Pass-Thru Programming Challenges

By Darren Todd

Pass-Thru programming is the process of updating a vehicle's ECU software via an interface tool, often referred to as a VCI (Vehicle Communication Interface). The VCI tool is connected to the vehicles OBDII connector to allow access to the vehicle's communication network(s). This method is in accordance with the SAE standard known as J2535, officially introduced into the U.S. in 2004, Europe in 2009 and Australia in 2013.

Performing Pass-Thru programming relies on having access to OE software, usually via a 'portal' with associated registration and costs. Access to this software (and other workshop relevant data) is a hot topic that has been discussed in Australia previously and is fortunately strongly lobbied by organisations such as the AAAA and their 'Choice of Repairer' campaign.

Access to vehicle information and data is a top priority. However, manufacturers are starting to 'lock out' aftermarket scan tools from accessing vehicle networks via the OBDII connector.

Traditionally, OBDII connectors are linked to a 'gateway' ECU. This ECU distributes messages between the multiple vehicle networks and the OBDII connector. There is a direct physical connection between the OBDII connector and the vehicle networks (e.g. CAN network of the powertrain).

As vehicle technology develops, manufacturers are becoming more concerned with vehicle 'hacking' and the implications of malicious (and even unintentional) software interference. It does not take much to imagine what could go wrong if systems such as lane keep assist, automated emergency braking or even autonomous driving were compromised!

Ford gateway ECU (integrated with OBDII socket)

Rear view of gateway (vehicle side).

Most manufacturers are now using the 'gateway' ECU to isolate the OBDII connector from the rest of the vehicle, effectively creating a firewall akin to the firewall on your home PC.

New vehicles from Ford Motor Company, for example, are equipped with updated gateway ECUs which physically isolate the vehicle's networks from the OBDII connector.

Any vehicle information or data accessed via the OBDII connector, must pass through the gateway ECU microprocessor. With a lack of physical connection and the addition of software security, accessing vehicle information other than basic legislated diagnostics, is prohibited.

Complex 'seed and key' security is implemented within the gateway ECU so only authorised devices can transmit carefully screened messages to the vehicle.

OK, enough theory - how does this affect you in the workshop?

For OE level diagnostics, cooperation is required from the manufacturer to bypass the security firewall. Without this there will only be basic OBDII fault data for emissions related systems.

Measuring CAN network resistances can only be performed on the vehicle-side of the gateway ECU connector i.e. it is not possible to measure the resistance between pin 6 and 14 of the OBDII connector (60 Ohms) to check wiring integrity.

In case of gateway ECU replacement, there is no way to discern the type of gateway ECU installed in a vehicle with a visual inspection; they are physically identical. Refer to the part number to ensure that the correct part is fitted.

To successfully diagnose, service and repair vehicles in the workshop, the "Choice of Repairer" campaign is an essential part of moving forward.

If you would like to learn more about the history, required equipment and real world applications of Pass-Thru programming, Bosch offer a comprehensive evening training session..

Darren Todd is the Senior Technical Service Trainer at Robert Bosch (Australia) Pty Ltd in Automotive Aftermarket and is responsible for developing and delivering their comprehensive technical program. Email automotive.training@au.bosch.com for information on Bosch Automotive Technical Training courses, including all 12 course descriptions, dates, times and locations.