# Some Shit About Trucks and Stuff I Guess

**Presented at DEFCON 24**

http://truckhacking.github.io

Six Q. Volts, Esq. Haystack McStuffins, PhD

June 1, 2020

## 1 Introduction

This guide serves as an introduction and basic reference to heavy vehicle networking and electronics. It is by no means a definitive guide. All the information herein is provided as-is, with no guarantee as to it's accuracy. We're human and we can screw up. Be careful when working on or operating Heavy Trucks. They are dangerous. Use common sense and don't do something like fuzz a moving vehicle while it is driving on the highway. If you find a mistake in the document, or for general hate-mail, email six_volts@sixvolts.org or haystackinfosec@gmail.com.

## 2 General Principles

There are a large number of electronic parts in a heavy truck or heavy vehicle. The term ECM, is used frequently, either as THE ECM, meaning the "Engine Control Module" or an ECM, an "Electronic Control Module". The lingo varies from manufacturer to manufacturer. Modern vehicles have a collection of ECMs to make everything turn diesel into spinning wheels. The engine itself may have multiple modules, or only one, again, depending on the manufacturer or the age of the vehicle. Here is (non-exhaustive) list of modules that may be found in vehicle:

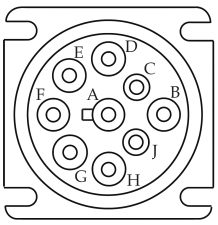
- ECM/MCM - Engine Control Module or Motor Control Module: this is for making the engine work. It control injectors, sensors, timings, and all those mechanical bits that make the diesel engine work. Sometimes this is the only interesting device in the truck.
- ACM - After-treatment Control Module: This is to control the engine's use of DEF (Diesel Exhaust Fluid) and regulate emissions. Some vehicles don't have one of these modules or integrate the functionality into the ECM/MCM.
- Brake Controller: There are several different varieties of these, depending on which brand of braking system the truck is using. This controls the pneumatic system

for the brakes and is typically connected to the vehicle buses. Bendix and Wabco are common brands.

- CPC - Common Powertrain Controller: this is another module that operates in a pair with the ECM/MCM on newer Detroit Diesel Vehicles.
- Body Controller: This module controls parts of the human-interfacing side of the vehicle such as lights, door locks, and things inside the cab of the truck.
- Transmission Controller: If the truck is equipped with an automatic transmission, it will have an extra ECM for the transmission. Manual transmissions are much simpler and don't require as many electronic controls, if any module at all.
- Instrument Cluster: Newer instrument cluster can be capable of some operations on its own and is more than a dumb read-out of things on the vehicle bus.
- Infotainment Unit or Radio: Yes, these are typically attached to the bus. This can be for reading vehicle speed for adaptive volume control, or to interface to wheel mounted buttons.

## 2.1 Diagnostic Ports

Most newer vehicle use a 9-pin Deutsch connector, specified in SAE J1939 part 13. This connector provides access to vehicle power, the J1939 vehicle network, the J1708/J1587 legacy network, and a few other pins that are available for other networks and proprietary uses. This connector is typically placed under the dash or nearby, left of the driver's seat in the cab of the vehicle. There are two versions of the connector which are mechanically identical - a gray/black connector and a newer green one. They differ in their support for 250Kbps (gray/black) or 500kbps (green).




| | |
|---|---|
| A | Ground |
| B | +12V/Battery |
| C | CAN/J1939 + |
| D | CAN/J1939 - |
| E | Reserved |
| F | J1708/J1587 + |
| G | J1708/J1587 - |
| H | Reserved |
| J | Reserved |

Figure 1: The 9-pin Diagnostic Connector typically found under the dash

Some vehicles (Volvo) have the J1939 port and an OBDII style connector. The pin-out for the OBDII-style connector differs from that of passenger cars. We have produced a PCB with the OBDII connector and screw terminals to assist in connecting to vehicles of this type (check the github). Older vehicles us a 6-pin connector without CAN/J1939 and only use J1708 - those vehicle are boring.

