

Automotive On-Board Networks

Nothingface <alpha@area49.net>

2004.5.11

Late model automobiles contain a considerable amount of electronic equipment compared with vehicles in the past. Although some of these electronic devices are user visible appliances, such as entertainment and navigation systems, many are devices under the hood including controllers for fuel injection, anti-lock brakes, and airbags. The number of devices used, as well as the sophistication, versatility, and programmability of the devices is continually increasing. Not surprisingly, these devices are also networked, allowing them to communicate with each other and with additional equipment outside the vehicle for diagnostics and configuration.

Automotive electronic devices enable the logging of vehicle sensor data, particularly in the event of an accident or a near miss. Little information about these logging devices is readily available, because those with the information (vehicle and aftermarket tool manufacturers) are making an effort to keep the information difficult for the public to obtain. (I was personally denied membership in the only discussion group I am aware of on this subject because I am not law enforcement, I do not own a \$2500 tool for downloading this information, and I was not nominated by members of the group.) The primary interest in this information is law enforcement for forensic analysis of an accident scene. Since few realize that this information is recorded, an officer could easily connect a device and download a vehicle's crash information without the driver's permission or knowledge. This could be done either at the scene of an accident, while the driver is distracted, or afterwards when the vehicle is at a repair shop that is not likely to be concerned about the driver's privacy.

The need for electronic devices on an automobile arose, at least in part (in the U.S.), from federal law. Citing environmental concerns, the federal government mandated certain fuel efficiency standards that necessitated electronic control. The first regulation was known as On-Board Diagnostics (OBD). OBD required a few basic sensors and diagnostic procedures, but did not standardize the interface. A standard interface was introduced with On-Board Diagnostics II (OBD2 in this article, elsewhere abbreviated as OBD II or OBDII). OBD2 was mandated for all automobiles sold in the United States from 1996 onward. The majority of the OBD2 specifications were written by the Society of Automotive Engineers (SAE), with one notable exception written by ISO. The OBD2 standard covers all the details necessary to make interoperable equipment that complies with the federal regulations. OBD2 covers much more than the mini-

mal “emissions control” functionality necessary to meet federal regulations.

The OBD2 specification is primarily concerned with the communications among on-board devices and between on-board and off-board devices. OBD2 specifies a single physical interface connector, called the diagnostic link connector (DLC), with 16 pins (in two rows of 8), located on the driver’s side of a vehicle. OBD2 specifies three data link layers, any one of which is required to be present in a vehicle. Two are specified by SAE, and one is specified by the International Organization for Standardization (ISO). The two SAE data link layers are variable pulse-width modulation (VPW) and pulse width modulation (PWM). The ISO data link layer is generally called “ISO format”, as it is the only significant portion of OBD2 to be specified by ISO. The ISO format data link layer is conveniently similar to RS-232, and many hobbyists have taken advantage of that property. OBD2 specifies a network layer, including network addresses and packet formats for a variety of applications. The network layer is shared by all data link layers (VPW, PWM, and ISO). All of OBD2 up to the network layer is required by federal regulations.

OBD2 also references the controller area network (CAN), specified by Bosch and ISO, for other vehicle purposes. The CAN physical layer is considerably faster than the three OBD2 physical layers. It is most often used for intravehicle communication between different control modules. The DLC is specified to include a connection to the CAN network. Vehicle manufacturers are likely to provide expanded functionality on the CAN network as opposed to one of the three OBD2 networks.

The OBD2 network layer specifies packet formats for several functions. A few of these functions are required by federal regulations. Since automobiles are required to have a network for mandated purposes, many, perhaps all, automobiles also use this network for other purposes. Most common is the use of OBD2 for additional diagnostic purposes beyond emission control. Also common is the use of the network for uploading or downloading arbitrary blocks of memory from on-board devices. That memory can contain parameters for running the vehicle, stored data from on-board sensors, or even executable code for on-board microprocessors.

The most common use of OBD2 is to examine diagnostic trouble codes (DTCs). A DTC is an error code that is stored when a vehicle determines some abnormal condition. The action of storing a DTC usually causes the check engine light (in OBD2 terms, the malfunction indicator lamp, MIL) to illuminate. Less critical errors can cause a DTC to be stored without triggering the MIL. A mechanic, using a device called a scan tool, can read the DTCs from the vehicle, decode the DTC meaning, and use that information to fix the vehicle. The scan tool also allows a user to clear the stored DTCs, which will cause the MIL, if illuminated, to shut off. Obviously, if the problem with the vehicle is not fixed, the DTC will be triggered again. Depending on the DTC that was triggered, freeze frame data can also be stored. Freeze frame data contains values from relevant vehicle sensors at the time the DTC was stored. Another common use of OBD2 is to provide additional diagnostic information. Data from vehicle sensors can be queried continuously and reported. Vehicle

subsystems can be requested to perform a self test procedure and report the results.

Beyond the diagnostic capabilities of OBD2, many configuration tasks can be done over the network. Anti-theft systems that require a key (physical or electronic) can be programmed over OBD2. Advanced vehicle subsystems, such as electronic traction control or tunable air suspensions, can be calibrated over OBD2. Electronic fuel injection was one early use of electronic control, and a substantial aftermarket exists for reprogramming the engine management computer, typically to achieve higher output power. The aftermarket product takes the form of a device to connect via the DTC that programs the engine management computer, or a replacement memory chip that directly replaces the chip in the engine. Sometimes the aftermarket programming device will configure other parameters, such as calibrating the speedometer and odometer for different sized tires.

Another use of OBD2, which is not specified by SAE, and has been kept fairly quiet by the automotive manufacturers, is the crash data recorder (CDR). The CDR is part of the air bag sensor and deployment system. The CDR stores information relating to what is called a “deployment event”, a condition that causes the air bag to inflate, or deploy. The CDR may store information about a non-deployment event and a re-deployment event. A non-deployment event is basically a near miss that the CDR determined to be significant. A re-deployment event is an event after the air bag deployed, and is a bit of a misnomer since current generation air bag cannot deploy more than once. The information stored can include speed of the vehicle, state of the brake and throttle, and status of the driver’s seat belt.

There has been some speculation about the next generation of OBD, so called OBD3. The government is likely to mandate more substantial emissions control devices and procedures. A CDR is not currently required by law, but may be in the future. In the name of convenience to the vehicle owner, the government may mandate a system that continually reports vehicle operating status in lieu of yearly inspections. Very little is known concretely about OBD3, but for those who do not trust that the government will always mandate what is best for its citizens, it would be wise to be aware and involved before unacceptable laws get passed, rather than after.

The information and functionality available on a modern automobile via electronic networks is considerable. Though there are some standards in place for these networks, many critical pieces are not standardized. The majority of vehicle owners are effectively prevented from accessing this information on their own vehicles due to the exorbitant costs of compatible equipment and the unwillingness of manufacturers to provide specifications on reasonable terms. The inaccessibility of this information prevents casual mechanics from easily working on their vehicles, as well as preventing concerned citizens from determining exactly what information their vehicle is storing about them. There is a lot to technically and sociopolitically explore to be able to pop open the electronic information in a vehicle as easily as one can pop the hood.

Further Reading *On-Board Diagnostics for Light and Medium Duty Vehicles Standards Manual, SAE HS-3000.* Society of Automotive Engineers, Inc.
<http://www.sae.org>