Introduction au CarHacking

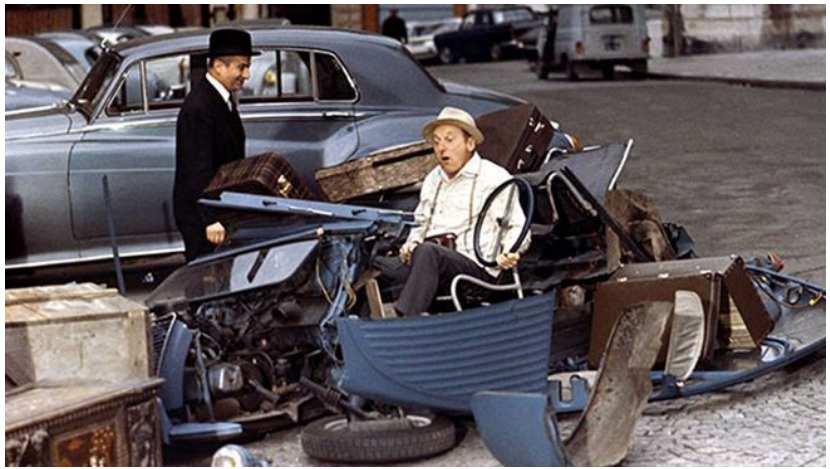
Comment construire sa “Car-in-a-box”

Philippe AZALBERT - *@Phil_BARR3TT*

Quarkslab

Car Hacking : comment débuter

- Utiliser sa voiture (ou celle d'un tiers) : **risqué**
- S'entraîner avec des logiciels spécifiques (ICSim…) : **limité**
- Monter un banc d'essai "Car in a Box" : **hacker style**



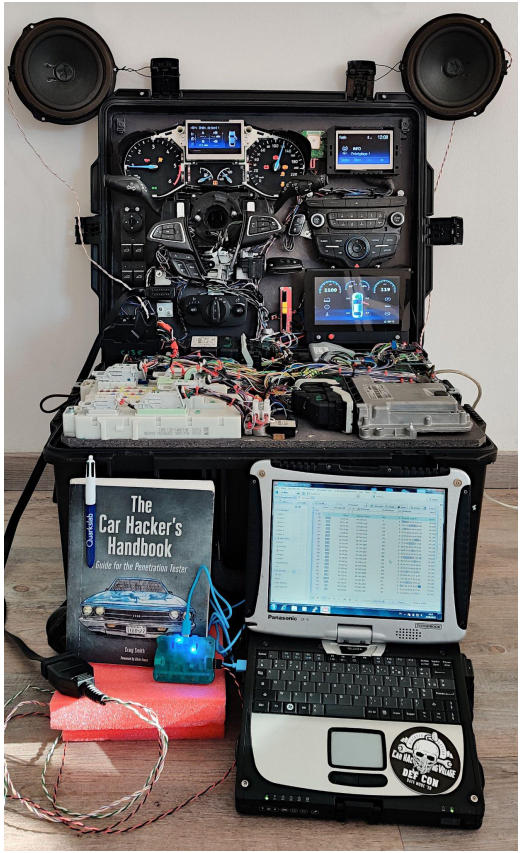


Illustration : [lien]

Choix du modèle et des calculateurs [1/3]

