Reverse engineering of CAN communication

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

The typical reverse engineering process is concerned with moving a sensor and watching the CAN network for message changes. For example, wind down a door window and see if this kicks-off changes in CAN frame data fields. Many CAN networks have many frames originating from many ECUs (electronic control units). This means it is difficult to watch all of them at the same time. It would be far easier if you could simply watch a smaller number of CAN data frames to observe changes by isolating the ECUs the frames originate from.

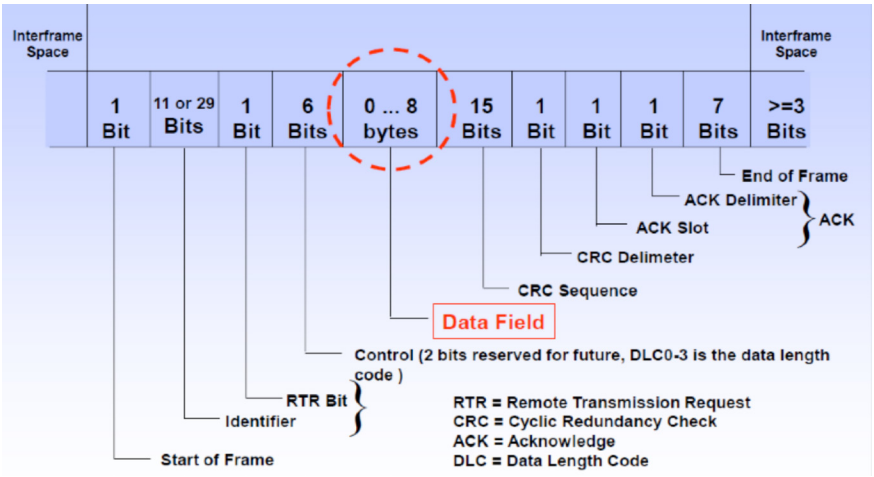


Figure 1: Construction of CAN frame (Source: Warwick Control)

This article describes 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. We show how to achieve this using Warwick Control's tool X-Analyser coupled with a Picoscope PC oscilloscope and a Kvaser CAN USB interface.

What is a CAN message electrical signature?

A CAN interface electrical signature is something that is largely unique about any CAN data frame sent by an ECU. Therefore, you would expect all bits transmitted by an ECU to have the same electrical characteristics. For example, a CAN bit comprising of the voltages of CAN High and CAN Low (CAN_H and CAN_L) should show something unique for each ECU due to the physical makeup of the CAN interface (e.g. node position and distance on the bus).

Figure 1 shows different fields that make-up a CAN data frame. Due to the nature of the contention-based access method of CAN, the arbitration field (containing the CAN ID) should not be considered for the electrical signature, as there may be several ECUs communicating within this field and therefore influencing the electrical signal.

Once the arbitration process is completed, there is just one ECU sending bits to the network. This is where you see a unique electrical signature for this ECU. To obtain a unique signature that represents its transmitting ECU, the measurements should be taken from this part of the CAN frame, which is when only one ECU is transmitting.

To illustrate the unique electrical characteristics of each ECU in a vehicle, Figure 2 and Figure 3 show the slight differences in the CAN_H and CAN_L voltages for two different ECUs from a modern passenger car. These are referred to as ECU A and ECU B. It can be seen that the CAN_H and CAN_L voltage levels are different for these two ECUs.

Generating electrical signatures

The methodology considered in gathering an electrical signature for each CAN bit, allowing us to ascertain the ECU it comes from, is to consider the CAN_H and CAN_L voltage values to associate CAN data frames to ECUs.

Method– Analysing the voltages of CAN_H versus CAN_L

Process:

- Log one example of each CAN message oscilloscope trace
- Isolate the CAN data field only
- Split CAN data field bits into dominant (logic 0) and recessive (logic 1)
- Calculate modal average value of CAN_H and CAN_L voltage levels for dominant bits only

Data is now ready for cluster plots.

