Hacking your (electric) car: the importance of Open Data

Gathering information from OBD (On Board Diagnostic) port of your car could be challenging

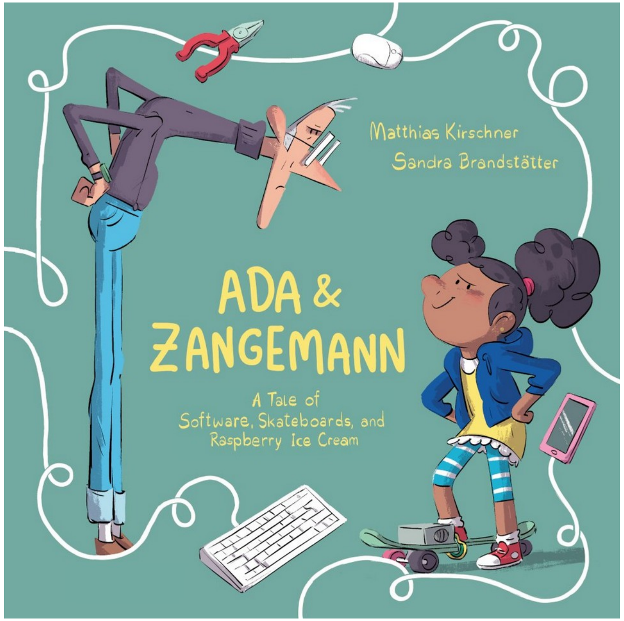
November 8th 2024 · SFSCON 2024

Luca Bonissi lucabon@fsfe.org

fsfe

Introducing myself

Name: Luca
Surname: Bonissi
Origin: Italy



- Firmware **programmer** of embedded electronic devices.

- Maintainer of **BonSlack**, porting of **Slackware** GNU/Linux distribution for various architectures.

- Volunteer as Italian **translator** for **FSFE**.

- Helps to maintain **Ada & Zangemann** repository.

- … and – for hobby – **ice cream** maker :-P

CARS AND SOFTWARE: many electronic devices

- Cars are actually **MANY computers** on **wheels**.

- These “micro” computers (called **ECU**, Engine Control Unit) are connected together through **CAN** (Controller Area Network) bus

- There is a port (**OBD**, On Board Diagnostic) in every (recent) car where the user could connect a CAN-bus adapter (usually with USB or Bluetooth interface) to read/write data from/to every ECU.

- Every ECU has a set of **PIDs** (Parameter IDs) that you can read and sometimes write.

- Every PID contains data related to one or more **sensors** and/or **settings**.

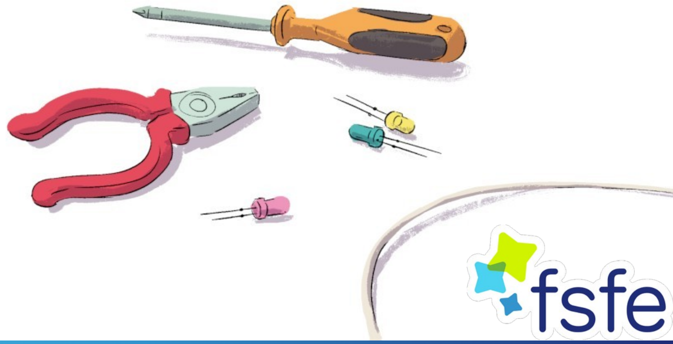
How these data could be useful?

- You can **identify problems** or gather **statistical** data, e.g. about fuel/energy consumption.

- You would like to **set** or **unlock features** that are not available, such as default indoor temperature or One Pedal Driving at power-up or increase the maximum charging current.

- You would like to **remotely control** the car without relying on proprietary services.

- Especially on <u>hybrid</u> or <u>electric</u> cars, you could know:
  * the **battery SOH** (State Of Health) that could be useful if you want to sell or purchase a car;
  * the **SOC** (State Of Charge) that could be used in combination with the EVSE (Electric Vehicle Supply Equipment) to stop the charge at a specific SOC or to start the charge during off-peak time.