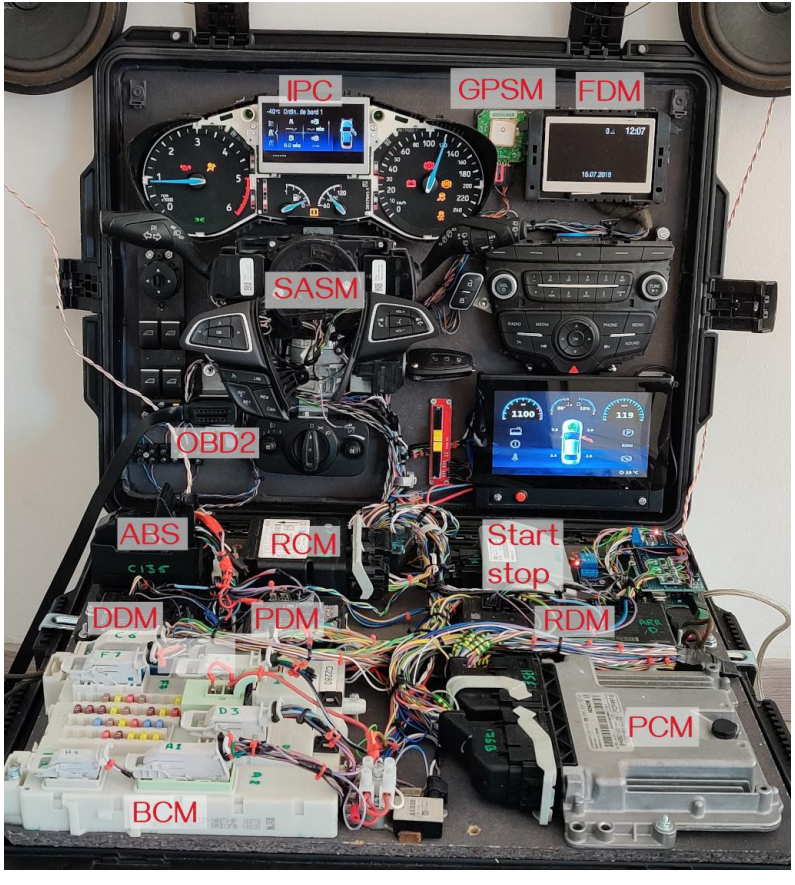
- Se baser sur un modèle qu'on **possède/auquel on a accès** facilite la collecte de certaines informations

- Attention aux modèles **trop anciens** (absence de fonctionnalités/protocoles d'intérêts) ou **trop récents** (prix des calculateurs, connectivité complexe, chiffrement des données…)

- Privilégier des **modèles courants** permet de trouver plus facilement et à moindre coût les différents calculateurs souhaités

Illustration : [lien]

Choix du modèle et des calculateurs [2/3]



Choix du modèle et des calculateurs [3/3]

ECU	+	-
Combiné d'instrument (IC)	Utile, affiche des infos sur l'état du véhicule	
Habitacle (BCM)	Coeur du véhicule, contrôle une majorité d'ECUs	
Gateway (GW)	Composant critique sur la sécurité des réseaux	
Info divertissement (IVI)	OS, grande surface d'attaque, intérêt visuel	Onéreux, risque de dispositif anti-vol
Télématique (TCU)	Connectivité Internet	Connectivité limitée, enrôlement
Injection (PCM)	Cible pour le chip tuning, beaucoup d'outils de dump	Grand nombre de capteurs à simuler pour avoir un intérêt
Airbag (RCM)	Intérêt pédagogique ?	Risque que le calculateur soit verrouillé
Autres	Dépend des caractéristiques	Intérêt généralement limité, volumineux

C’est quoi un ECU ?

ECU : **E**lectronic **C**ontrol **U**nit

L’**ECU** traite des informations provenant de **CAPTEURS**, contrôle des **ACTIONNEURS** et communique avec d’autres **ECUs ou des serveurs** via des réseaux câblés ou sans-fil.

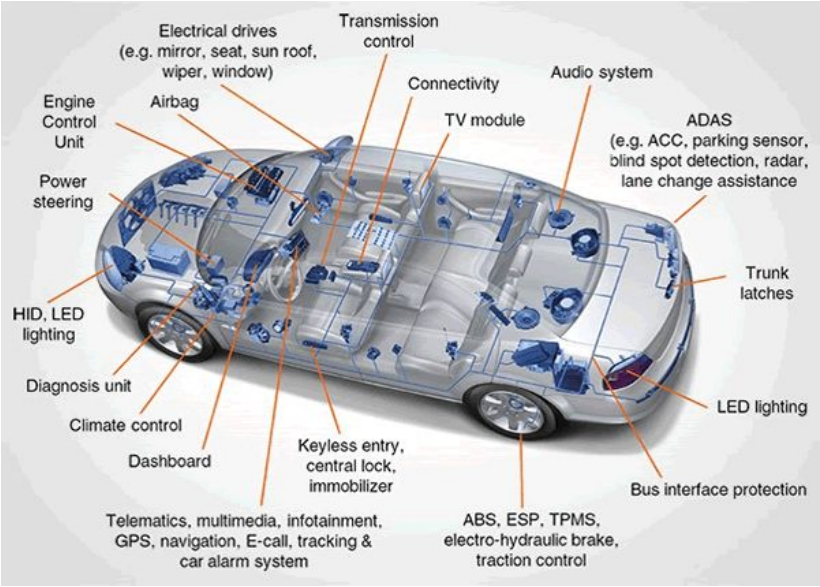


Illustration : [1] [2]

