CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

Reverse engineering of CAN communication

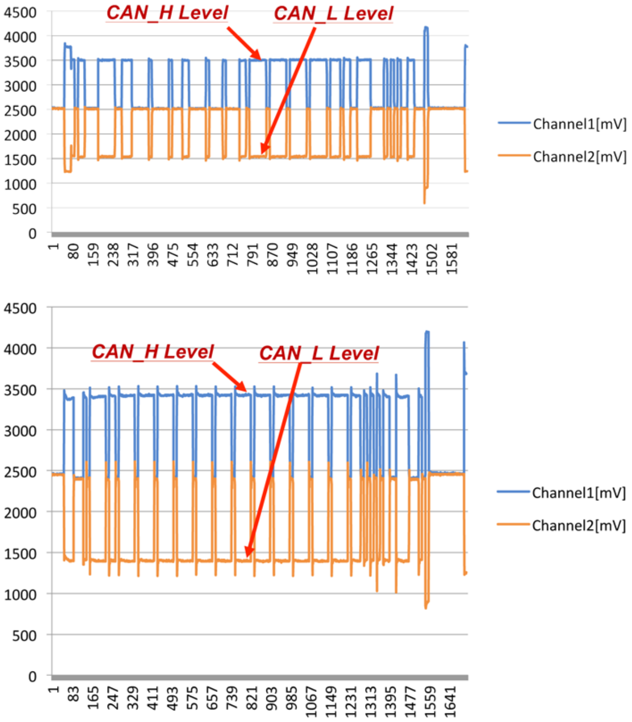
Sometimes you may need to reverse engineer the CAN communication. Examples are automotive competitor analysis, telematics applications such as fleet management, and disabled driver applications.

Dr. Chris Quigley, David Charles, and Richard McLaughlin explain in the article “Reverse engineering of CAN communication” a process that allows the user to identify, which CAN data frames are transmitted by a particular ECU. This is achieved by getting the electrical signature of each CAN data frame and matching known frames with unknown ones. Therefore, the transmitting ECU of the unknown CAN data frame can be determined.

The method for determining, which identifiers come from a particular ECU is to first get electrical signature plots of known diagnostic response frames and compare with electrical signature plots of the real-time control frames. The authors show how to achieve this using Warwick Control’s tool X-Analyser coupled with a Picoscope PC oscilloscope and a Kvaser CAN USB interface.

The method shown in this article can be used as evidence to support hypotheses when reverse engineering. Many times, during reverse engineering exercises, the authors want to isolate CAN data frames from a particular ECU. This method of plotting electrical signatures by noting the modal average of CAN_H versus CAN_L levels for each CAN data field bits has shown that it is a very good assistance in accomplishing this.

The approach discussed in this article is not limited to Classical CAN networks. CAN FD is the obvious next network to look at. However, electrical signatures could be obtained for many other network technologies e.g. Flexray, which uses also a differential signaling approach. It may be possible to characterize the signals on a LIN network. However, a slightly revised approach would need to be adopted for deriving an electrical signature since it does not use differential signaling.



Electrical characteristic of ECU A and ECU B (Photo: Warwick Control)

Download the complete article in PDF format here or the full magazine.

hz