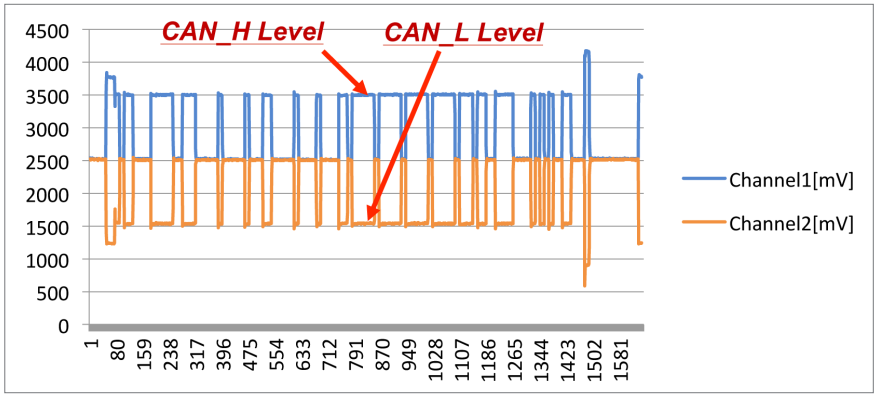


Figure 2: ECU A – electrical characteristics (Source: Warwick Control)

Example in X-Analyser: Figure 4 shows the display in X-Analyser utilizing the Picoscope interface. Here you can see CAN data frames are logged on the top half of the display. One of the CAN data frames is selected (highlighted), and the physical signaling of that frame is shown on the lower half of the display. Note that from this, we can gather the voltage levels of the dominant bits in the data field (CAN_H, CAN_L).

These waveforms can be exported as an Excel file to show readings of the CAN data frame at a sample point. This is done within X-Analyser by the "export frame" button to export the selected frame and using the "export all" button to export all the frames on that collection. An example of the data that is exported is shown in Figure 5.

The information given in the Excel file is:

- Frame ID (hexadecimal)
- DLC
- Data (bytes in hexadecimal)
- Error frame (true or false) (false if a good CAN frame)
- Samples per second
- Exported on (date)
- Time (of sample for that frame, starts at zero)
- CAN-H and CAN-L voltages
- Region name (region of the frame the data showing, is in)
- Additional region (shows where bit stuffing occurs)

Once this information is exported to Excel, we can calculate cluster points using the method taking the modal average of CAN_H and CAN_L voltages from CAN data field (dominant bits only).

The data is analyzed by recording the level of CAN_H and CAN_L dominant bit voltage levels within the data field and coming up with a single modal average measure for both CAN_H and CAN_L. These can then be put onto a cluster plot so that the clustering of CAN messages from a particular ECU can be observed. The following case study illustrates the data collection methods, and process utilized in plotting the CAN ID clusters from the Excel modal average values. This allows a researcher/ ▷

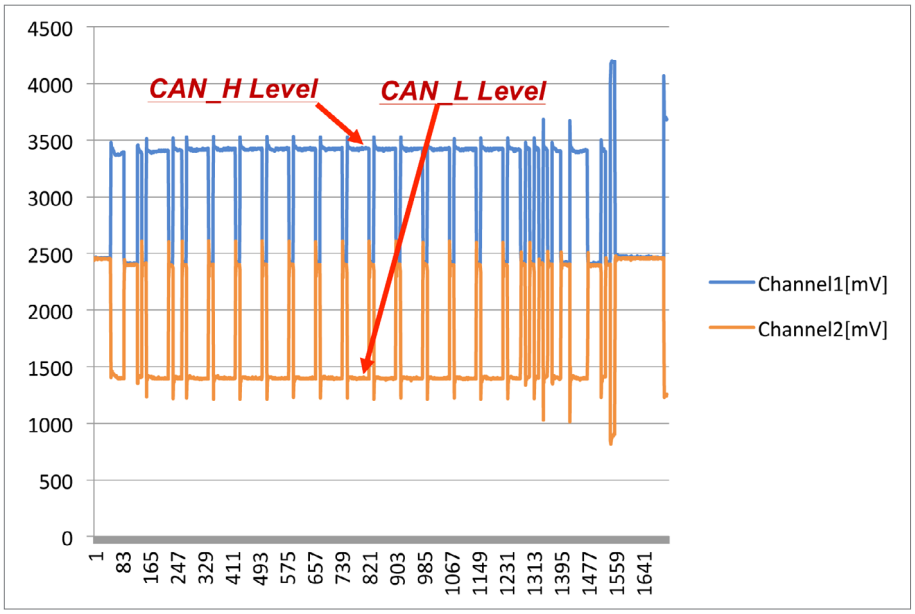


Figure 3: ECU B – electrical characteristics (Source: Warwick Control)

engineer to ascertain, which ECU has originated the real-time CAN data frame.

