



## CAN Hacking: The In-vehicle Network

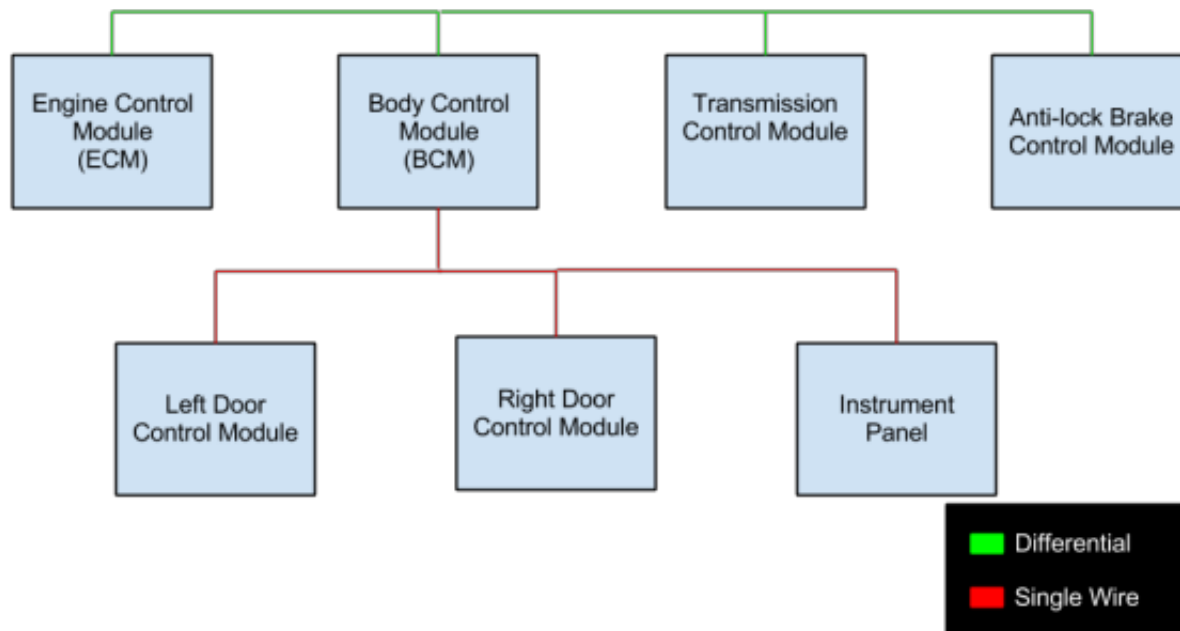
October 22, 2013 by [Eric Evenchick](#) 43 Comments

[Last time](#), we discussed how in-vehicle networks work over CAN. Now we'll look into the protocol and how it's used in the automotive industry.

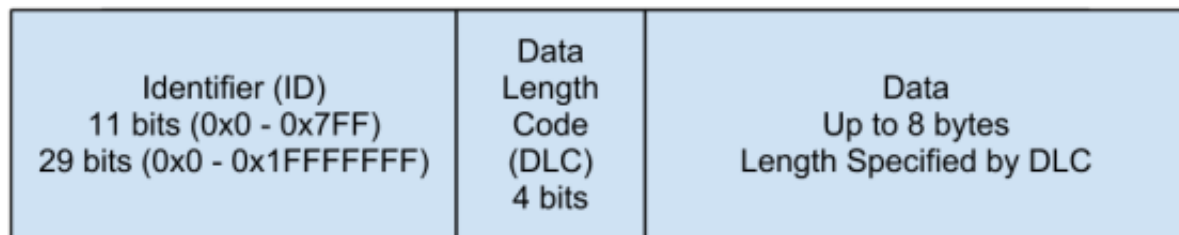
### The Bus

On the hardware side, there's two types of CAN: differential (or high-speed) and single wire. Differential uses two wires and can operate up to 1 Mbps. Single wire runs on a single wire, and at lower speeds, but is cheaper to implement. Differential is used in more critical applications, such as engine control, and single wire is used for less important things, such as HVAC and window control.

Many controllers can connect to the same bus in a multi-master configuration. All messages are broadcast to every controller on the bus.



An oversimplified in-vehicle network



The structure of a CAN message

From a software perspective CAN message consists of 3 parts: an identifier, a data length code, and up to eight bytes of data.