Réseaux de communications inter-ECUs

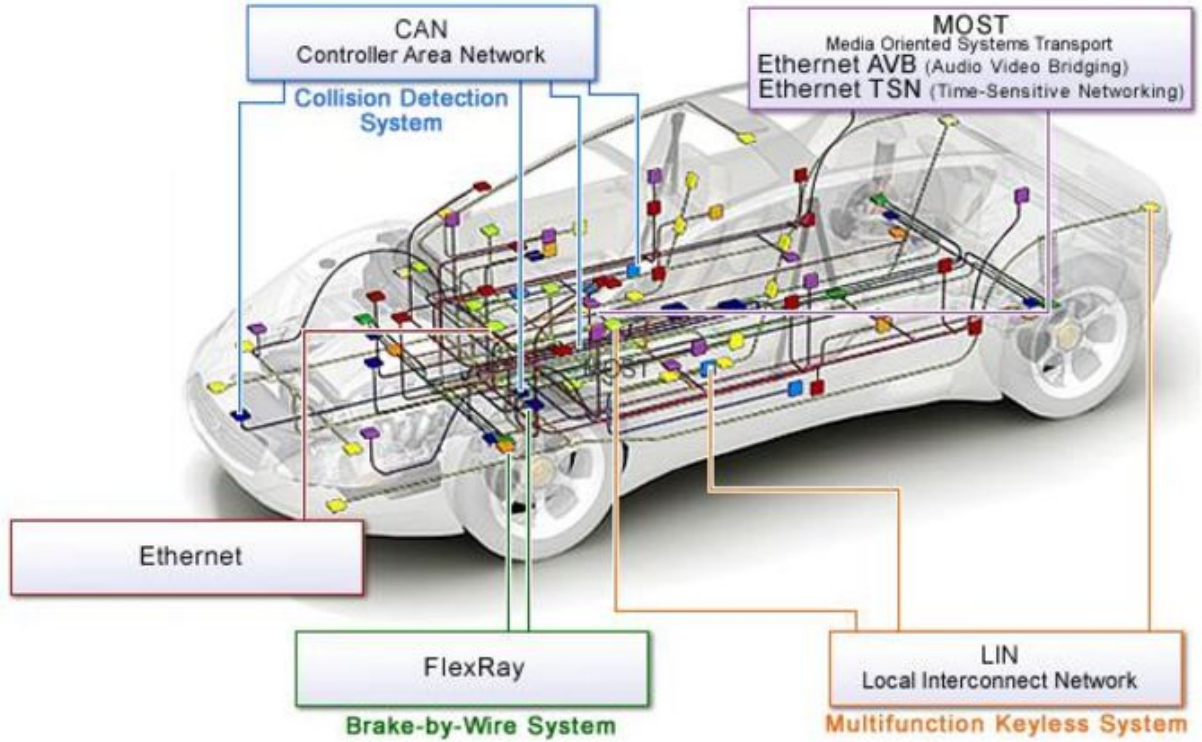
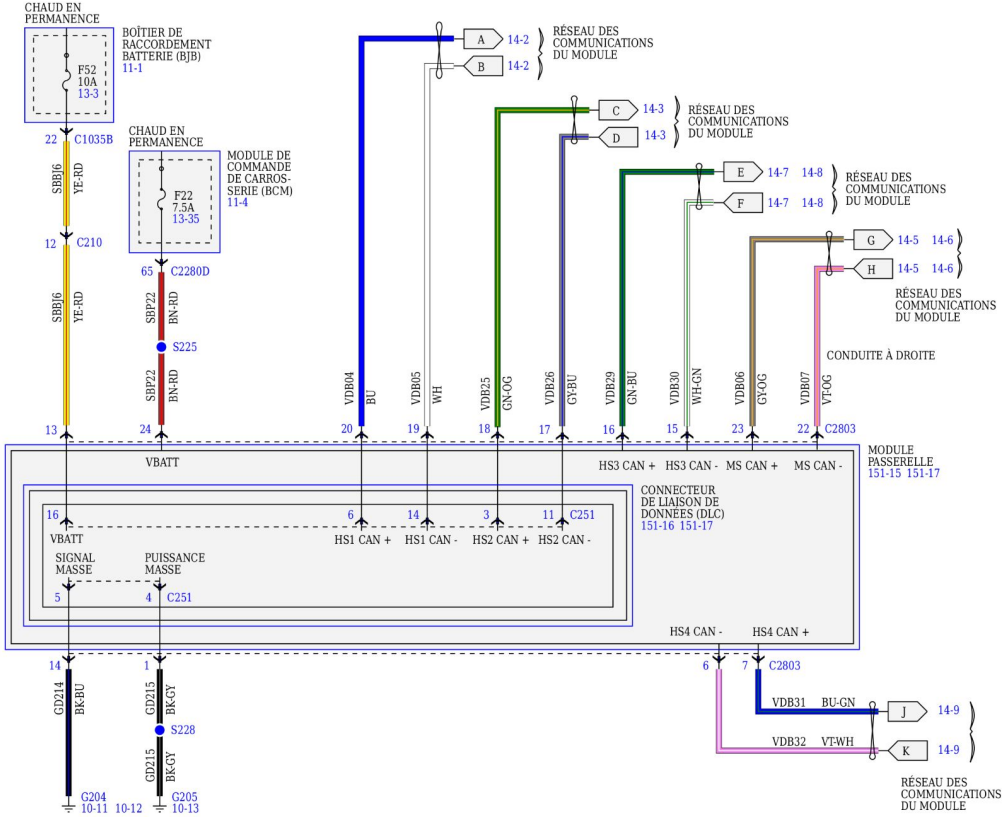


