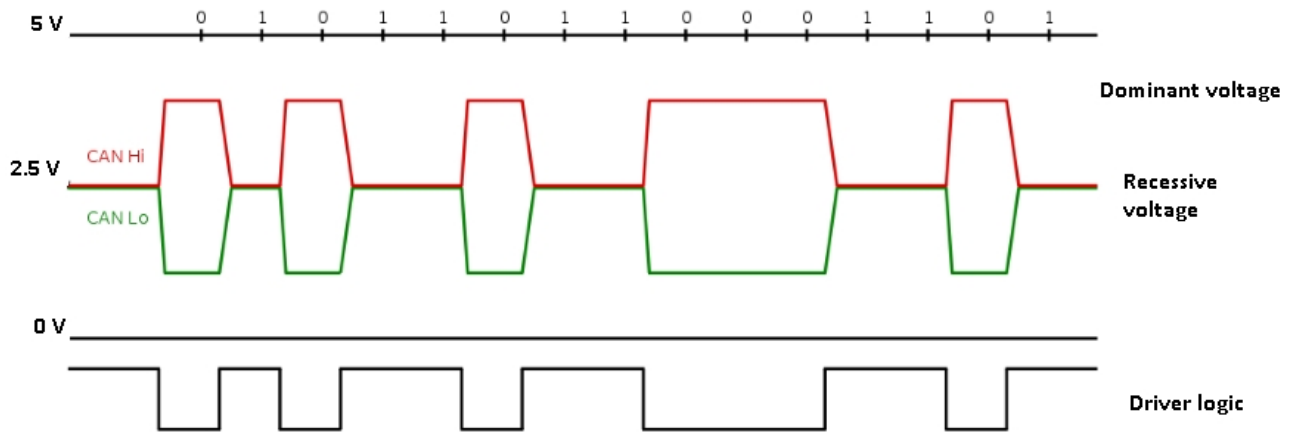


# turbolevo

## [canbus]

- [canbus basic](#)
- [exploring canbus](#)
- [canbus esp32 project](#)
- [tutorial](#)
- [transceiver SN65HVD230 datasheet example ESP32 project](#)
- [transreiever TJA1050T: datasheet](#)

High-speed CAN signaling per ISO 11898-2

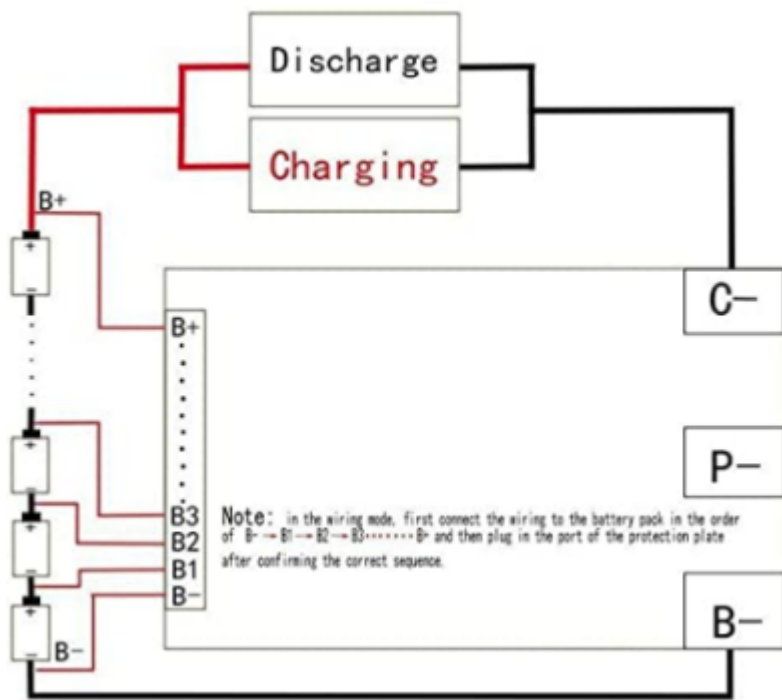


## firmware

- [firmware\\_status.json](#)
  - [firmware.bin](#)