Methodology for identifying transmitting ECU

The basis for this methodology is that each ECU on the CAN network will exhibit its own unique electronic characteristics which are influenced by aspects such as its electrical components and tolerances, CAN transceiver, connector characteristics, and location in the CAN network. This can therefore be used to match unknown CAN data frames with known CAN data frames. In the automotive industry, the real-time control CAN data frames are proprietary. However, the identifiers diagnostic messages used for manufacturing and service garages are standardized in the ISO 15765 series and/or across an automotive manufacturer.

It is well known that many vehicles using standardized CAN identifiers to make a diagnostic request to the engine controller: For example, CAN-ID 7E0h and that the engine controller responds on CAN identifier 7E8h. Therefore, the summary of the methodology is described by the following steps:

- Send diagnostic requests
- Get signatures of all responses and real-time CAN data frames
- Analyze and plot the data on a cluster diagram

Figure 6 shows an example of the equipment setup utilizing X-Analyser connected to the CAN network via the Kvaser CAN/USB interface and the Picoscope interface. Referring to Figure 6, the Kvaser interface is used to generate diagnostic request messages, and the Picoscope is used to receive the diagnostic response message for analysis of the physical signature.

X-Analyser software is used to create the transmitters of CAN-ID $7E0_h$ (or 700_h to $7FF_h$ for other ECUs) through the object transmitter and uses the Kvaser interface to send these messages onto the bus. The Picoscope will see the sent transmitter (CAN-ID $7E0_h$) and read the response to this message of CAN-ID $7E8_h$. The frame bits of the data frame with the CAN-ID $7E8_h$ can then be analyzed through the analog network analyzer in X-Analyser.

More information about the diagnostic request can be found in ISO 15765-4:2016 [1]. The basic information needed is diagnostic request have the hexadecimal CAN-IDs ranging from 700_h to $7FF_h$. The standard emission diagnostic request message is known to be ID $7E0_h$ and the expected response from the ECM (Engine Control Module) is ID $7E8_h$. Referring to ISO 15765-4:2016, page 29, it also known that the TCM (Transmission Control Module) diagnostic request CAN-ID is $7E1_h$, and the response frame uses the CAN-ID $7E9_h$. Many of the other ECUs are manufacturer-specific, but most can be ascertained utilizing an OBD tool for a particular car model. For example, in many models, the ABS ECU is known to have a request of using the CAN-ID $7E2_h$ and a response using the CAN-ID $7EA_h$.

A diagnostic response's ID will increase in value by 8 and give the response i.e.;

Request ID = $7E0_h$ Response ID = $7E8_h$ 8 = $7E8_h$ to $7E0_h$

An example of diagnostic request CAN data frame is;

CAN-ID = $7E0_h$ DLC = 8 Data = $02\ 10\ 01\ 00\ 00\ 00\ 00\ 00_b$

Therefore, we expect a response from the Emissions (Engine) ECU using the CAN-ID $7E8_h$.

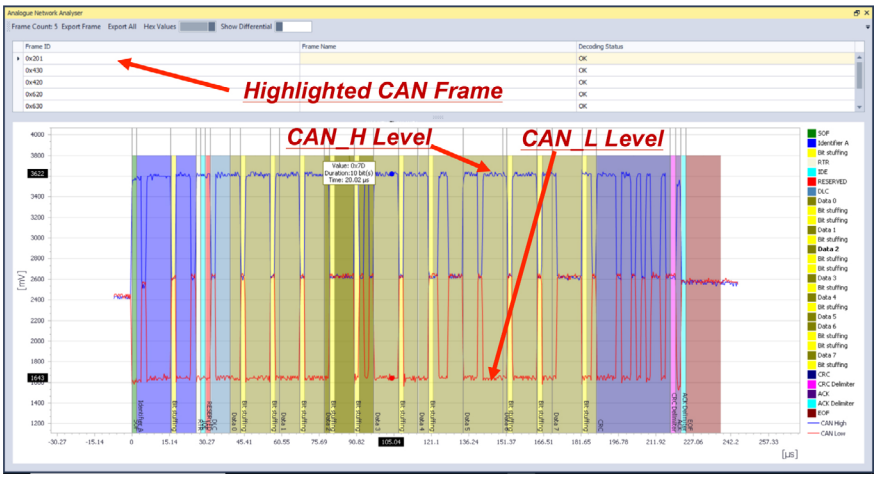


Figure 4: Highlighting a CAN frame within a Picoscope display (Source: Warwick Control)