The problem: manufacturers do not share ECU/PIDs info

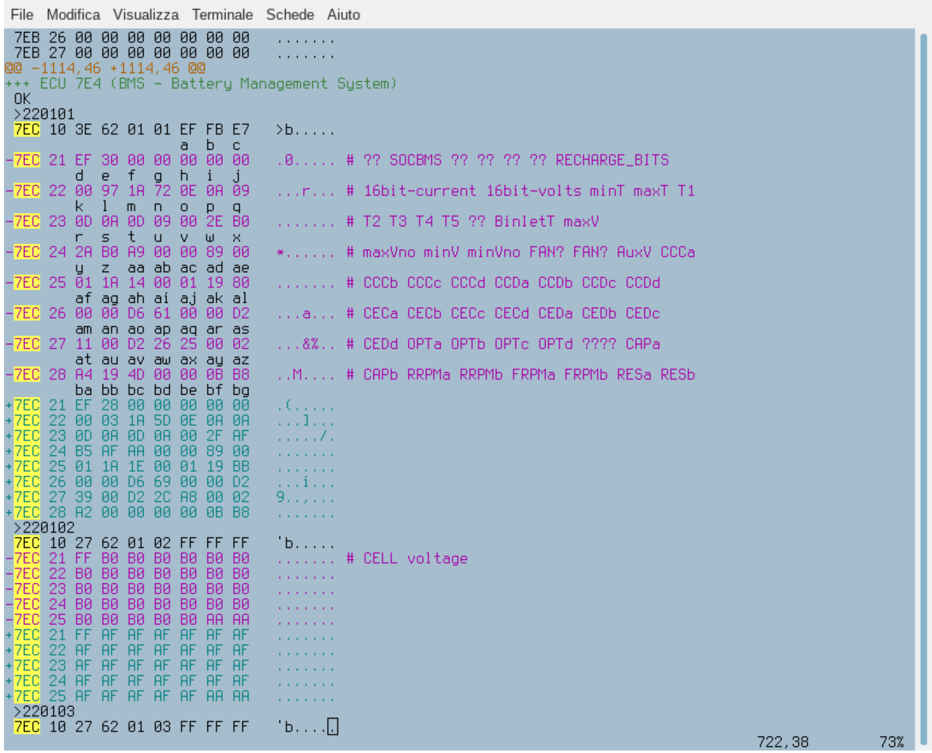
- Users do not know which ECU and related PIDs are available in their car.

- The PIDs information is something like the owner’s manual: it should be available to the end user!

- Most of the PIDs are (or should be) read-only, so you cannot compromise the car safety.

- Mostly applications that have (some) informations are proprietary or the information about ECU/PIDs are not released with an Open Data license.
  And some information are wrong… :-(

How to (try to) regain control of your car?



```
 7EB 26 00 00 00 00 00 00 00   .......
 7EB 27 00 00 00 00 00 00 00   .......
@@ -1114,46 +1114,46 @@
+++ ECU 7E4 (BMS - Battery Management System)
 OK
 >220101
 7EC 10 3E 62 01 01 EF FB E7   >b.....
                    a  b  c
-7EC 21 EF 30 00 00 00 00 00   .0..... # ?? SOCBMS ?? ?? ?? ?? RECHARGE_BITS
        d  e  f  g  h  i  j
-7EC 22 00 97 1A 72 0E 0A 09   ...r... # 16bit-current 16bit-volts minT maxT T1
        k  l  m  n  o  p  q
-7EC 23 0D 0A 0D 09 00 2E B0   ....... # T2 T3 T4 T5 ?? BinletT maxV
        r  s  t  u  v  w  x
-7EC 24 2A B0 A9 00 00 89 00   *...... # maxVno minV minVno FAN? FAN? AuxV CCCa
        y  z  aa ab ac ad ae
-7EC 25 01 1A 14 00 01 19 80   ....... # CCCb CCCc CCCd CCDa CCDb CCDc CCDd
        af ag ah ai aj ak al
-7EC 26 00 00 D6 61 00 00 D2   ...a... # CECa CECb CECc CECd CEDa CEDb CEDc
        am an ao ap aq ar as
-7EC 27 11 00 D2 26 25 00 02   ...&%.. # CEDd OPTa OPTb OPTc OPTd ???? CAPa
        at au av aw ax ay az
-7EC 28 A4 19 4D 00 00 0B B8   ..M.... # CAPb RRPMa RRPMb FRPMa FRPMb RESa RESb
        ba bb bc bd be bf bg
+7EC 21 EF 28 00 00 00 00 00   .(.....
+7EC 22 00 03 1A 5D 0E 0A 0A   ...]...
+7EC 23 0D 0A 0D 0A 00 2F AF   ...../.
+7EC 24 B5 AF AA 00 00 89 00   .......
+7EC 25 01 1A 1E 00 01 19 BB   .......
+7EC 26 00 00 D6 69 00 00 D2   ...i...
+7EC 27 39 00 D2 2C A8 00 02   9..,...
+7EC 28 A2 00 00 00 00 0B B8   .......
 >220102
 7EC 10 27 62 01 02 FF FF FF   'b.....
-7EC 21 FF B0 B0 B0 B0 B0 B0   ....... # CELL voltage
-7EC 22 B0 B0 B0 B0 B0 B0 B0   .......
-7EC 23 B0 B0 B0 B0 B0 B0 B0   .......
-7EC 24 B0 B0 B0 B0 B0 B0 B0   .......
-7EC 25 B0 B0 B0 B0 B0 AA AA   .......
+7EC 21 FF AF AF AF AF AF AF   .......
+7EC 22 AF AF AF AF AF AF AF   .......
+7EC 23 AF AF AF AF AF AF AF   .......
+7EC 24 AF AF AF AF AF AF AF   .......
+7EC 25 AF AF AF AF AF AA AA   .......
 >220103
 7EC 10 27 62 01 03 FF FF FF   'b.....
                                                                   722,38        73%
```

1) Scan all available ECU/PIDs (this operation could take some days).