# BMS

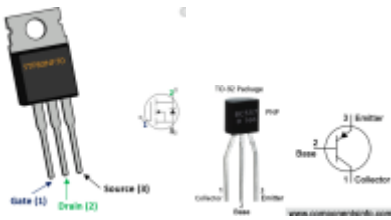
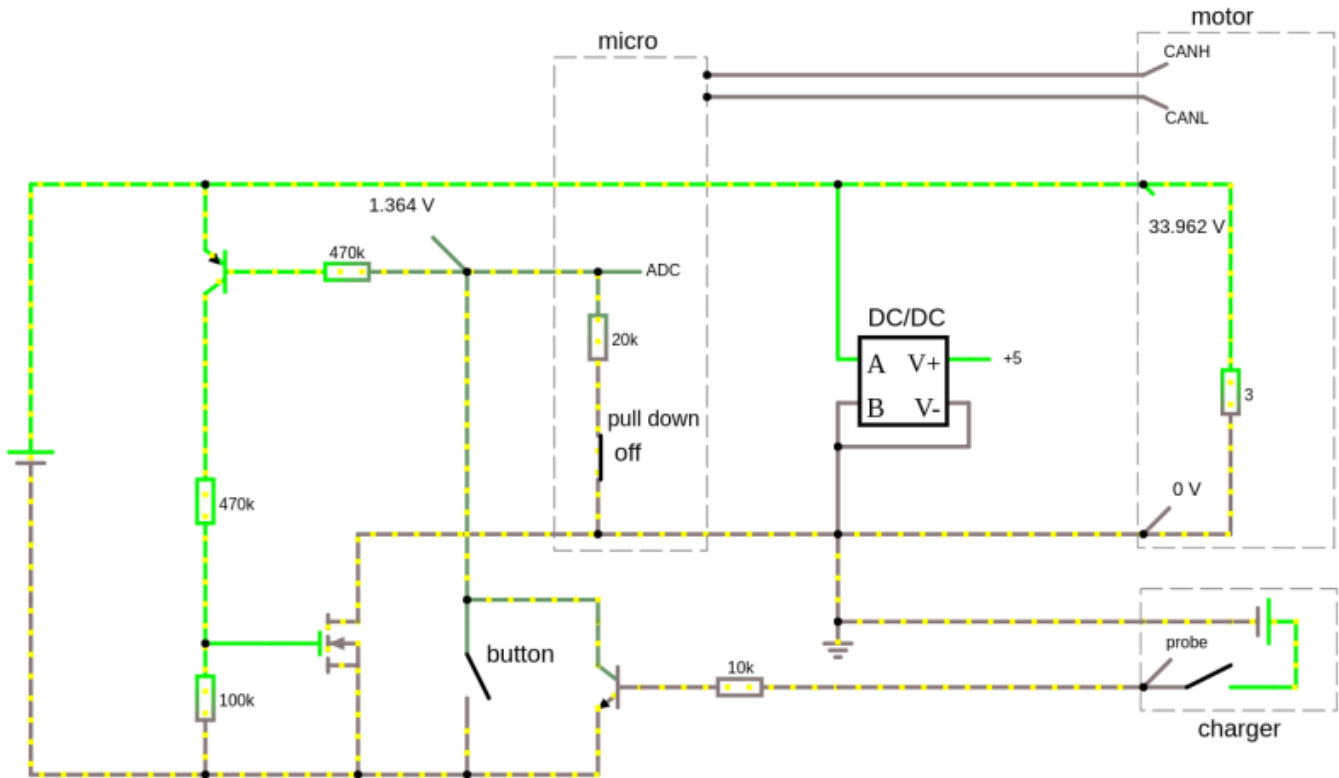
Same port charge and discharge balance PCM for 36V



- B-: Connect to the negative pole of the battery pack
- P-: No Connect
- C-: Connect to the negative electrode of charge and discharge

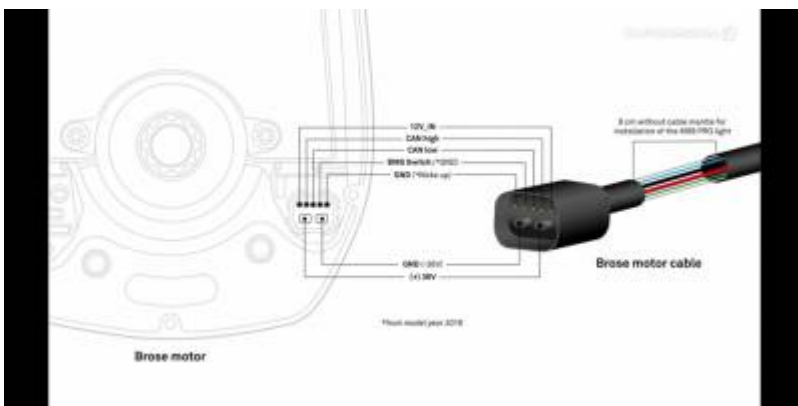
Please connect B- line firstly, and then connect voltage monitoring wiring harness. The last step is to connect charge and discharge lines. If you want to remove them, the order should be reversed. Please pay attention to the connection order, or it will damage the component.

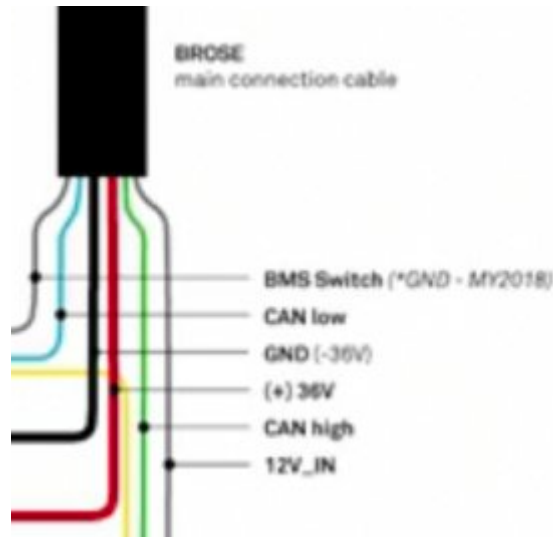
## Electronic



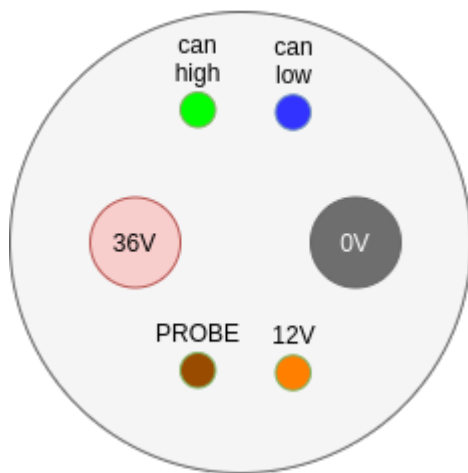
- [https://lsc.com/product-detail/DC-DC-Converters\\_UMW-Youtai-Semiconductor-Co-Ltd-LM2596S-3-3\\_C347420.html](https://lsc.com/product-detail/DC-DC-Converters_UMW-Youtai-Semiconductor-Co-Ltd-LM2596S-3-3_C347420.html)