	A	B	C	D	E	F	G	H
1	Export of Decoded CAN Frame			Time (us)	CAN High (V)	CAN Low (V)	Region Name	Additional Region
2	Frame ID	1CFFBC00		0	2.264	2.217	SOF	
3	DLC	8		0.144000009	2.303	2.257	SOF	
4	Data	C4 F8 FF FF 0B 27 C8 07		0.288000018	2.264	2.257	SOF	
5	Error Frame	FALSE		0.432000028	2.303	2.257	SOF	
6	Samples per Second	6944444		0.576000037	2.303	2.257	SOF	
7	Exported On	01/02/2018 10:43		0.720000046	2.303	2.257	SOF	
8				0.864000055	2.303	2.257	SOF	
9				1.008000065	2.303	2.217	SOF	
10				1.152000074	2.303	2.257	SOF	
11				1.296000083	2.264	2.257	SOF	
12				1.440000092	2.264	2.257	SOF	
13				1.584000101	2.303	2.257	SOF	
14				1.728000111	2.303	2.257	SOF	

Figure 5: Example Excel data exported for an extended CAN frame (Source: Warwick Control)

If there is no response to other requests, it means that this diagnostic function is not supported in this vehicle. The plotted chart in Figure 7 shows the diagnostic response messages in the 1st candidate car. From this, we ascertained the Electrical Signatures of CAN-IDs 728_h, $7E8_h$, 738_h, and 768_h. From the manufacturer's specification, it is possible to establish the functions of these ECUs.

Data capture on X-Analyser and Picoscope

The clusters show, which messages are associated with the same ECU. The results from two candidate vehicles are shown on the next page. Candidates 1 and 2 were electrically good CAN networks i.e. good grounds and low noise. The methodology used here was to plot the modal CAN-H and CAN-L values from the data segment of the CAN data frame to produce the clusters shown. This modal value would be taken from the region of the CAN data field bits for dominant ones only.

Candidate 1: In the 1st Candidate vehicle, the diagnostic request messages were sent with the response results that plots the electrical signature shown in Figure 7.

Here we are plotting the cluster points using CAN_H versus CAN_L. From the specification of this vehicle, the resulting diagnostic response frames are interpreted as follows:

- CAN-ID 728_h – Instrument cluster
- CAN-ID $7E8_h$ – Engine ECU
- CAN-ID 738_h – Steering ECU
- CAN-ID 768_h – Brake control module ECU

After the diagnostic response signature is established, we then collected the real-time CAN control frames and plot the electrical signature shown in Figure 8.

Here we have established that the general electrical signatures of the real-time CAN data frames closely match up with the diagnostic response messages. Therefore, we can ascertain that they come from the following ECUs:

- CAN-IDs 190_h, 275_h 430_h, 433_h, 460_h from Instrument ECU

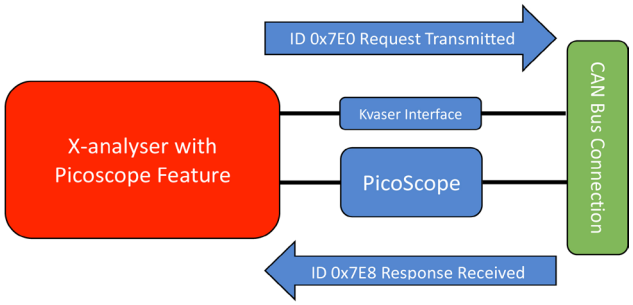


Figure 6: X-Analyser connection to a car via Kvaser interface and Picoscope PC oscilloscope (Source: Warwick Control)

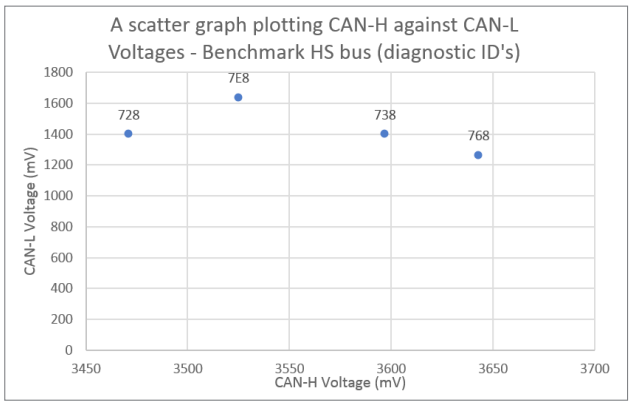


Figure 7: Cluster plot of the diagnostic response CAN messages for vehicle candidate 1 – CAN_H modal voltage versus CAN_L modal voltage (Source: Warwick Control)