The identifier (ID) is used to specify what the message means, and who's sending it. Typically standard IDs are 11 bits, but there are also 29 bit extended type IDs. The ID also defines the priority: the lower the ID, the higher the message's priority.







The data length code (DLC) is 4 bits, and specifies how many bytes of data will be in the message. In some applications, a DLC of 8 is always used, and unused data bytes are padded with zeros.

Finally, the 8 bytes of data contain the actual information. The meaning of the information is inferred from the message ID, and the length is specified by the DLC.

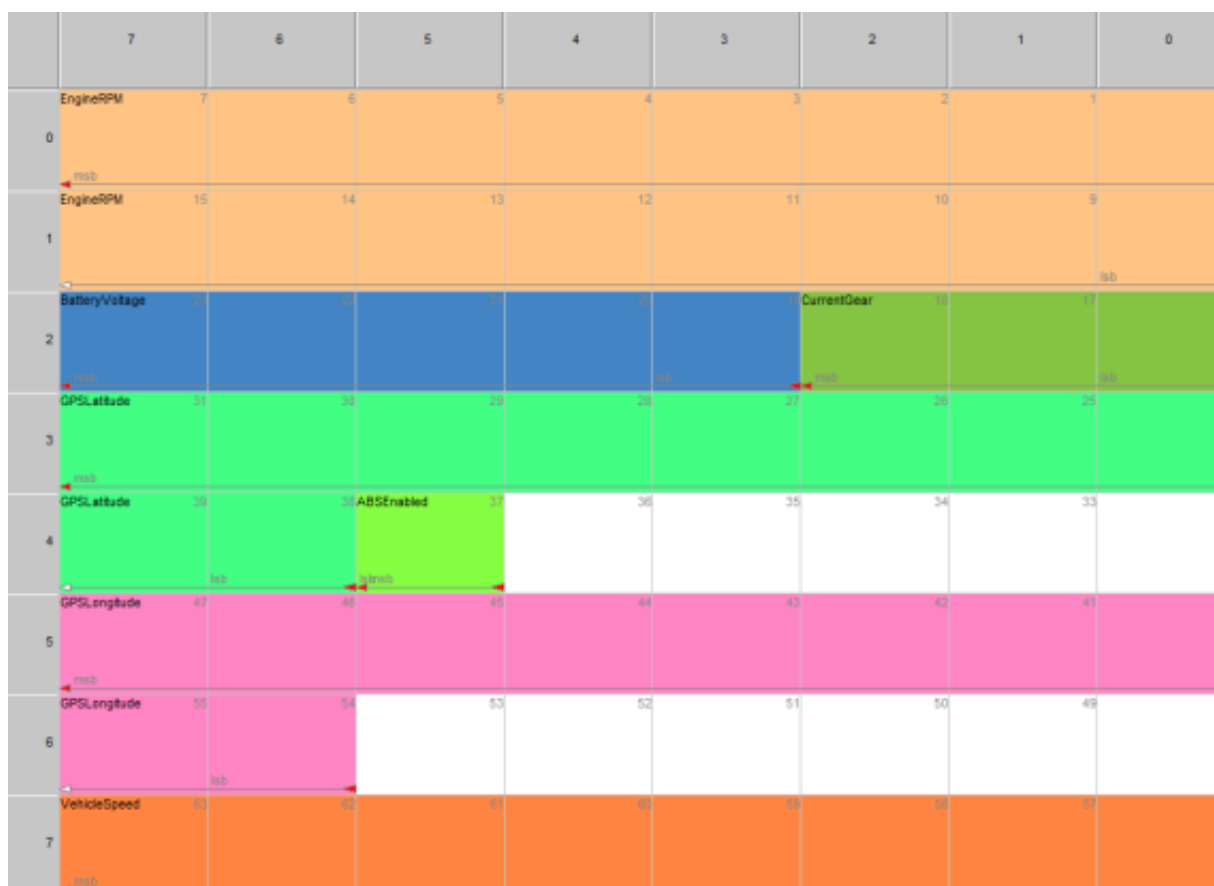
## Decoding & Databases

To make sense of the 8 data bytes, the controller will decode the data into signal such as

engine RPM, fuel level, or brake pedal position. Each signal has a start bit and end bit, which are used to select the correct bits out of the 8 bytes. No signal information is transmitted over the bus. Instead all controllers must agree on the layout of messages and signals beforehand. Below is the table of signals, and the graphical layout of a sample message.