## turbo levo





Female front view



- il bms viene attivato da una tensione di controllo di 5v sul cavo marrone
- a bms attivo compare 12v sul cavo arancione
- il caricabatterie viene attivato da NTC sul pin ?
- I dati sono fondamentalmente "little endian", cioè a1 fe ff è 0xFFFFFEA1.
- Corrente, tensione e i valori di capacità sono per lo più "volte 1000"

combinazione non funzionante scheda massimo: motore 5.0.4, bms 2.23.1

## Pican2

- [manual](#)

turbo levo: 250khz canbus

```
sudo ip link set can0 up type can bitrate 250000
```

or

[/etc/network/interfaces](#)

```

auto can0
  iface can0 inet manual
  pre-up /sbin/ip link set can0 type can bitrate 250000
  up /sbin/ifconfig can0 up
  down /sbin/ifconfig can0 down

```

```
cansniffer can0 -c -t 0
```

```

0.000000 100 03 22 02 06 00 00 00 00 .".....
0.000000 101 05 62 02 06 F5 08 FA B2 .b.....
0.000000 200 60 00 14 DA 05 00 00 00 `.....
0.000000 201 00 00 00 00 62          ....b
0.000000 202 DA 16 00 00 74 80 03 00 ....t...
0.000000 203 00 00 00 00 00 00 0B 00 .....
0.000000 204 00 00 00 00 00 00 00 00 .....
0.000000 300 03 5A 0B 5A 28 00 64      .Z.Z(.d.
0.000000 400 01 00 0C 00              ....
0.500217 401 FA A0 00 00 00 00 00 00 .....
0.000000 402 60 00 00 00 14 DA 05 00 `.....
0.000000 403 5C 00 00 00 D4 0D 06 00 \.....
0.126410 450 09 01                  ..
0.149914 451 09 01 00 00 64          ....d
0.000000 454 03 5A 0B 5A 28 00 64      .Z.Z(.d
0.000000 665 00 00 00 00 53 17 53 00 ....S.S.
0.000000 666 52 07 01 01 52 01 62 26 R...R.b&

```

senza assistenza non funzionante

```

0.000092 200 5D 00 CC AC 05 00 01 00 ].....
0.000000 201 00 00 00 00 62          ....b
0.000000 202 DA 13 00 00 6A D9 03 00 ....j...
0.000000 203 00 00 00 00 00 00 0A 00 .....
0.000000 204 00 00 00 00 00 00 00 00 .....
0.000000 300 03 5A 0B 5A 23 00 23      .Z.Z#.#
0.000000 400 01 00 0C 00              ....
0.000000 401 CA A0 00 00 00 00 00 00 .....
0.000000 402 5D 00 00 00 CC AC 05 00 ].....
0.000000 403 5C 00 00 00 D4 0D 06 00 \.....
0.000000 450 10 01                  ..
0.000000 665 00 00 00 00 53 17 53 00 ....S.S.
0.000000 666 52 07 01 01 52 01 62 26 R...R.b&

```

filtrare i messaggi con id 300 (il 777 è una netmask)

```
candump can0,300:777
```

record traffic

```
candump -l can0
```

analyze

```
log2asc -I candump-2021-03-17_135219.log can0
```

## canbus turbo levo

livelli di assistenza dal più basso

```
300 03 5A 0B 5A 23 00 23
300 03 5A 0B 5A 28 00 64
300 03 5A 0B 5A 64 00 64
```

## comandi e notifiche dalla batteria

**300** comando assistenza ogni 50ms:

- la batteria manda un codice: 300#03ww0B5Aaa00pp
  - aa: assistenza (esempio 0x28 che corrisponde a 40 in decimale)
  - pp: picco (esempio 0x64 che corrisponde a 100 in decimale)
  - ww: walk a A5. Quando non attivo 5A
- il motore risponde: 454#035A0B5Aaa00pp

**400** ?? ogni 100ms: 400#01 00 0C 00

**401** ?? ogni 100ms: 401#**CA A0** 00 00 00 00 00

- A0CA = 41162mV = **41.162V**

**402** ?? ogni 3s: 402#**5D** 00 00 00 CC AC 05 00

- 5D = **93%**
- 0005ACCC = 371916mWh = **371.916Wh**

**403** capacità massima (divisa per 1.12) ogni 3s: 403#5C 00 00 00 **D4 0D 06 00**

- 0x00060DD4 = 396756mWh = **396.756Wh** → 396.7561.12 = **444wH** ===== ??? ===== \*  
100#300000 solo 3 volte ogni 50ms un messaggio 450 \* 450#0601 \* 450#0801 \* 450#0901 \*  
450#1001 solo una volta \* 100#0322020200000000 \* 100#0322020300000000 \*  
100#0322020400000000 \* 100#0322020700000000 \* 100#0322020600000000 solo una volta  
\* 101#101B620202433937 \* 101#213237322D313030 \* 101#223230313230382D \*  
101#23332D3531373700 \* 101#1017620203393833 \* 101#2137303130323033 \*  
101#2231323230333031 \* 101#23343631BFA60001 \* 101#1017620204575342 \*  
101#2143363031313135 \* 101#223531334E000000 \* 101#23000000BFA60001 \*  
101#05620207B80BFAB2 \* 101#05620206F508FAB2 ===== notifiche dal motore ===== \*  
**454** stato assistenza ogni 50ms: 454#03ww0B5Aaa00pp \* 454#035A0B5A**1E**000A pulsante - \*  
454#03**A5**0B5A**1E**0023 walk \* 454#035A0B5A**1E**0023 eco \* 454#035A0B5A**28**000A pulsante - \*  
\* 454#035A0B5A**28**000E pulsante + \* 454#035A0B5A**28**005A trail \* 454#035A0B5A**5F**000E