### 2.1.1 Vehicle Diagnostic Cables

The trucking industry and vehicle diagnostic vendors are seriously proud of their cables. They're worse than BestBuy about markup, sometimes charging over $100 for a J1939-to-DSUB15 cable. You can make one from parts (parts list on github) with a soldering iron and some patience, or buy one from china through AliExpress or eBay.

## 2.2 Fault codes

A Fault code is a diagnostic code indicating something is wrong with the vehicle or engine. These can be simple, such as the oil pressure is low, or more complicated - like "ECM Internal Chip Error". That typically means you need an new ECM. Fault codes may not render truck or module inoperable, but they may prevent it from functioning correctly.

## 2.3 Operating Modes

Trucks typically have three main operating modes, and each one has limitations.

- Key-off: Truck is off. Key is in off position. Some networks may continue to generate traffic for a short time after the vehicle has been shut off.
- Key On, Engine Off: Most of the electronics will power up and operate in this mode in preparation for the engine running or diagnostics. This is typically the mode for security analysis. You don't need an actual engine to get electronics to this state.
- Key On, Engine Running: The engine is running and burning dinosaur juice. This is tough, because it costs a decent amount of money to keep the engine running. Several systems only work in this mode, but this requires an entire truck, or at least an operating engine, which again can be expensive.

# 3 Electrical Principles

## 3.1 Truck Wiring

The recommended wiring for differential signals (CAN/J1939, J1708, etc) is twisted-pair 18-guage wire with one twist per inch. Automotive grade wire is highly recommended, such as stranded GXL automotive wire. You can easily make small segments of twisted wire by chucking two lengths wires into a drill on one end and a vice on another. Run the drill until the wire tightens to slightly more than one twist per inch, since it will loosen slightly when you release it from the drill and vice. Cut off the ends that were in the vice and drill and it is ready to use.

### 3.1.1 Truck Power

Most trucks operate on 12V DC power for their electronics. This usually connects directly to a lead-acid the battery for the vehicle. Some city buses and other specialty vehicles operate on 24V power. Be mindful of this when plugging into a heavy vehicle if the device is designed for 12V and not protected against 24v.

## 3.2 Differential Signals

Differential signals use two wires, a "high" and a "low" (Sometimes labeled P/N for positive and negative). Rather than having a signal at a set voltage and using a ground for reference, the two signals in a differential pair use each other as references. The biggest advantage to this is noise immunity - a spike of noise on both the high and low wires doesn't alter the difference between the two.

## 3.3 ECM Sensors

As you wire up different vehicle components, some of them may refuse to work or throw errors until certain sensors or other devices are connected. There several different types of sensors on ECMs, and we've grouped them into some basic categories:

- "Passive" Signals: simple resistance or voltage values, either fixed or do not change much over time normally
- "Active" Signals: These are typically PWM (pulse-width modulation), variable reluctance, or any other continuously changing signals
- Multiplexed Signals: Truck lingo for attached to a vehicle network like CAN. Some sensors and devices have dedicated networks, sometimes with only two nodes.

### 3.3.1 Passive Signals

Passive signals can typically be emulated with either a fixed resistor or an adjustable potentiometer or rheostat. Some traps to watch out for are power dissipation. Some of these sensors can pull a large amount of current, and so any resistor/potentiometer you use needs to be an appropriate wattage. Unfortunately, much of this information isn't included in the Vehicle/Engine service manuals. You'll need to do some basic circuit analysis and use common sense. If you don't know what Ohm's law is, Google it. Sensors that can be set like this include things like pressures, temperatures, and liquid levels. The sensor values might change slowly during the operation of a real vehicle, but they can be typically be set to a normal value and left alone. Some of the "normal" values for sensors can be found in the service manual for each engine or vehicle. Some of the sensor values are correlated and will throw errors if they don't make sense. If the temperature going into the engine is 1500 degrees and it comes out at negative three, something is askew and some of the ECMs will set a fault code.