Name	Message	Multiplexing/G...	Startbit	Leng...	Byte Order	Value Typ
 EngineRPM	HackadayMessage	-	8	16	Motorola	Signed
 CurrentGear	HackadayMessage	-	16	3	Motorola	Signed
 BatteryVoltage	HackadayMessage	-	19	5	Motorola	Signed
 ABSEnabled	HackadayMessage	-	37	1	Motorola	Signed
 GPSLatitude	HackadayMessage	-	38	10	Motorola	Signed
 GPSLongitude	HackadayMessage	-	54	10	Motorola	Signed

A table of CAN signals that make up a message



A sample CAN message layout

To help program controllers that agree on messages and signals, a CAN database is used. This database contains definitions of all messages and signals. The most popular format is DBC, which is a proprietary (but ASCII based) format by Vector. The DBC editing tool, **CANDB++**, is free (as in beer). The databases are used to auto-generate code that can interpret the messages.

With a database file in hand, you can easily sniff the CAN bus and interpret all kinds of data. One example is a hack we featured that **sniffed the bus for steering wheel button**

presses. You can also pretend to be controllers by sending spoofed data onto the bus. For example, you could send a fake engine RPM to the instrument cluster.



No, this car wasn't actually doing 8000 RPM.

The majority of the communications during normal operation work by decoding a database. However, for diagnostic applications, there are special protocols that are used. Next time, we'll look at how these protocols work, and what fun can be had with them.

## CAN Hacking

- Introductions
- The In-vehicle Network
- CAN Protocols (planned for 10/29/13)
- Building CAN Hardware (planned for 11/5/13)

CAN Hacking: Introductions      DEF CON: Hacking Hardware and Cars

Wristband RFID unlocks car door and starts engine

Wii U to be released this weekend, Wii U GamePad to be torn apart on workbenches across the land

Radar detector integrated with dashboard display screens and steering wheel controls

Filed Under: [Featured](#), [Network Hacks](#), [news](#) Tagged With: [automotive](#), [CAN](#), [CAN Hacking](#)



## Comments

matt says:

October 22, 2013 at 1:07 pm

So where exactly do you get the DBC databases? I assume the manufacturers dont supply them.

[Reply](#)

[Report comment](#)

Reset says:

October 22, 2013 at 1:36 pm

There is no "legal chance" to get the DBC files from a car manufacturer and the manufacturer does not exchange DBCs between each other. There is no standard, because you can make conclusions about the build in sensors or other hardware. It is also not allowed to drive cars with direct CAN access from outside the cars closed system on public streets, but what you do on private ground depends on you. Only cars with special licenses can drive in public. But If you have CAN access, it is very easy to verify the CAN messages, by switching, pushing or whatever. You can push a button and look on the messages, what values changes. For example, the linux kernel have the VW/Audi SocketCan in it, til version 3.6.0. With the SocketCAN utils on:

<https://gitorious.org/linux-can/can-utils/source/16c970d40e6c19dde705bad4751bab1a3a4f3a0d>:

you have open source cansniffer, candump and canplayer utilities. It is very easy to

analyse CAN messages.

[Reply](#)

[Report comment](#)

**Nate B says:**

**October 22, 2013 at 9:12 pm**

Do you have a cite for it not being legal to drive a car with direct CAN access on public roads? What country does that pertain to?

[Reply](#)

[Report comment](#)

**Reset says:**

**October 22, 2013 at 11:36 pm**

I know that Europe and the USA does not allow direct CAN access.

[Reply](#)

[Report comment](#)

**CarKnow (@CarKnowLLC) says:**

**October 25, 2013 at 7:38 am**

That's not really a citation, and to the best of my knowledge, not true. I know there are statutes that dictate one cannot view the data in realtime (much like anti-texting and driving laws), but even for safety critical systems, while ill-advised, it's not illegal so long as you don't impact federally mandated systems (e.g. emissions, in the US).

**fartface says:**

**October 26, 2013 at 10:00 pm**

So scangauge violates the law then. Because mine access the canbus and they claim it's legal. and yes it CAN change things like reset the SES light as well as other functions.

[Reply](#)

[Report comment](#)

**KWest says:**

**October 22, 2013 at 1:40 pm**

Databases are used by OEM and those close enough to the OEM to get access. Top level aftermarket ECU's will sometimes include.dbc files again depending on who

you are. I don't know of any free tools what will use .dbc files, the most accessible I can think of Matlab/Simulink, again you need a few hundred dollars of hardware plus the software to get started.