- pulsante - \* 454#035A0B5A5F0021 ??? \* 454#035A0B5A5F0064 turbo \*
- 454#035A0BA55F0064 ??? \* 451#0601000023 ogni 500ms: 451#06010000ee eco medio \*
- 451#0801000028 ogni 500ms: 451#08010000rr trail medio \* 451#0901000064 ogni 500ms:
- 451#09010000tt turbo medio \* 451#10010000236464 ogni 500ms: 451#10010000EERRTT
- valori di picco \* 200#640000000000xx80 ogni 3000ms: xx=00,01,02 \* 201#xxyy00000062
- ogni 100ms velocità yy256+xx
- 202#DA0C000011E00300 ogni 1000ms
  - 203#000000000000FF0F ogni 100ms
  - 204#0000000008000000 ogni 1000ms
  - 450#1001 ogni 500ms
  - 665#0000000053175300 ogni 3000ms
  - 666#5207010152016226 ogni 3000ms

## boot

```
(1617469247.937764) can0 300#035A0B5A5F0064 ripetuto ogni 50ms
... 1500ms
(1617469249.435393) can0 451#10010000235A64
(1617469249.440476) can0 300#035A0B5A5F0064
(1617469249.484886) can0 451#060100001E
(1617469249.490226) can0 300#035A0B5A5F0064
(1617469249.534973) can0 451#0801000028
(1617469249.539717) can0 300#035A0B5A5F0064
(1617469249.586432) can0 451#090100005F
(1617469249.592035) can0 300#035A0B5A5F0064
(1617469249.593631) can0 454#035A0B5A5F0064
```

## cambio assistenza

cambio da eco a trail

```
(1617469276.343015) can0 300#035A0B5A1E0023 eco
(1617469276.343445) can0 454#035A0B5A1E0023 eco
(1617469276.343725) can0 450#1001
(1617469276.390647) can0 451#10010000235A64
(1617469276.390948) can0 450#0601
(1617469276.393315) can0 454#035A0B5A1E0023
(1617469276.394615) can0 402#1E000000E4C80100
(1617469276.402787) can0 201#F000980862
(1617469276.415188) can0 203#3104C01827000400
(1617469276.439159) can0 451#060100001E
(1617469276.439468) can0 450#0801
(1617469276.443232) can0 400#01002C00
(1617469276.443671) can0 454#035A0B5A28000E push button + to trail
(1617469276.444935) can0 300#035A0B5A1E0023 change not seen by battery
(1617469276.489558) can0 451#0801000028
(1617469276.489863) can0 450#0901
```

```
(1617469276.493218) can0 401#688B000061100000
(1617469276.493657) can0 454#035A0B5A28000E push button + to trail
(1617469276.495070) can0 300#035A0B5A1E0023 change not seen by battery
(1617469276.505281) can0 201#F000A20362
(1617469276.517696) can0 203#6C04008F10000400
(1617469276.530005) can0 204#0000000000000000
(1617469276.539479) can0 451#090100005F
(1617469276.542272) can0 202#DA0E0000CE240500
(1617469276.543320) can0 454#035A0B5A28000E push button + to trail
(1617469276.543680) can0 400#01002C00
(1617469276.545379) can0 300#035A0B5A28000E change understood by battery
(1617469276.592594) can0 401#258B0000AB100000
(1617469276.593319) can0 454#035A0B5A28000E push button + to trail
(1617469276.594156) can0 300#035A0B5A28005A change confirmed by battery to
trail
(1617469276.607799) can0 201#F0000C0862
(1617469276.620174) can0 203#9004700818000400
(1617469276.642031) can0 400#01002C00
(1617469276.643320) can0 454#035A0B5A28005A motor is in trail mode
(1617469276.643764) can0 300#035A0B5A28005A
```