### 3.3.2 "Active" Signals

Some sensors, such as the accelerator pedal, typically require a constant signal as to which position they are in to not throw a fault. Many of them are a PWM signal, which can be generated using a simple microcontroller or function generator. Other active signals like the Vehicle Speed Sensor can be a little more tricky. Usually there is a shaft coming out of the transmission going to the drive wheels, and on this shaft is toothed steel ring.

Figure 2: Tail-Shaft Tone Ring (center) Vehicle Speed Sensor (left)

This ring spins past a sensor that detects the change in magnetic field, generating a series of pulses. One of the electronic modules then counts these pulses, and interprets them as the speed of the moving vehicle. This signal can be reasonably high voltage in a moving truck. This sensor can be used to put "virtual miles" on a ECM sitting on the bench.

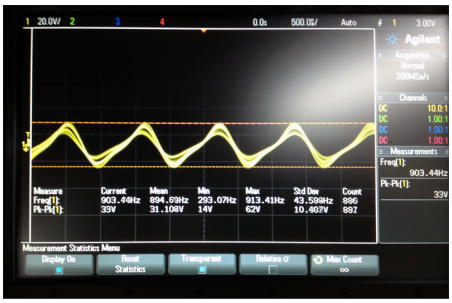



Figure 3: Signal trace from a Vehicle Speed Sensor

### 3.3.3 Multiplexed Signals

Newer vehicles have sensors and devices that are sometimes networked on their own. These can be on small, two-node CAN buses with non-standard baud rates. Some ECMs have dedicated CAN channels between modules, such as "Engine CAN" between the MCM and CPC modules on some vehicles. These can be other CAN variants besides J1939 such as ISO-CAN or regular 11-bit CAN with a proprietary messages.

### 3.4 Truck-In-A-Box

Conceivably, with a proper understanding of the network and sensors, one could assemble a collection of modules from a Truck, connect them together appropriately, and put them in an enclosure along with the necessary controls to emulate many of the sensors to create a "Truck-in-a-Box". This apparatus would be cheaper than an actual heavy vehicle and, because most of the electronics work just fine Key-On, Engine Off, this Truck-In-a-Box would be very useful for security and forensics analysis. So that's what we did - as shown in figure 4.

The original device pictured was built around a Navistar ECM, emulating a Navistar ProStar vehicle with a MaxxForce 13 engine.

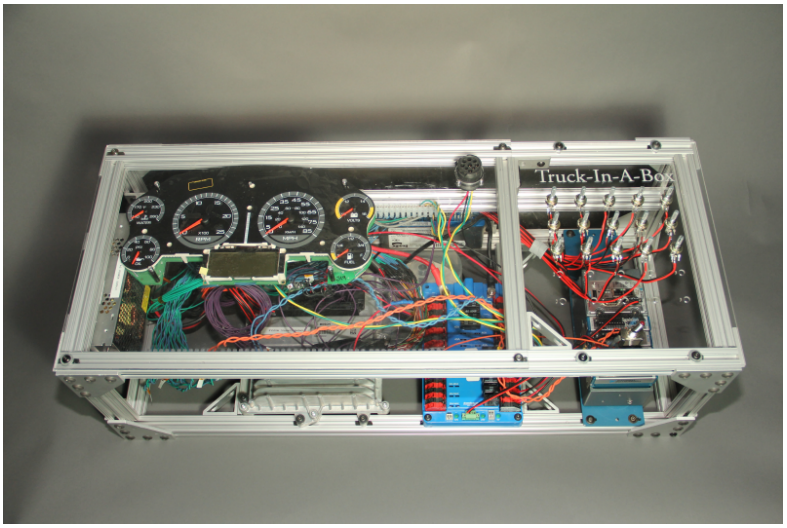



Figure 4: Truck-In-A-Box

## 4 SAE J1708 & J1587

### 4.1 Communication Hardware

J1708 is based on RS-485, a serial protocol that uses differential signaling supporting up to 20 nodes, with a maximum bus length of 40 meters. The bus runs at 9600 bits per second and can be interfaced with a standard UART on a computer or microcontroller. The circuit is active low and uses a dominant/recessive schema for bus contention and

### 4.2 J1708 Physical Layer

Byte format, message length, checksums, timing

### 4.3 MIDs and PIDs

#### 4.3.1 Packed PIDs

#### 4.3.2 Data Link Escape (Proprietary Extensions)

### 4.4 Old Transport Layer: The shitty one

### 4.5 New Transport Layer: reliable delivery

### 4.6 Truck Duck J1708 Implementation

PRU implementation, using our driver, etc.