[Reply](#)

[Report comment](#)

**galah says:**

**October 22, 2013 at 3:19 pm**

Few hundred dollars? A OBDII bluetooth adaptor off ebay is more like 10. Works well with android apps.

[Reply](#)

[Report comment](#)

**KWest says:**

**October 24, 2013 at 12:29 am**

Does that 10 dollar adapter integrate with Matlab/Simulink? Or does that android app support .dbc files? I'm talking about using putting .dbc files to use, not getting on the CAN bus for cheap, I realize that there are cheap CAN adapters out there. I have a cheap USB one connected right beside my Kvaser interface.

The cheap unit works great for monitoring the bus, however when you want to do anything more like isolating a node and filtering it's data the professional interface is a must.

[Reply](#)

[Report comment](#)

**CarKnow (@CarKnowLLC) says:**

**October 25, 2013 at 7:39 am**

You actually can interface those adapters to MATLAB and other programs. The bigger issue is that accessing non-OBD CAN data is tricky and requires direct manipulation of the AT commands (e.g. in an ELM327). Both devices have their place.

**KWest says:**

**October 25, 2013 at 12:55 pm**

You can put together a simple serial model that would interface with serial to CAN dongle, however to use .dbc files and VNT CAN blocks you need a supported device. Simulink is more than likely overkill for all but the top level guys that are doing real deep CAN bus work, like integrating aftermarket ECU's into OEM applications. If you want to sniff the bus to roll

up your windows with an Arduino there is no need to go down this rabbit hole.

**charliex says:**

**October 25, 2013 at 3:03 pm**

The Arduino is not fast enough for all CAN buses, I struggled with the 16Mhz AT90CAN til i rewrote a lot of the atmel CAN routines. I found when i was logging i'd loose a lot of messages and not be able to reply fast enough. But saying that i am one of the "like integrating aftermarket ECU's into OEM applications" guys, now it keeps up with all my 'pro' tools. There are a lot of decent ARM's with CAN the STM32s spring to mind.

But logging is still logging, IMHO its better to go that little bit above to be sure you're logging all the data, and replying fast enough.

But if you're only sending out CAN messages or reading OBD II PID's the arduinoish ones are fine, so use those for the final devices.

**Eric Evenchick says:**

**October 22, 2013 at 5:43 pm**

I once wrote a DBC parser in Python. It wasn't too bad, since the format is ASCII based. Unfortunately, I lost it in a drive failure... this is before I learned that Git is a good thing.

[Reply](#)

[Report comment](#)

**matt says:**

**October 22, 2013 at 9:28 pm**

I was hoping someone who say there is a community effort out there to document the CAN bus for various cars, especially since there is so much parts commonality between either model years, of various models of the same manufacturer.

[Reply](#)

[Report comment](#)

**fartface says:**

**October 26, 2013 at 10:03 pm**



GM and other actively sue groups like that into the ground. I was very active in a GM ECM reverse engineering group and GM not only threatened major lawsuits, but threatened that we would be in federal export violation of military equipment if we did not stop publishing our data and findings.

If you do create a nice document, publish it anonymously so the lawyers can not find you and do so on multiple sites so they cant squash it.

[Reply](#)

[Report comment](#)

**CarKnow (@CarKnowLLC) says:**

**October 25, 2013 at 7:41 am**

Depending on the OEM, canbushack.org (not affiliated with these guys) has some good tips. Madox.net has Mazda info, Swedespeed for Volvo, ...

[Reply](#)

[Report comment](#)

**nickpl says:**

**October 22, 2013 at 1:14 pm**

Your (link) is missing the link:  
"Last time (link), we discussed..."

[Reply](#)

[Report comment](#)

**Mike Szczys says:**

**October 22, 2013 at 2:47 pm**

Indeed, thanks.

[Reply](#)

[Report comment](#)

**Chris says:**

**October 22, 2013 at 1:24 pm**

Really looking forward to the rest of this! Cant wait to have a play with CAN

[Reply](#)

[Report comment](#)

**denis says:**

October 22, 2013 at 1:28 pm

wouldnt mind more info on these databases too, when i sniffed out the steerignwheel and i-drive controlls on my car i just bashed the buttons and parsed the logs untill i found something plausible, took a few days, and that was just for basic user inputs never mind interesting stuff like wheel speeds and central locking status and what have you.