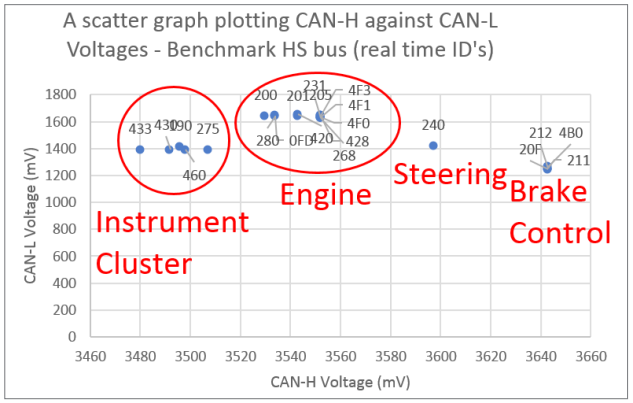


Figure 8: Cluster plot of the real-time CAN messages for vehicle candidate 1 – CAN_H modal voltage versus CAN_L modal voltage (Source: Warwick Control)

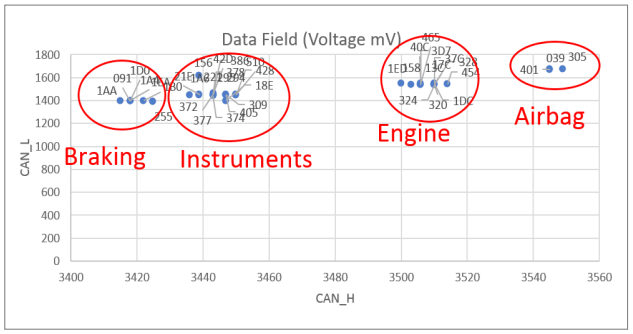


Figure 9: Cluster plot of the real-time CAN messages for vehicle candidate 2 – CAN_H modal voltage versus CAN_L modal voltage (Source: Warwick Control)

- CAN-IDs 200_h, 201_h, 205_h, 231_h, 268_h, 280_h, 420_h, 428_h, $4F0_h$, $4F1_h$, $4F3_h$ from Engine ECU
- CAN-ID 240_h from EHPAS ECU
- CAN-IDs $20F_h$, 211_h, 212_h, $4B0_h$ from Brake control ECU

This information will allow reverse engineering methods to help ascertain the functions of these CAN messages. In X-Analyser, it is possible to isolate these messages and perform various investigation methods to determine the functions of the individual signals within these messages.

Candidate 2: To further verify the validity of this method, a similar method was performed on a 2nd candidate vehicle for which the CAN specification was available. The result is illustrated in Figure 9 showing the electrical signatures of the captured real-time data of this vehicle.

Here we can observe that the messages come from the following ECUs:

- CAN IDs 091_h, $1AA_h$, $1A4_h$, $1B0_h$, $1D0_h$,$1EA_h$, 255_h from Brake control ECU
- CAN IDs 156_h, $18E_h$, $1A6_h$, $21E_h$, 221_h, 294_h, 295_h, 309_h, 372_h, 374_h, 377_h, 378_h, 386_h, 405_h, 428_h, $42D_h$, 510_h from Instrument ECU
- CAN IDs $13C_h$, 158_h, $17C_h$, $1DC_h$, $1ED_h$, 320_h, 324_h, 328_h, 376_h, $3D7_h$, $40C_h$, 454_h, 465_h from Engine ECU
- CAN IDs 039_h, 305_h, 401_h from Airbag ECU

Summary and Conclusion

The method shown in this article can be used as evidence to support hypotheses when reverse engineering. Many times, during reverse engineering exercises, we 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 shown 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.