## 5 SAE J1939

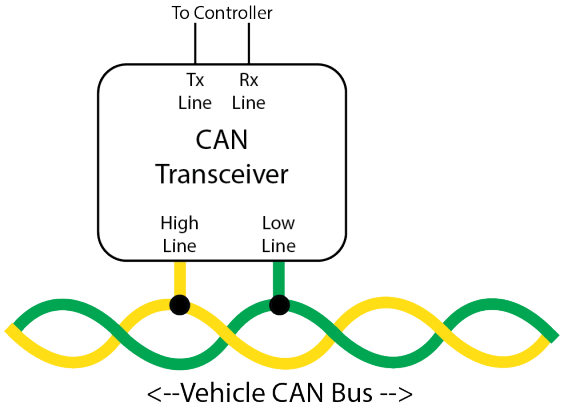



Figure 5: A simple CAN Transceiver

J1939 Is a protocol that sits on top of CAN bus. There are two parts to the CAN bus specification, part-A and part-B. Part A is what most passenger cars use, which uses 11-bit message IDs. Heavy trucks use part-B which specifies a 29-bit message ID. Both part-A and part-B share the 64-bit (8-byte) message payload size.

### 5.1 CAN and J1939 Hardware

The CAN bus is a differential-signaling communications protocol originally designed for vehicles, released by Bosch in the 80s. Every device on the network needs a transceiver, which are typically small 8-pin ICs. This is typically connected as shown in figure 5 with a Tx/Rx lines going to the controller and the differential-pair connection to the shared bus. CAN bus operates at speeds up to 1Mbit/s, however, heavy trucks traditionally use 250Kbps CAN for J1939. Newer vehicles with a green connector under the dash support 500Kbps speeds.

### 5.1.1 Bus Termination

CAN bus requires terminating resistors on the ends of the bus to prevent signal reflection. You can think of it like this: if you transmit a message down the wire, it travels down the wire in both directions from the node that sent it. When it gets to the end of the wire, the terminating resistor stops the message from traveling back down the wire again. If the resistor wasn't there, the message would bounce back toward the direction it came from and

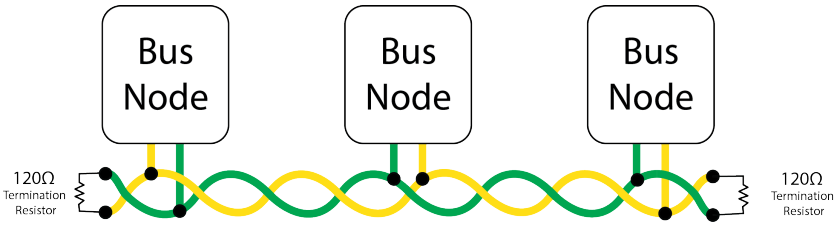



Figure 6: A 3-node CAN bus with termination.

## 5.2 Frame Format

Source addresses, destination addresses, extended CAN IDs, extended data page, etc

## 5.3 Proprietary extensions

## 5.4 Transport Layer

### 5.4.1 Broadcast Announce Messages (BAM)

### 5.4.2 Connection Mode

## 5.5 Truck Duck Implementation

J1939 Kernel Extension, J1939 canutils, Python socket module, our J1939 driver

# 6 ISO15765

## 6.1 Security Checks

## 6.2 Transport Layer

## 6.3 Integration with J1939

It uses its own transport layer over J1939, which has its own transport layer. Why.