Illustration : [lien]

Reconnaissance [1/3]

- Rechercher en ligne des informations techniques pour identifier les calculateurs, réseaux disponibles dans le véhicule
- Un grand nombre de sites / forums dédiés à chaque modèle sont disponibles, permettant d'avoir des informations hétérogènes (schéma, outils de dump/modification…)
- Chaque constructeur propose un site dédié aux garages, avec un accès payant. On y trouve les schémas précis pour chaque modèle et de temps en temps des fichiers de mise à jour
- Vérifier si des bases de données CAN (.dbc) ne sont pas disponibles en ligne, tel que https://github.com/commaai/opendbc

Reconnaissance [2/3]



Reconnaissance [3/3]

Multi-marques	https://www.ateliodoc.com	Mercedes	http://www.startekinfo.com/
Audi	https://erwin.audi.com/erwin/showHome.do	Mini	http://www.minitechinfo.com/
BMW	http://www.bmwtechinfo.com/	Mitsubishi	http://www.mitsubishitechinfo.com/
Citroen	http://public.servicebox.peugeot.com/pages/index.jsp	Nissan	https://www.nissan-techinfo.com/home.aspx
Fiat	https://www.technicalinformation.fiat.com/tech-info-web/web/in	Peugeot	http://public.servicebox.peugeot.com/pages/index.jsp
Ford	https://www.etis.ford.com/	Porsche	https://techinfo2.porsche.com/PAGInfosystem/VFModuleManager?Type=GVOL
Honda	https://techinfo.honda.com/rjanisis/logon.aspx	Renault	https://newdialogys.renault.com/
Hyundai	http://www.hyundaitechinfo.com/	Saab	http://epsiportal.com/Site/SAAB
Jeep	http://www.techauthority.com/	Smart	http://www.smarttekinfo.com/SmartTek/
Kia	https://kiatechinfo.snapon.com/default.aspx	Tesla	https://service.teslamotors.com/
Land Rover	http://www.landrovertechinfo.com/	Toyota	http://techinfo.toyota.com/
Lexus	https://techinfo.lexus.com/	Volvo	http://www.volvotechinfo.com/
Mazda	https://www.mazdaserviceinfo.com/	Volkswagen	https://erwin.vw.com/

Où acquérir les calculateurs

- **Accéder à une épave et la démonter**
  + Accès à tous les calculateurs, les faisceaux
  - Long, requiert des outils adaptés

- **Casse**
  + Permet de vérifier visuellement l'état du calculateur avant achat
  - Choix limité

- **Internet**
  + Grand choix de pièces la connectivité Internet des autres calculateurs
  - Risque d'acquisition d'un calculateur défectueux

Démontage d’un véhicule

Rappel de sécurité

- Si vous trouvez un connecteur jaune **connecteur jaune connectors**, cela signifie qu’il est relié au système d’airbag, **attention** !
- Les airbags sont des systèmes **pyrotechniques**
- Il est recommandé dans ce cas de **débrancher la batterie** et attendre quelques minutes avant de procéder au démontage de ces équipements

Recommandations pour l’acquisition en ligne

- **Privilégier un site permettant de voir les autres pièces du même véhicule**
  Évite tout problème d’enrôlement, compatibilité