Reply

[Report comment](#)

**CarKnow (@CarKnowLLC) says:**

October 25, 2013 at 7:40 am

How about a Wiki? Sparse now, but hoping to build it up. Would love to see what you've sniffed on your Bimmer!

[http://vehicle-reverse-engineering.wikia.com/wiki/Vehicle\\_Reverse\\_Engineering\\_Wiki](http://vehicle-reverse-engineering.wikia.com/wiki/Vehicle_Reverse_Engineering_Wiki)

Reply

[Report comment](#)

**elwarpismo says:**

October 22, 2013 at 1:33 pm

Also forgot to add the break. Although to be honest, I kinda like the idea of first article always being fully displayed...hmmmm

Reply

[Report comment](#)

**Philip McKenna says:**

October 22, 2013 at 1:51 pm

In addition to single-wire CAN and high speed CAN some people may also be interested in learning about CAN-FD. CAN-FD uses the same physical layer as highspeed CAN but the CAN controller allows a higher bitrate during data transmission allowing CAN-FD to be backwards compatible with highspeed CAN with higher datarates(currently around 8MB/s) or to transmit longer messages of up to 64 bytes.

For some more details on CAN-FD see:

<http://can-newsletter.org/assets/files/ttmedia/raw/30e0cfdc05de5f831221487388087eb8.pdf>  
[http://www.vector.com/portal/medien/cmc/events/commercial\\_events/VectorCongress\\_2013](http://www.vector.com/portal/medien/cmc/events/commercial_events/VectorCongress_2013)

Reply

[Report comment](#)

**Pascal K says:**

**October 22, 2013 at 2:02 pm**

Suppliers won't give you there dbc files or CANdB Files. But it is common to just listen for some changes on the bus. Since every can node has a own Id you can just connect to the bus (most common is Baudrate 500k (then 250k and 125k)) so grab the steering wheel e.g. and turn it. With a small tool like PCAN VIEW, Vehicle Spy you can see the data changes. If there is a field which might have the data you want to see inside, try some filters like datasize 32bit or 8 bit and use different formats try two's complement and tada we got the value of a Hyundai sedan in less then 5minutes. That is what companys do for testing parts of vehicles.

Also note, data size is not fixed to 8Byte, that was years ago, look into the framed messages and there is also CAN-FD.

For diagnostics things get more difficult since the ECUs wait for commands to send there data and there is a exhaustive use of protocols, like XCP, CCP...

[Reply](#)

[Report comment](#)

**Maokai says:**

**October 22, 2013 at 2:17 pm**

Looking forward for more of this stuff. Thumbs up.

Also, why on earth is there an emergency stop on top of his dashboard?

[Reply](#)

[Report comment](#)

**Konrad says:**

**October 22, 2013 at 3:27 pm**

I bet it's a conversion to a autonomous-driving car. There the emergency stop makes sense if the car starts to act crazy ;)

[Reply](#)

[Report comment](#)

**Eric Evenchick says:**

**October 22, 2013 at 5:40 pm**

It's a prototype vehicle... the e-stop is a nice feature.

[Reply](#)

[Report comment](#)

Anybodysguess says:

October 22, 2013 at 2:31 pm

Why is there no break?

[Reply](#)

[Report comment](#)

Mike Szczys says:

October 22, 2013 at 2:49 pm

It does seem to clog up the front page a bit, huh? Added.

[Reply](#)

[Report comment](#)

Vic says:

October 22, 2013 at 4:30 pm

Most car manufacturers use the ASAM ODX standard for databases and there are multiple implementations of it...vector being one of the implementors. These databases contain everything from communication parameters to ecu variant identification templates to compute-methods for data sent on the bus. Most of the generic auto-shops out there use simple software provided by ECU manufacturers(eg. bosch, siemens) and grant access to simple DTC info and error memory info. Flash sessions or variant coding for instance require elevating the diagnostic session through a key and also much deeper manufacturer-specific knowledge.

[Reply](#)

[Report comment](#)

fIndr says:

October 27, 2013 at 7:20 am

There are multiple things that happen over the automotive networks.. there is the normal communication between ECUs (how fast am I going? are the doors open? what is the steering wheel angle?). The standard format for documenting the format of these messages is a DBC.

ODX or CDD (Vector CANdela) describe the diagnostic databases, i.e. what you can query using an external tool. These would be extremely helpful if they were released because they contain all of the diagnostic services (not just the legislated ones), and define all of the DTCs.