# 7 RP1210

In the early days of electronic diagnostics on heavy vehicles, different vehicle diagnostic adapter (VDA) vendors' drivers had different interfaces. This placed an undue burden on ECM software writers; supporting each VDA meant supporting each VDA's driver, which was a nontrivial task. Recommended Practice 1210 (RP1210), created and promulgated by the Technical Maintenance Council of the American Trucking Associations (ATA TMC), standardizes the function calls used to initialize devices and to send, receive, and filter messages.

## 7.1 Use with CAN

## 7.2 Use with J1708

## 7.3 Use with J1939

## 7.4 Use with ISO15765

## 7.5 Debug logging with the Dearborn Group DPA

In the authors' experience, the best VDA for reverse-engineering purposes is the Dearborn Group (DG) DPA series. The DG driver suite includes options for robust logging of all RP1210 calls made to the device, greatly easing the process of dynamic analysis of diagnostic software.

## 7.6 Function Hooking

# 8 ECM Internals

Most Heavy Truck ECMs were, simply put, never designed to be opened after they were manufactured. Most of the ruggedness designed into them was to deal with the environment trucks can operate in - nearly anything. ECMs need to be water proof, expected to work covered in road grime, oil, or nearly anything. See figure 7.

Some ECMs have simple gasket seals and conformal coating, but are relatively simple to open. Some of the designs glue the PCB into the case and have to be milled apart to get at the internals. Several manufacturers use flex-circuits typically glued to the inside of aluminum case. Some of the flex-based ECMs wrap the design in a U-shape, making the tear-down procedure very nearly a destructive process.

Despite the physical construction issues, ECMs can be relatively simple embedded systems. Many of them run on older architectures that don't contain storage on the main processor, so they have external flash memory for program and data storage. Removing these chips and imaging them is relatively simple with an appropriate chip reader and a hot-air rework station. Newer systems that use integrated System-on-Chips with on-board storage are more challenging.

Thankfully, JTAG ports are common on newer ECMs and given that most of them can be updated over the vehicle bus, remote retrieval of code and data is also possible.