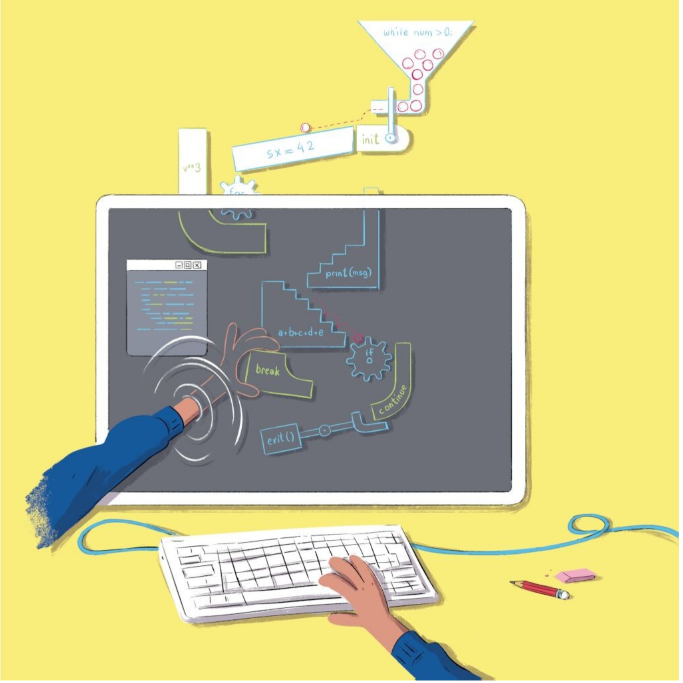
2) Get PIDs in different condition (while driving, with different settings, with different SOC, pedal pressed/depressed, etc.)

3) Discard PIDs that **never change** (they are usually car identifiers – such as VIN – or software/model version).

4) Compare the remaining PID and try to find their meaning.

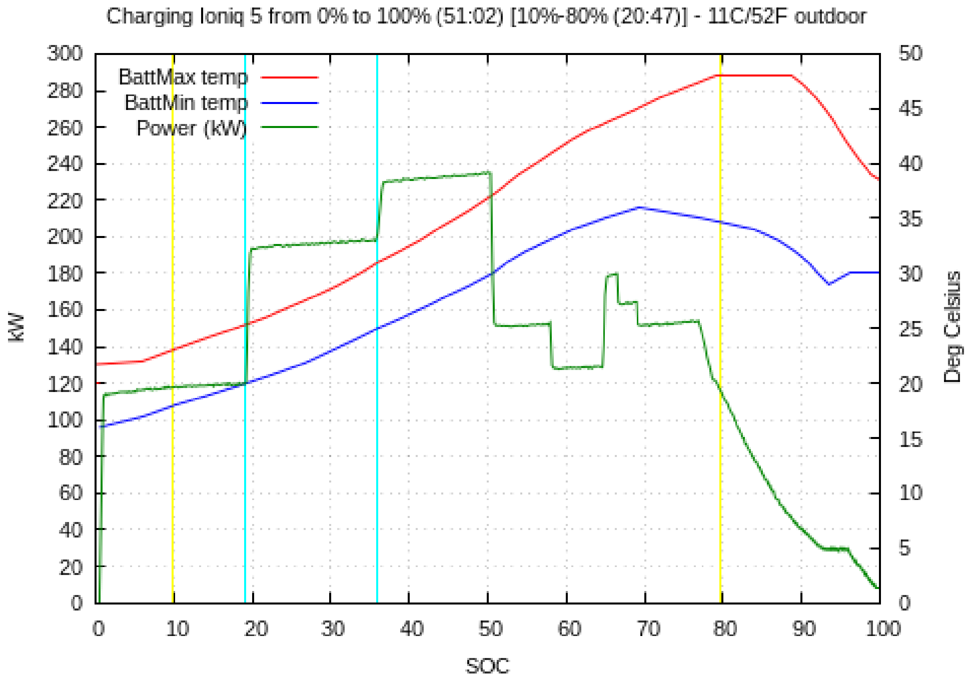
Example: Hyundai Ioniq 5 (my car...)

