VOLVO

Volvo Group North America

Ray Istenes
Senior Regulation Specialist
Volvo Group Trucks Technologies
13302 Pennsylvania Avenue
Hagerstown, MD 21742
April 6, 2016

Clerk of the Board
Air Resources Board
1001 I Street
Sacramento, CA 95814

Re: Volvo Group Comments to Proposed Revisions to On-Board Diagnostic System Requirements for Heavy-Duty Engines, Passenger Cars, Light-Duty Trucks, Medium-Duty Vehicles and Engines

Dear Clerk of the Board;

The Volvo Group respectfully submits the following comments in response to the Notice of Public Availability of Modified Text and Availability of Additional Documents posted on March 21, 2016.

Comments on FRO 1968.2 (Proposed 15-Day Notice)

(g)(1.2.2) SAE J1962 "Diagnostic Connector":

Comment: The latest published version of ISO 15031-3 is February 9th 2016 and SAE J1962 is currently being published.

(g)(4.7.4)(B) Software Calibration Verification Number:

Comment: The proposed modification requires the ECU to send a negative response code for a CVN request which occurs after a reprogramming event, volatile or non-volatile memory clear, or battery disconnect before the CVN has been calculated in the ECU. A more transparent and easier way to implement this feature would be to use 0x0000 as a default CVN as specified in (g)(4.7.4)(C) for CVN communicated from other ECUs/smart devices.

(g)(4.10.2) Erasure of Emission-Related Diagnostic Information:

Comment: The requirement that prohibits the OBD system to clear DTCs from only one ECU if that ECU supports more than just comprehensive components should be reconsidered.

In the reasoning for this updated requirement ARB refers to I/M "cheating", however, the reason why permanent DTCs were introduced more than ten years ago was to prevent I/M cheating. ARB states that there are too many issues with improper implementations of permanent DTCs. The proposed modification will be more difficult to implement and verify, yet easier to by-pass. The relief from this requirement for ECUs supporting just CCM is not truly a relief because the consequence will be to have two different strategies and implementations, two verification methods and two ways to handle OBD ECUs in the aftermarket. This will affect the OEM development, fault tracing methods in the aftermarket, service literature and training of service technicians for minimal or no environmental gain.

The technical side is that most ECU diagnostic communication software is built around OSI-layers, there is one module getting the CAN frames and transmitting a diagnostic service message to the upper layer of the software. The diagnostic communication module (DCM) receives the message without knowing the sender or how it was sent (physically or functionally). The DCM executes the service message and sends the response back to the lower layers which will truncate the message into CAN-frames and send to the tool (See Figure 1). It will be a technical burden to "hack" the OSI-stack in order to let the service "Clear DTC" to know how it was addressed, for just one of the services. Many OEMs base their software implementations on functionality defined by Autosar and this change will cause an update of the Autosar platform or software workarounds done by the system supplier, and some of the standard documents (e.g. SAE J1979, ISO 14229, ISO 27145) may need to be updated.

Thus, the risk for mistakes and misinterpretation is extremely high. There will be different DCM's between the OBD ECU's and the rest of the vehicle, which will double the verification for the vehicle manufacturer. Service methods will be affected for all ECUs (OBD ECUs and non-OBD ECUs) on the same network. This means that all faults in all ECUs (OBD and non-OBD) must be fixed before sending the Clear DTC service.

The SAE J1699-3 is the conformance test specification but it focuses on SAE J1979 communication which is by definition only sent functionally. This means that there is no conformance tool for the enhanced diagnostics and it may be very difficult to make a tool which supports all enhanced diagnostic protocols (ISO 14229-1 is implemented by many but not all OEMs for enhanced diagnostics).

Implementing the proposed medication introduces considerable risk for service technicians to by-pass these systems in the field. One method to by-pass the requirement would be to pull the fuse to the ECU when you want to clear codes, this works if the ECU stores the DTCs in KAM. Another way to tamper is to pull the fuse to the other ECUs (if DTCs are stored in non-volatile memory) and send the Clear DTC service. It is possible to go to "Programming Session" for the other ECUs and then return to normal operation after the Clear DTC service has been sent. The requirement will not prevent anyone from cheating at the I/M station and it would be more prudent to improve the SAE J1699-3 standard and the tool to verify the implementation of Permanent DTCs. Another improvement would be to implement the readout for Permanent DTCs in the I/M stations.