- **Préférer un calculateur vendu avec son connecteur**
  Gain de temps et de fiabilité lors de la construction du banc

- **Certains sites détails l’état général du véhicule ‘donneur’**
  Cela permet d’anticiper l’état probable du calculateur (gros choc avant = no go pour Airbag/PCM…)

Illustration : [lien]

Câblage

Cette étape est la plus chronophage

- A l'aide de la documentation, identifier les pins VCC et GND
- Tous les capteurs et actionneurs ne sont pas utiles pour, prendre le temps d'identifier le strict nécessaire
- Dans certains cas (Airbag), la masse de l'ECU se connecte directement sur le boîtier
- En l'absence des connecteurs de l'ECU, l'utilisation de connecteurs Dupont femelle peut être envisagée

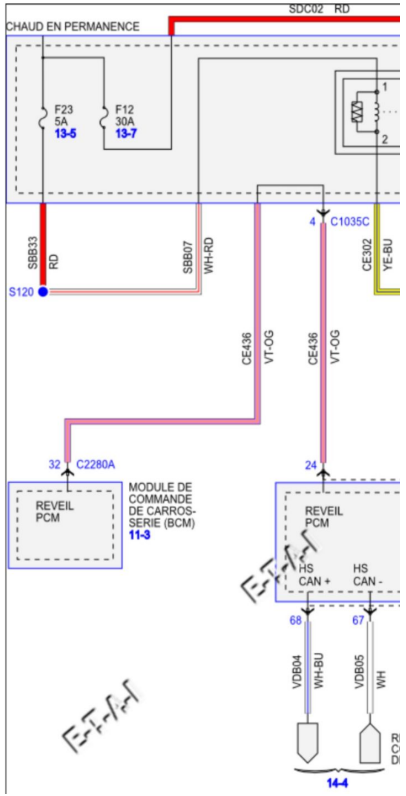
Illustration : [lien]

Démarrer les ECUs [1/2]

- Les ECUs sont conçus pour être **économe en veille**, différentes méthodes sont utilisées pour les démarrer :
  - **Pin d'entrée** dédiée
    Vérifier la présence d'un pin "Wake"
  - **Trame de réveil**
    Cela peut être un message spécifique sur le bus CAN ou toute activité sur ce dernier

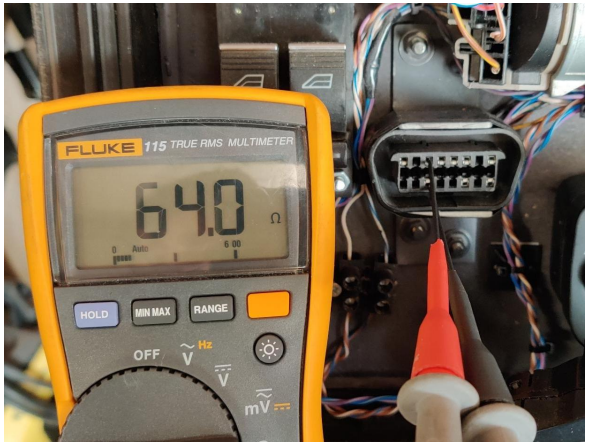
```
$ cangen -I i -D FFFFFFFFFFFFFFFF -L 8 -g 10 can0
```

- Si un **BCM** est présent, il gère habituellement l'envoi des trames de réveil pour la majorité des ECUs



Démarrer les ECUs [1/2]

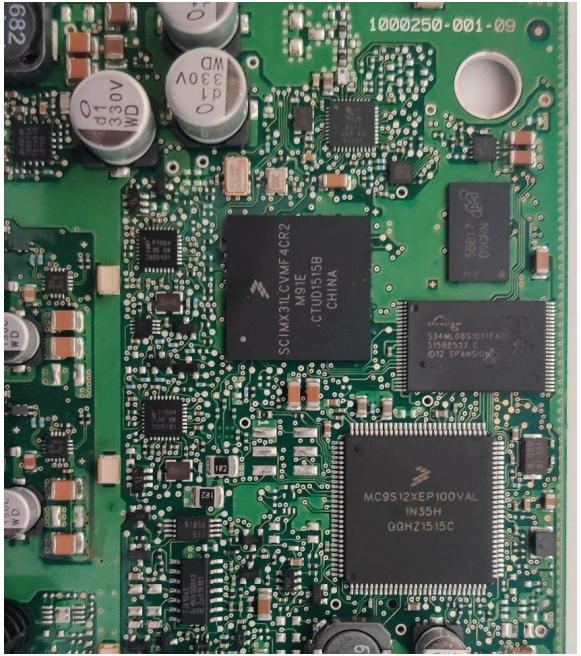
- Si un calculateur semble ne pas démarrer, vérifier :
  - **Alimentation inadaptée**
    Certains calculateurs nécessitent un **fort courant de pointe** au démarrage, une alimentation 12V - 8/10Ah peut être requise
  - **Absence des terminaisons sur le bus CAN**
    CUne fois les différents ECUs reliés, vérifier que chaque bus CAN dispose bien de ses terminaisons 120 ohms, ayant une impédance de 60 ohms