usando la pulsantiera da manubrio da 035A0B5A230023 passiamo a 035A0B5A280064 e poi ancora a 035A0B5A230023

```
da eco 230023 a trail 280064
(1616856882.433107) can0 454#035A0B5A230023
(1616856882.451847) can0 300#035A0B5A230023
(1616856882.483108) can0 454#035A0B5A280023 .....280023
(1616856882.501262) can0 300#035A0B5A230023
(1616856882.533102) can0 454#035A0B5A280023
(1616856882.551567) can0 300#035A0B5A280023 .....280023
(1616856882.583099) can0 454#035A0B5A280023
(1616856882.602087) can0 300#035A0B5A280064 .....280064
(1616856882.633096) can0 454#035A0B5A280064 .....280064

(1616856883.453047) can0 300#035A0B5A280064 si ripete
(1616856883.483098) can0 454#035A0B5A280064
...

da trail 280064 a turbo 640064
(1616856883.583094) can0 454#035A0B5A64000E .....64000E
(1616856883.601562) can0 300#035A0B5A280064
(1616856883.633099) can0 454#035A0B5A64000E
(1616856883.651660) can0 300#035A0B5A64000E .....64000E
(1616856883.683099) can0 454#035A0B5A64000E
(1616856883.701612) can0 300#035A0B5A640064 .....640064
(1616856883.733098) can0 454#035A0B5A640064 .....640064

(1616856883.752432) can0 300#035A0B5A640064si ripete
(1616856883.783101) can0 454#035A0B5A640064
```

```

...

da turbo 640064 a trail 280064
(1616856884.983095) can0 454#035A0B5A28000C .....28000C
(1616856885.003758) can0 300#035A0B5A28000C .....28000C
(1616856885.033091) can0 454#035A0B5A28000C
(1616856885.054984) can0 300#035A0B5A280064 .....64
(1616856885.083091) can0 454#035A0B5A280064 .....64

(1616856885.103894) can0 300#035A0B5A280064 si ripete
(1616856885.133090) can0 454#035A0B5A280064
...

da trail a eco
(1616856886.183087) can0 454#035A0B5A23000C .....23000C
(1616856886.203557) can0 300#035A0B5A280064
(1616856886.233082) can0 454#035A0B5A23000C

(1616856886.253126) can0 300#035A0B5A23000C .....23000C
(1616856886.283088) can0 454#035A0B5A23000C

(1616856886.302297) can0 300#035A0B5A230023 .....230023
(1616856886.333089) can0 454#035A0B5A230023 .....230023
...

```

usando la pulsantiera da batteria il messaggio di cambio è il 0x300

## walk button

- 454#03A50B5A1E0023 walk button in eco mode

```

... bla bla
(1616830448.882233) can0 **454**#035A0B5A230023 walk button not pressed
(1616830448.925175) can0 400#01000C00
(1616830448.926888) can0 **300**#035A0B5A230023

(1616830448.932194) can0 **454**#03**A5**0B5A230023 walk button from motor
first press

(1616830448.932795) can0 201#0000000062
(1616830448.944892) can0 203#00000000000000B00
(1616830448.975620) can0 401#6BA1000000000000
(1616830448.977216) can0 **300**#035A0B5A230023 battery does not receive the
button...
(1616830448.982189) can0 454#03A50B5A230023
(1616830449.025394) can0 400#01000C00
(1616830449.027363) can0 **300**#03**A5**0B5A230023 ...battery receive
button signal and emit ack A5
(1616830449.032194) can0 **454**#03**A5**0B5A230023 walk button pressed

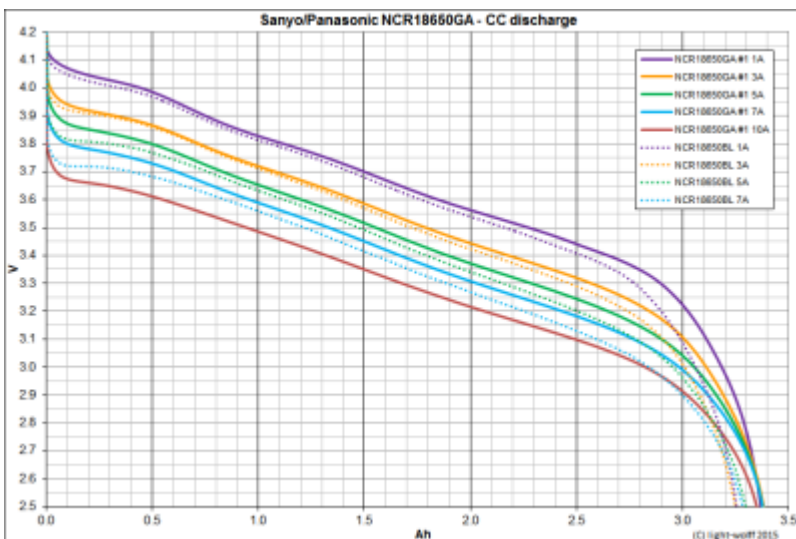
```

```
(1616830449.032790) can0 201#0000000062
(1616830449.044926) can0 203#000000000000B00
(1616830449.075404) can0 401#6BA1000000000000
(1616830449.076995) can0 **300**#03**A5**0B5A230023 battery receive button
signal and emit ack A5
(1616830449.082191) can0 454#03A50B5A230023
(1616830449.082471) can0 450#1001
(1616830449.124302) can0 451#10010000236464
(1616830449.124598) can0 450#0601
(1616830449.127063) can0 400#01000C00
(1616830449.129049) can0 300#03A50B5A230023
(1616830449.132188) can0 454#03A50B5A230023
(1616830449.134761) can0 201#0000000063
(1616830449.147178) can0 203#000000000000B00
. . . .

(1616830448.826973) can0 300#035A0B5A230023
(1616830448.832199) can0 **454**#03**5A**0B5A230023 button non pressed (5A)
(1616830448.832787) can0 201#0000000062
(1616830448.844919) can0 203#000000000000B00
(1616830448.874624) can0 403#5C000000D40D0600
(1616830448.882233) can0 454#035A0B5A230023
(1616830448.925175) can0 400#01000C00
(1616830448.926888) can0 **300**#03**5A**0B5A230023 battery changes from A5
to 5A to stop walk
```