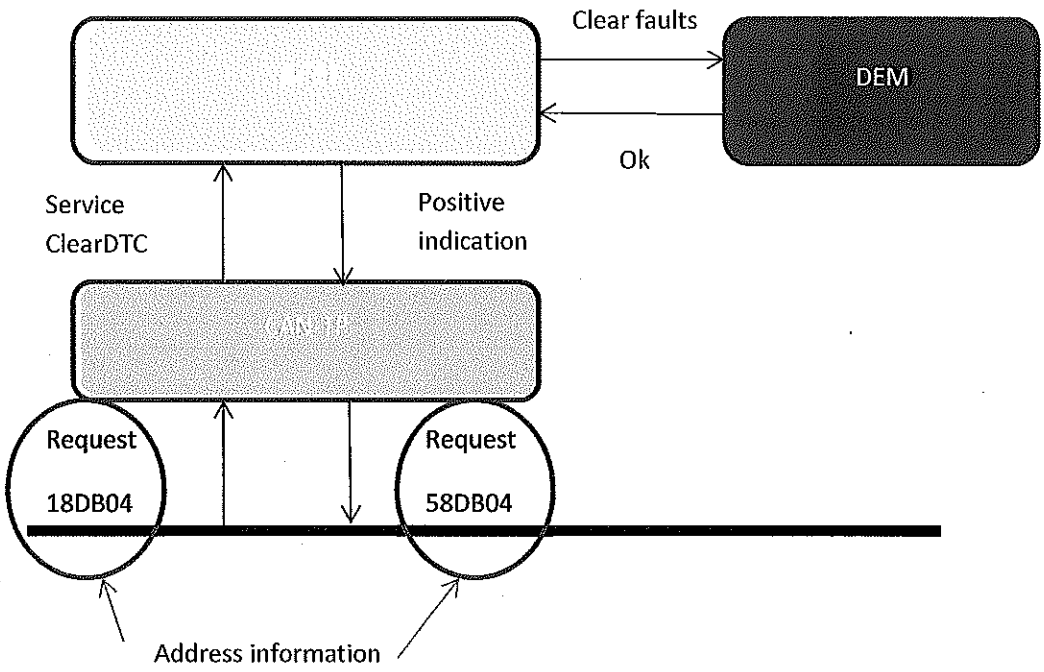


Figure 1: Example of OSI-layering in modern diagnostic software.

(g)(6.9) Vehicle Operation Tracking Requirements

Comment: The proposed modification provides that additional data collected may be used by ARB or their subcontractors if consent is granted. Volvo is concerned that this data is thereby available to other parties since it is on an open protocol. Drivers may then end up in a dependency situation towards their employer and may not have the same possibility to "not consent". The consent becomes ineffective in terms of protecting data privacy.

Comments on FRO 1968.2 (Proposed 45-day notice)

(g) (1.10.5) thru (1.10.11) SAE J1939 Consisting of:

Comment: This set of documents is not applicable to FRO 1968.2 since SAE J1939-73 is not an allowed OBD diagnostic protocol for LDT/PC.

(g) (4.4.6)(D)(ii) Permanent fault codes:

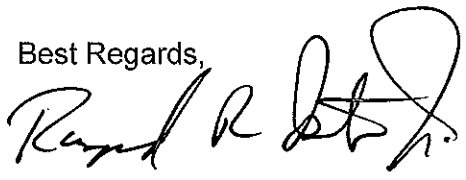
Comment: We assume this requirement was added due to a perceived risk of I/M tampering. However, this requirement is not easy to fulfill, the standardized mechanisms of the OSI-stack must be bypassed (ugly hack). This will lead to implementations which are difficult to secure the desired functionality and to verify. Another problem is that SAE J1699-3 cannot verify this requirement because it is very dependent upon how each manufacturer has implemented the reprogramming of ECUs.

One way to solve this is by using signaling between ECUs but there are ways to disable this, e.g. by pulling fuses to the ECUs which are not to be reprogrammed. Another way to bypass this requirement is to use enhanced diagnostics to set those ECU's in Programming Session where they operate in boot (no application), Clear DTCs in one ECU and then return to normal operation.

In addition, most of the OBD II functionality is located in one ECU and usually not distributed over multiple ECUs. The OBD II function may use information from other ECUs but that concerns CCM. Thus if one OBD II function is distributed over multiple ECUs, each of the ECU's should report the readiness information for that system. The tool can detect that the same system may be ready in one ECU but not in all. This has been discussed in SAE J1979. Therefore there are already mechanisms existing and implemented in the ECUs today to prevent I/M tampering.

The Volvo Group appreciates the opportunity to comment on this rule. Should ARB have any question or comments regarding Volvo Group recommendations, please direct them to Ray Istenes, Volvo Group Trucks. [Raymond.istenes@volvo.com, (301) 790-5528].

Best Regards,



Raymond R. Istenes, Jr.