Bonus : dump all the things

Lors du câblage de chaque ECU, en profiter pour :

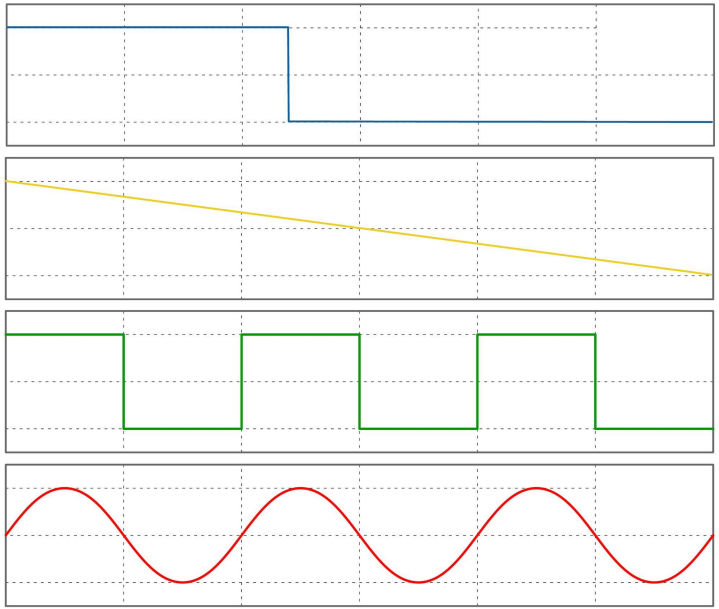
- Identifier les principaux **MCU/SOC** et puces mémoire
- Dumper toutes les **EEPROM** et mémoires **FLASH**
- Si possible, dumper les parties **PROGRAM** et **DATA** du SOC / MCU
- Localiser les accès de debug (JTAG…)