## Batterie litio

- Sanyo NCR18650GA 3350mAh - 10A



## Bluetooth

**bluetooth snooping** it was recommended to first turn bluetooth off, enable snooping (develop menu), enable bluetooth, do tests, disable bluetooth, disable snooping; exactly in this order

```
adb bugreport bugreport.zip
# unzip FS/data/misc/bluetooth/logs/
```

```
DC:9E:23:1F:92:96 RSSI: -51 AdvertisementData(local_name='SPECIALIZED',
manufacturer_data={525:
b'\x02]\x03\x00\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff',
service_uuids=['00001816-0000-1000-8000-00805f9b34fb'])
scanner stop
[Service] 00001801-0000-1000-8000-00805f9b34fb (Handle: 8): Generic
Attribute Profile
[Service] 0000180a-0000-1000-8000-00805f9b34fb (Handle: 9): Device
Information
  [Characteristic] 00002a29-0000-1000-8000-00805f9b34fb (Handle: 10):
Manufacturer Name String (read), Value: b'SPECIALIZED' ''
  [Characteristic] 00002a28-0000-1000-8000-00805f9b34fb (Handle: 12):
Software Revision String (read), Value: b'V1.7.0' ''
[Service] 00001816-0000-1000-8000-00805f9b34fb (Handle: 14): Cycling Speed
and Cadence
  [Characteristic] 00002a5b-0000-1000-8000-00805f9b34fb (Handle: 15): CSC
Measurement (notify), Value: None
    [Descriptor] 00002902-0000-1000-8000-00805f9b34fb (Handle: 17):
Client Characteristic Configuration) | Value: b'\x00\x00' ''
  [Characteristic] 00002a5c-0000-1000-8000-00805f9b34fb (Handle: 18): CSC
Feature (read), Value: b'\x03\x00' ''
  [Characteristic] 00002a55-0000-1000-8000-00805f9b34fb (Handle: 20): SC
Control Point (write,indicate), Value: None
    [Descriptor] 00002902-0000-1000-8000-00805f9b34fb (Handle: 22):
Client Characteristic Configuration) | Value: b'\x00\x00' ''
[Service] 00000001-0000-4b49-4e4f-525441474947 (Handle: 23): SDP
  [Characteristic] 00000011-0000-4b49-4e4f-525441474947 (Handle: 24): HIDP
(read), Value:
b'\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff' ''
  [Characteristic] 00000021-0000-4b49-4e4f-525441474947 (Handle: 26):
Unknown (write), Value: None
[Service] 00000002-0000-4b49-4e4f-525441474947 (Handle: 28): Unknown
  [Characteristic] 00000012-0000-4b49-4e4f-525441474947 (Handle: 29):
Hardcopy Control Channel (write), Value: None
[Service] 00000003-0000-4b49-4e4f-525441474947 (Handle: 31): RFCOMM
  [Characteristic] 00000013-0000-4b49-4e4f-525441474947 (Handle: 32):
Unknown (read,notify), Value:
b'\x01\x10$\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff' ''
    [Descriptor] 00002902-0000-1000-8000-00805f9b34fb (Handle: 34):
```

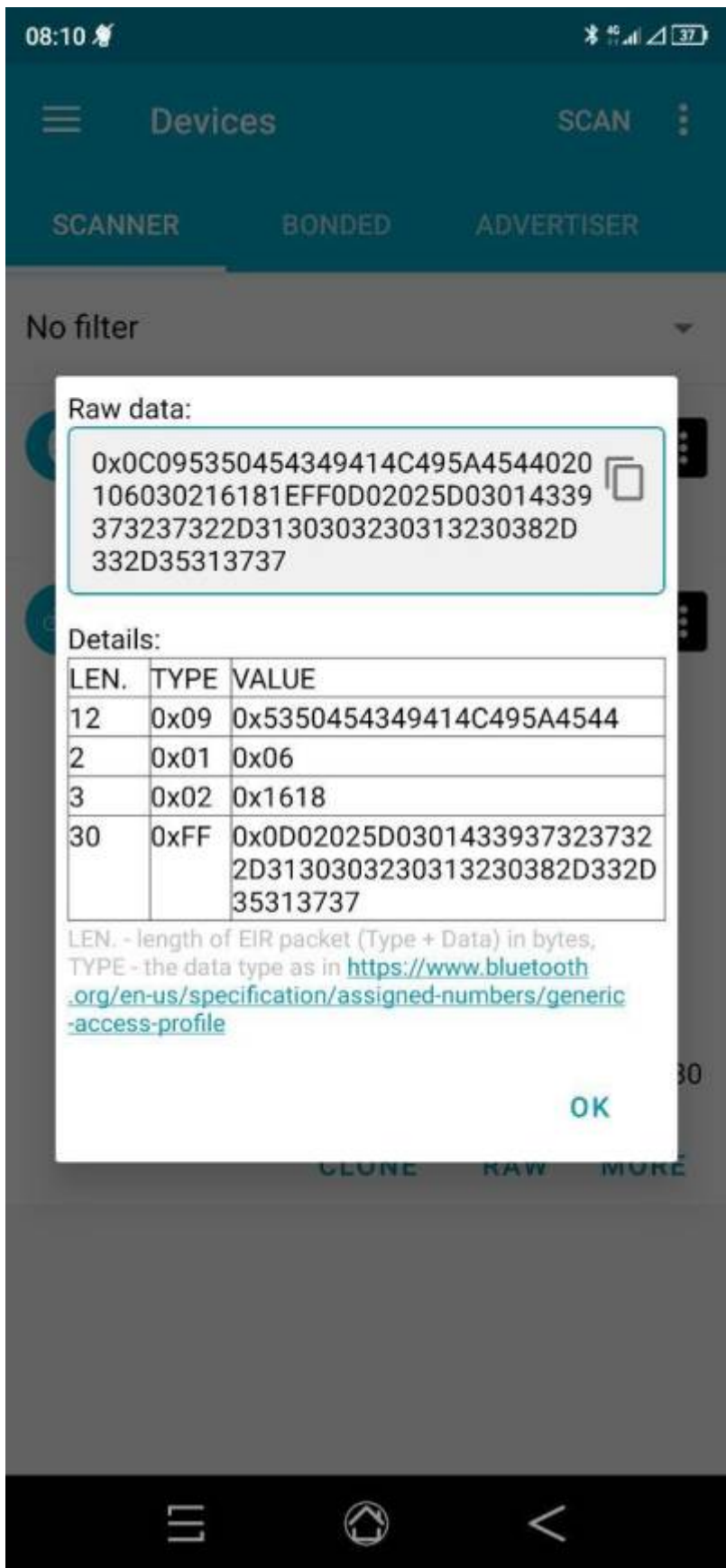
Client Characteristic Configuration) | Value: b'\x00\x00' ''  
(venv)