[Reply](#)

[Report comment](#)

charliex says:

October 27, 2013 at 11:59 am

A2L is a lot more useful (for ecu oems that use it), those are the holy grail.

[Reply](#)

[Report comment](#)

Trav says:

October 22, 2013 at 5:24 pm

Someone gave me a joystick off of an electric forklift. It uses the CANbus, now if I can only figure out the proper wiring so I don't let out the magic smoke when I go to test it....

[Reply](#)

[Report comment](#)

Eric Evenchick says:

October 22, 2013 at 5:41 pm

Oh, you've just reminded me that I should talk about how CAN is wired in a future post. Usually the DB9 connectors use pin 7 for CAN+ and pin 2 for CAN-.

[Reply](#)

[Report comment](#)

Joel says:

October 22, 2013 at 9:37 pm

HSCAN is also standardized in pins 6 and 14 on vehicles with an OBDII connector (and that have an HSCAN network of course!)

[Reply](#)

[Report comment](#)

ET says:

October 23, 2013 at 10:07 am

I'd definitely like a post on wiring/connectors.

I've only worked with it briefly, but for the machines I was working on, we used these god-awful Deutsch connectors.

Bulky (for the number of wires), expensive, and only attached to the delicate wires, not the tough outer plastic/rubber sheath of the cable (wire bundle).

I'd like to see the other stuff that gets used, what's common, what's standard, what's not, etc.

[Reply](#)

[Report comment](#)

rogier21 says:

October 22, 2013 at 8:53 pm

How did you plugin the CANbus on the car? I assume it's all well protected?

Reply

[Report comment](#)

matt says:

October 22, 2013 at 9:26 pm

The OBD2 port which is present on every car in the US from 1996 onwards.

Reply

[Report comment](#)

techb says:

October 22, 2013 at 8:57 pm

This comment isn't about the content, but more on the way it was presented. On the homepage of HaD, it looks like there is a double post of sorts. The bold green in the actual article is almost the same as the post name itself. Thought it was a bug at first lol. Maybe make the article section headers a darker green or something. Anyway, haven't made a post since the new overloads. I like the direction and what is being done. I see more and quality things here and am welcomed to the changes.

Reply

[Report comment](#)

Squirrel says:

October 23, 2013 at 8:56 am

Next up, MIL-STD-1553?

Reply

[Report comment](#)

rich says:

October 23, 2013 at 12:47 pm

There is basic info on the standardised OBD diagnostics parameters here.

[http://en.m.wikipedia.org/wiki/OBD-II\\_PIDs](http://en.m.wikipedia.org/wiki/OBD-II_PIDs)

If your looking to play around it is a good place to start.

Reply

[Report comment](#)

**charliex** says:

October 24, 2013 at 12:15 pm

The note i'd add to this is to take away the focus on 8 bytes, that's just what the underlying CAN protocol is using

From a diagnostic/reprogramming software point of view, ie where we're looking at it from, the actual message from the cars systems can be considerably longer, usually it is ISO 15765-2/ISO-TP the message is broken up into 8 byte packets, carrying 7 bytes of information, then typically reassembled inside the j2534 software and presented to the host software. look up CAN multi-frame message on wikipedia for details.

Nearly all reflash tools use multiframe messaging for instance, but if its via J2534 then it takes care of it, you can send long messages into J2534 and it'll just split it up into multiple CAN frames, and reverses the procedure for incoming.

[Reply](#)

[Report comment](#)

**CarKnow (@CarKnowLLC)** says:

October 25, 2013 at 7:35 am

This is a subject very near and dear to our hearts here at @CarKnowLLC. We create CAN/GSM bridges (we call them "CARduinos"), but even with access to CAN — you really need an understanding of what exactly is on the network to accomplish anything.

On our company website (I don't want to linkspam, so Google us), we have a link to a Wiki we've created in the hopes of building a user community for sharing reverse engineered CAN parameters. While it's rather sparse now, we have more data that we've collected internally and hope to publish soon. We hope you join us in doing the same, so that we can all access the information transmitted within the vehicles we own and operate. There's a lot of great potential here, and who knows — if we get enough user interest, we might be able to sway an OEM or two to the dark side.

Happy to opine, discuss, etc. if anyone has questions our company can help with. The hardware should be available for preorder shortly, either directly on our site or as part of a crowdfunding campaign.

[Reply](#)

[Report comment](#)

## Leave a Reply