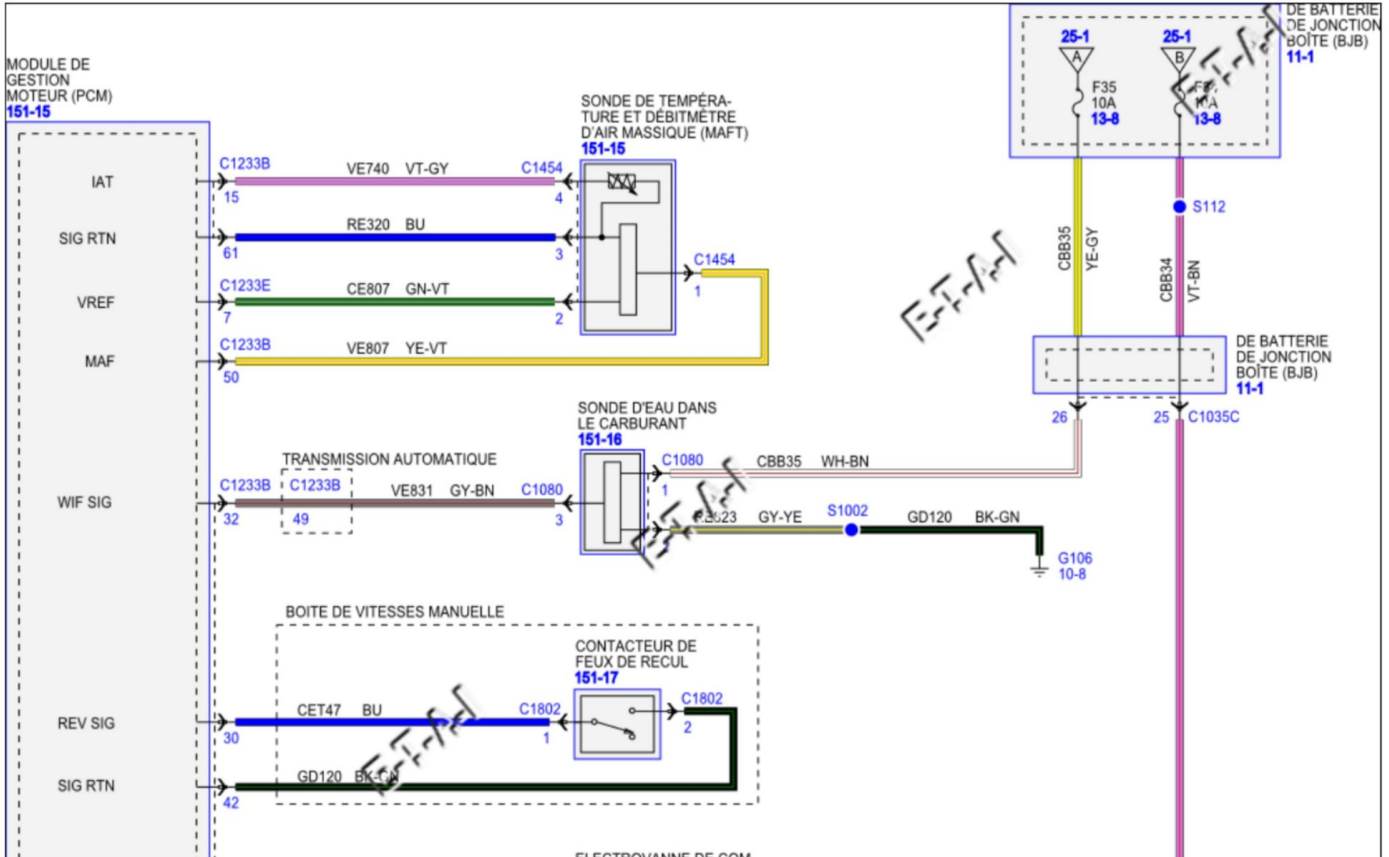
Emulation de capteurs [1/4]

On retrouve 4 types de signaux sur les capteurs communément employés :

- **Relais à la masse (ou +12V)**
  L'entrée vaut 1 si connecté à la masse
- **Résistance variable**
  Habituellement un signal 5V passant dans un potentiomètre 1-5KOhm
- **Signal carré**
  Signal 5V
- **Signal sinusoïdal**
  Plus complexe à émuler, requiert des composants spécifiques



Emulation de capteurs [2/4]



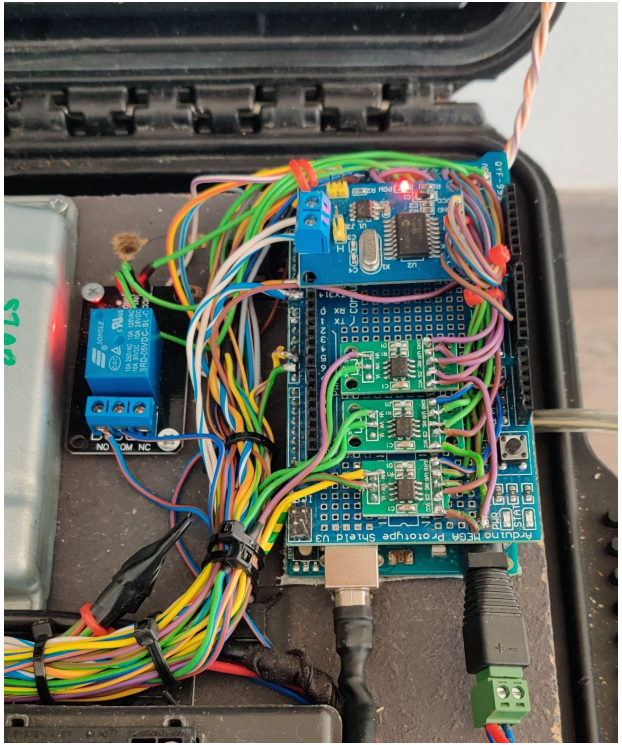
Emulation de capteurs [3/4]

Solution employée dans la Q-Car : un Arduino MEGA et des potentiomètre digitaux

La modulation **PWM** n'est pas suffisamment précis pour générer de bons signaux carrés, l'utilisation d'un timer s'avère plus efficace

Conseils :