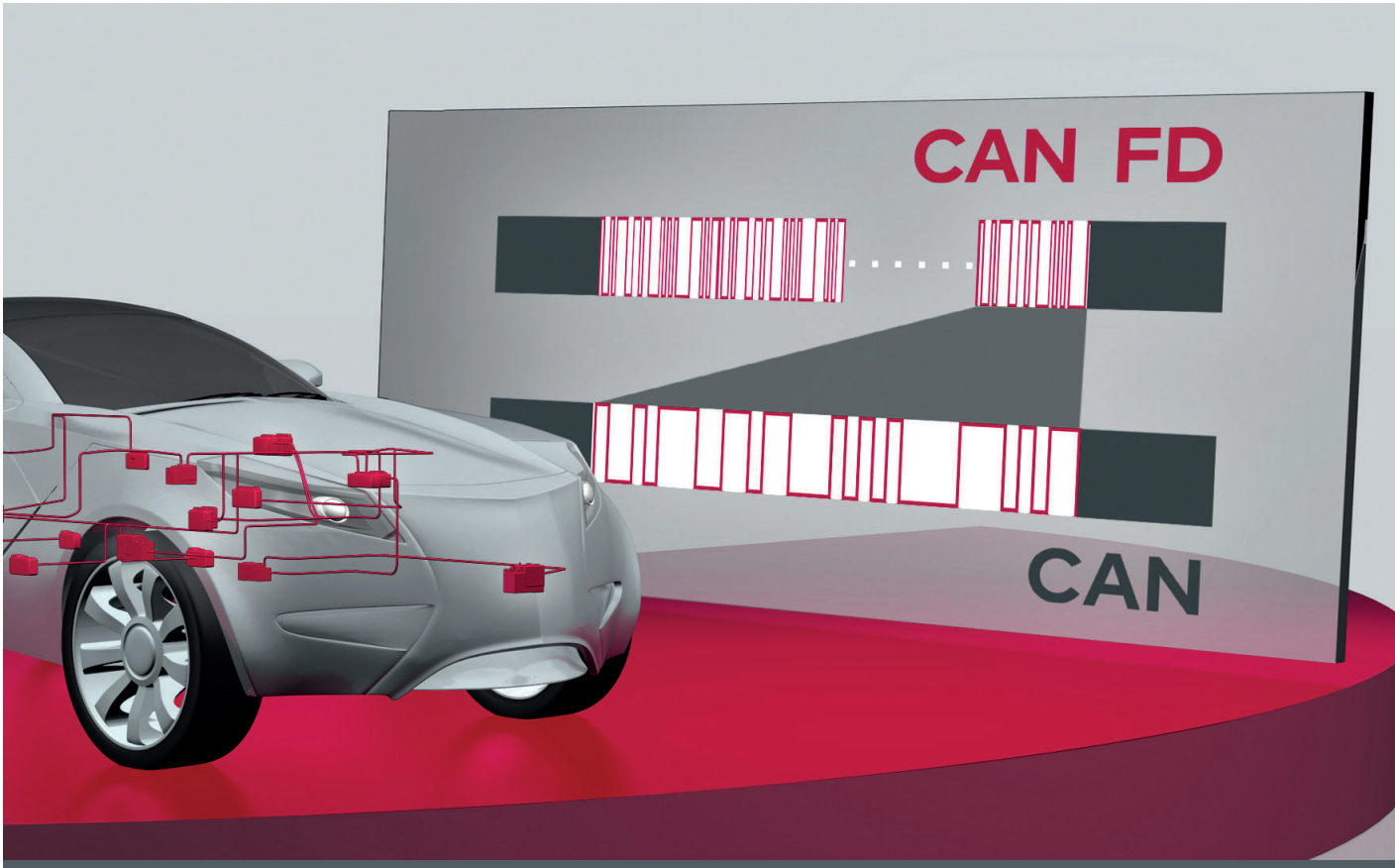
References

[1] ISO 15765-4 (2016) - Road vehicles — Diagnostic communication over Controller Area Network (DoCAN) Part 4: Requirements for emissions-related systems

Authors

Dr. Chris Quigley, David Charles, Richard McLaughlin
Warwick Control Technologies
enquiries@warwickcontrol.com
www.warwickcontrol.com

VECTOR



First Class Solutions
for Your CAN (FD) Projects

Your Universal Tool Chain

Increase efficiency of your projects with the universal tool chain from Vector:

- > High-professionial tools for testing, flashing and calibrating ECUs
- > Flexible network interfaces
- > New all-in-one network disturbance interface
- > Powerful logging solutions for test fleet operators
- > High performance oscilloscope
- > Proven design tools for network architectures
- > Easy to configure AUTOSAR basic software
- > Worldwide engineering services and trainings

More information: **www.can-solutions.com**

More CAN power by Vector: benefit from 30 years of networking experience.