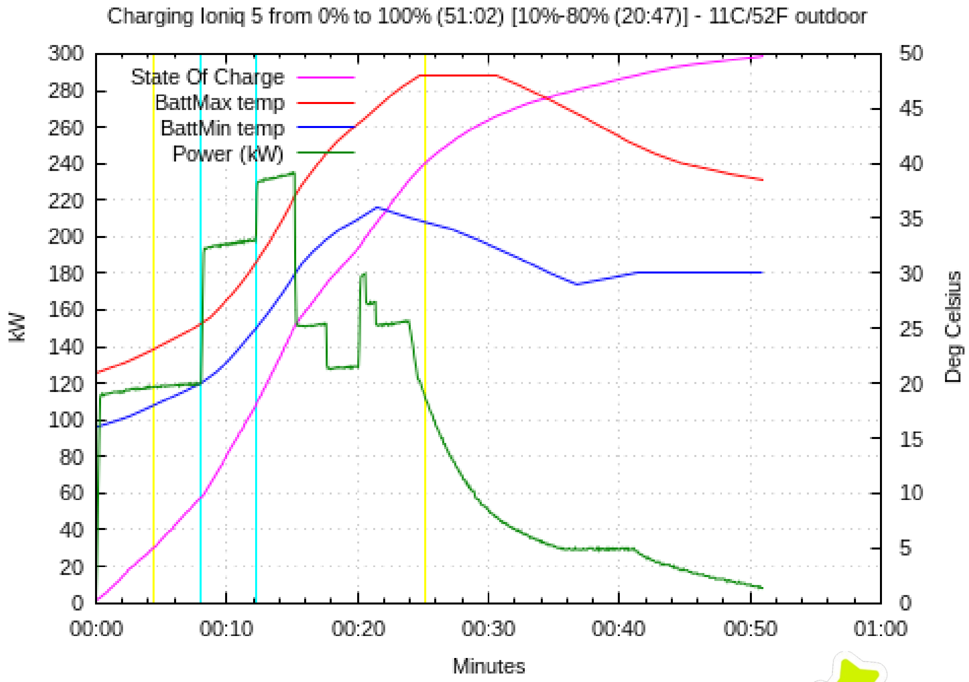
- Found 35 **ECUs**.
- 1004 total **PIDs**.
- 27532 total **bytes** of data.
- Discovered about 330 **variables**: odometer, battery information, temperatures, OBC (On Board Charger) status, steer, brake and accelerator pedal, tires pressure.



Example: Hyundai Ioniq 5 (my car...)

Charging session from 0% to 100%. Note that the charging power depends from the battery minimum temperature, so you can know the time needed for recharge by fetching the battery temperature.





Next (possible) steps

- Give to users **applications** to scan their car.

- Create a **shared database** with collected (anonymised) information by users available with an open license.

- Try to **contact manufacturer** and ask them to release information as Open Data.

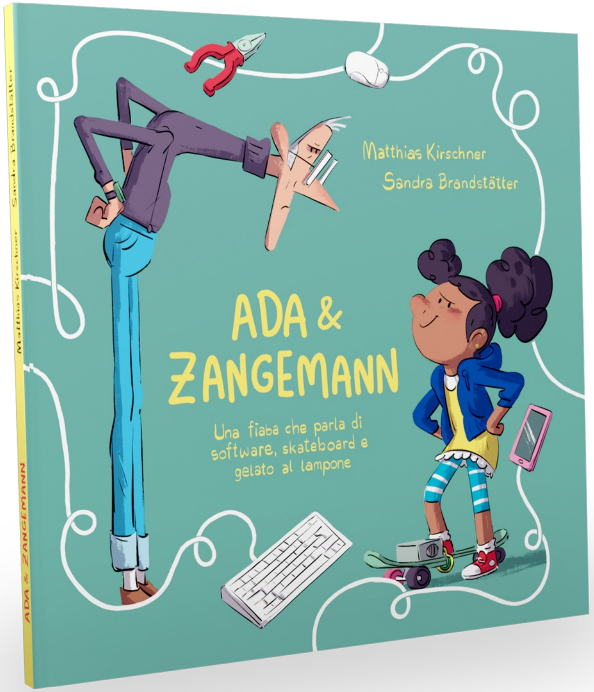
Question and answer?

For a (very alpha) software:

https://bonissi.it/obd/
https://bonissi.it/ocpp/

Contact: lucabon@fsfe.org

Support the FSFE's work!


Matthias Kirschner
Sandra Brandstätter
ADA & ZANGEMANN
Una fiaba che parla di software, skateboard e gelato al lampone

https://fsfe.org/donate

fsfe