and set the time etc)
 - ▶ **Privacy Protection (*ETSI 303645 P5.8)**
 - ▶ Option: Island Mode by default: Connected Mode only if user accepts statement

*Possible Standard: ETSI EN 303 645 „Cyber Security for Consumer Internet of Things“

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

Take Home / Denkanstöße

- ▶ Das Problem wächst (noch)
 - ▶ Lifetime
 - ▶ Grid Situation
 - ▶ Reputation
- ▶ Responsibilities
- ▶ Complex Environment with a lot of legacy hardware

Thanks for listening!



- ▶ **Bastian Widmer**
- ▶ hello@bastianwidmer.ch
- ▶ bastianwidmer.ch
- ▶ [@dasrecht@chaos.social](https://twitter.com/dasrecht)



- ▶ **Roland Marx**
- ▶ solar@marxram-consulting.com
- ▶ <https://de.linkedin.com/in/marxram>
- ▶ <https://github.com/marxram/deye-esp-mqtt-bridge>