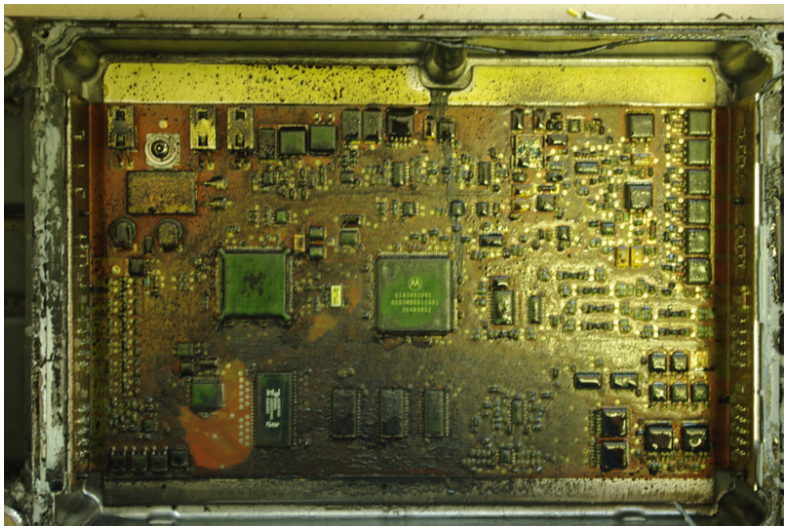


Figure 7: The inside of a ECM covered in... something gross.

```
00073728  ED F0 BF EB CB C5 D9 D3 E5 DF F3 EB FF F9 FF FF FF FF FF FF C4 BE D2 CB  íð¿ëËÅÙÓåßóëÿùÿÿÿÿÿÿÄ¾ÒË
00073752  DE D8 EB E5 F9 F2 FF FF FF FF FF FF BC FF C9 C3 D7 D0 E4 DE F2 EB FF F8  ÞØëåùòÿÿÿÿÿÿ¼ÿÉÃ×ÐäÞòëÿø
00073776  FF FF FF FF FF FF C2 BB D0 C8 DD D6 EA E4 F8 F2 FF FF FF FF FF FF B9 FF  ÿÿÿÿÿÿÂ»ÐÈÝÖêäøòÿÿÿÿÿÿ¹ÿ
00073800  C7 C0 D5 CE E3 DC F1 EA FF F8 FF FF FF FF FF FF BE B8 CA C4 D6 D0 E1 DC  ÇÀÕÎãÜñêÿøÿÿÿÿÿÿ¾¸ÊÄÖÐáÜ
00073824  EE E8 F9 F3 FF FF FF FF B6 FF C0 BB CB C6 D5 D0 E0 DA EA E5 F4 EF FF FA  îèùóÿÿÿÿ¶ÿÀ»ËÆÕÐàÚêåôïÿú
00073848  FF FF B9 B4 C2 BD CB C7 D5 D0 DE DA E8 E3 F1 EC FA F6 B3 FF BC B8 C6 C2  ÿÿ¹´Â½ËÇÕÐÞÚèãñìúö³ÿ¼¸ÆÂ
00073872  CF CB D9 D4 E3 DE EC E7 F6 F1 FF FA 7E 7E 7E 7F 7E 82 80 80 83 80 80  ÏËÙÔãÞìçöñÿú~~~~.~‚€€ƒ€€
00073896  80 80 80 80 FF 80 FF FF FF FF FF FF 46 31 4A 55 36 41 4B 43 36 33 57 4C  €€€€ÿ€ÿÿÿÿÿÿF1JU6AKC63WL
00073920  [redacted]  D0 D3 CB CE C8 C9 C8 C8 C4 C4 C4 C4 C4 C4 C4 C4 00 00  [redacted]ÐÓËÎÈÉÈÈÄÄÄÄÄÄÄÄ..
00073944  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......................
00073968  00 00 00 00 00 00 00 00 EC EC EC EC EC EC EC EC EC EC EC EC EC EC  ........ììììììììììììì
```

Figure 8: Data from a direct chip read with the VIN number highlighted

Embedded system forensics is still in its infancy for a number of reasons, including the large number of different designs and architectures. The future of research into heavy vehicles clearly needs to include device tear-down and firmware analysis.

# 9 Telematics

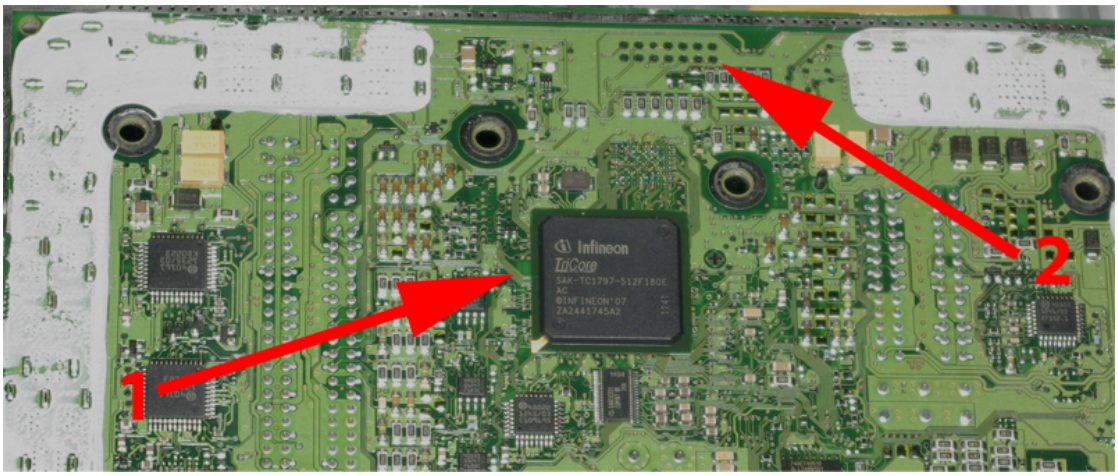



Figure 9: Modern ECM with integrated SoC (1) and JTAG/Programming port (2)