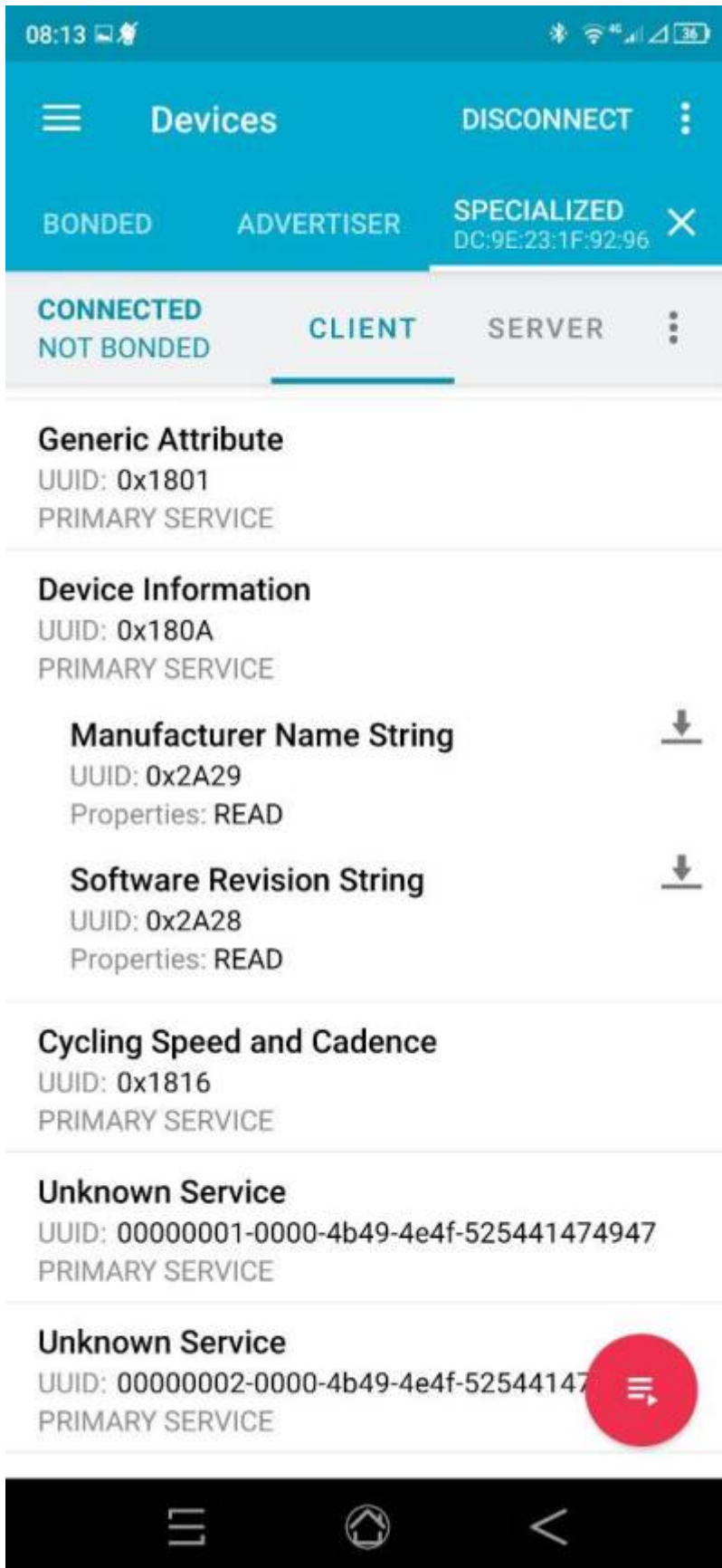
serial:

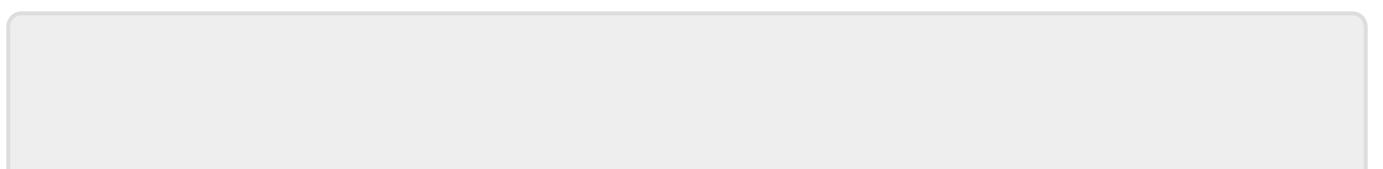
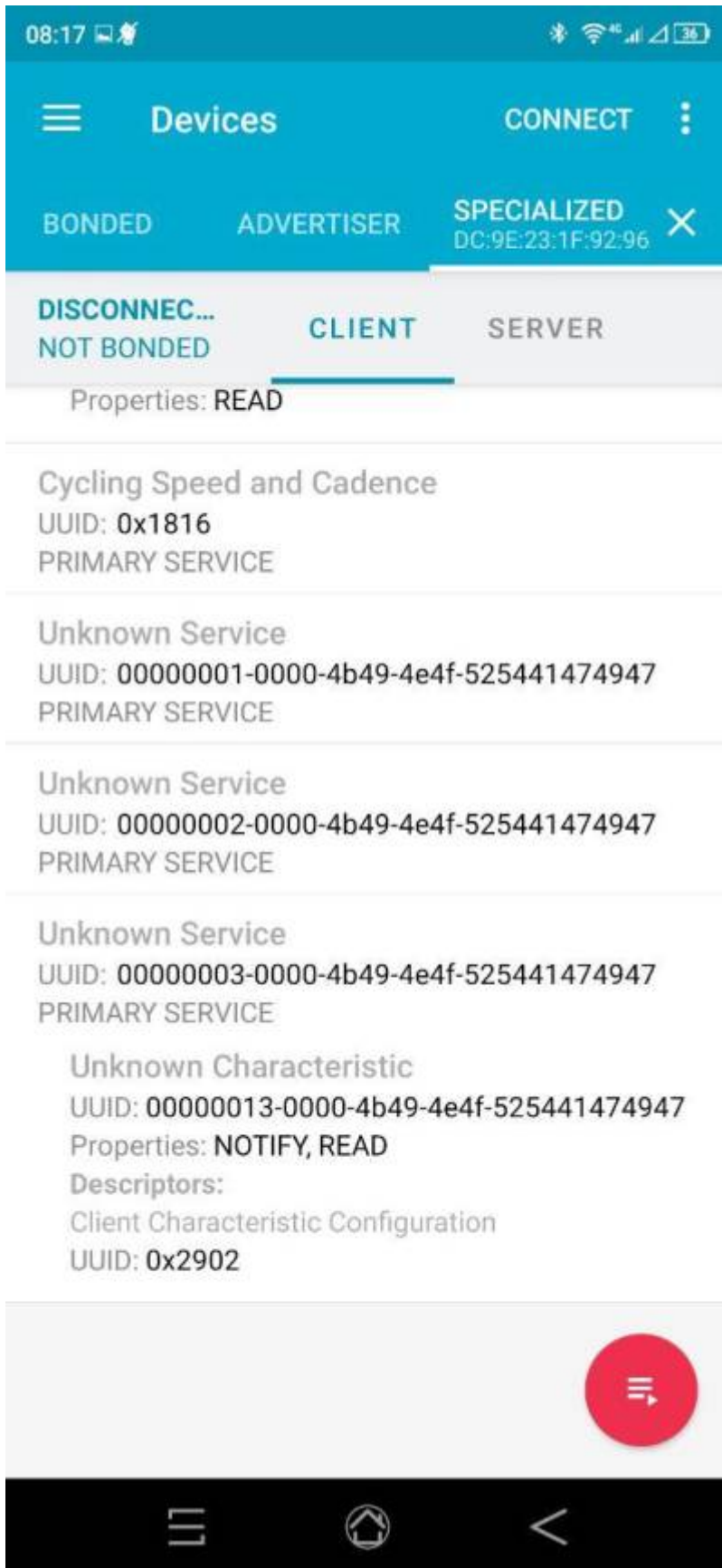
- [Service UUID: 0000000100004b494e4f525441474947]
- [UUID: 0000001100004b494e4f525441474947] 00000011-0000-4b49-4e4f-525441474947
- Value: 0210575342433630313131353531334e000000ff
- 0000 02 01 22 19 00 15 00 04 00 0b 02 10 57 53 42 43 ..“.....WSBC
- 0010 36 30 31 31 31 35 35 31 33 4e 00 00 00 ff 601115513N....

[UUID: 0000001300004b494e4f525441474947] Handle: 0x0021

- **00:01**:BB:AA:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 302 a 312
- **00:03**:1d:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 24 a 30
- **00:05**:XX:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff XX progressivo
- **00:06**:4e:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 0 a 103
- **00:0c**:BB:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff BB SOC **state of charge**
- **01:00**:XX:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff XX da 0 a 196
- **01:01**:XX:02:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 00 a 255
- **01:02**:6c:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 0 a 65281
- **01:04**:f0:6f:07:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff progressivo
- **01:05**:XX:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 1 a 3
- **01:07**:XX:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 27 a 51
- **01:10**:XX:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff XX=0x67,0x24,0x5c
- **01:0c**:LL:HH:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff da 0 a 65510
- **02:0b**:20:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff unico valore 32







From:  
<https://wiki.csgalileo.org/> - **Galileo Labs**

Permanent link:  
<https://wiki.csgalileo.org/projects/zibaldone/electronic/turbolevo?rev=1648447464>

Last update: **2022/03/28 08:04**