- L'accès à un outil de diagnostic est fort utile pour rechercher / déterminer les bons niveaux des signaux
- Quelques capteurs/actionneurs critiques (airbag, ceintures) ont une impédance spécifique pour confirmer leur présence (habituellement 2 ohms)



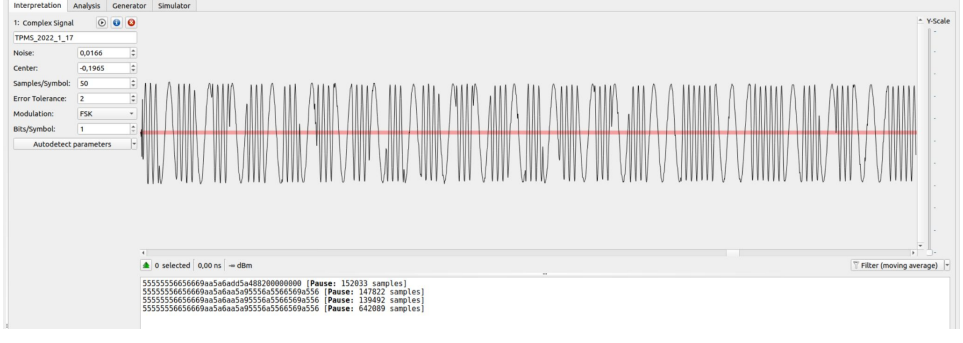
Emulation de capteurs [4/4]

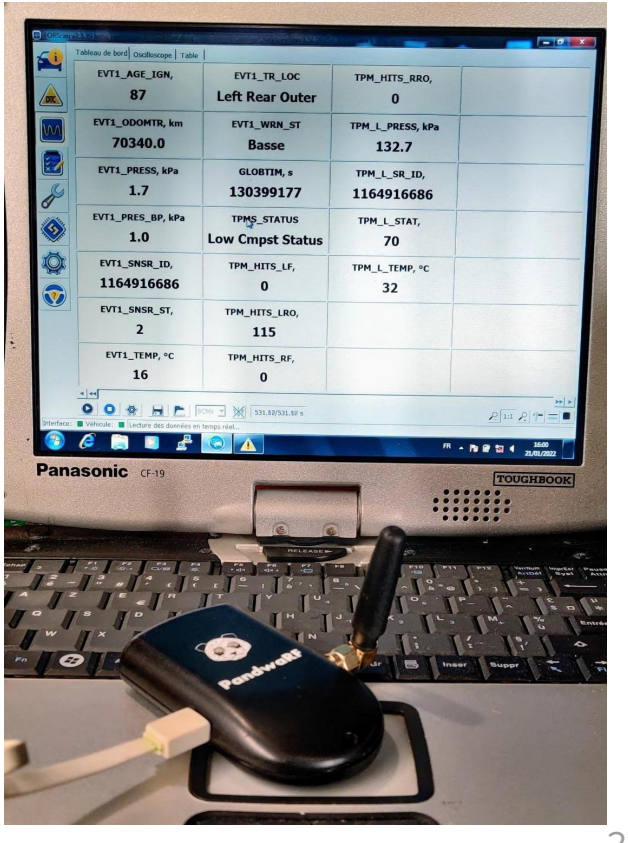
Tous les capteurs ne sont pas filaires

Certains véhicules sont dotés de **TPMS** (Tire Pressure Monitoring System) direct.

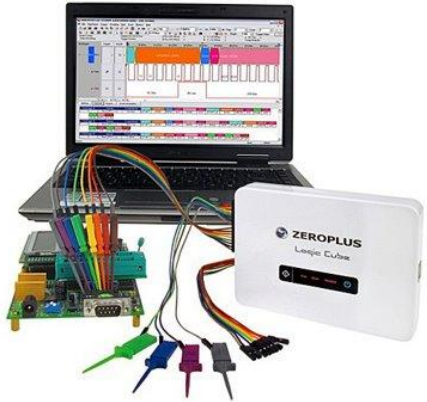
Avec un équipement **SDR** adapté, on peut générer les signaux FSK (Frequency Shift Keying) correspondant.

Le projet RTL_433 liste plusieurs modulations connues de capteurs TPMS : https://github.com/merbanan/rtl_433/tree/master/src/devices





Quelques outils utiles



Merci !

Quarkslab

Thank you

Contact information:

Email: contact@quarkslab.com

Phone: +33 1 58 30 81 51

Website: www.quarkslab.com

@quarkslab

Quarkslab