C5 A Proposed Practice for the Correct Forensic Interrogation of Non-Volatile Memory Data in Evidentiary Vehicle Electronic Control Units

William Rosenbluth, MS, Automotive Systems Analysis, Inc., 12015 Canter Lane, Reston, VA 20191*

This presentation will impact the forensic community and/or humanity by discussing information on new forensic practices and procedures in a new and growing area of forensic technical investigation, electronic data recovery and documentation. It is important for the practicing forensic professional be familiar with proper procedures so that he or she can avoid pitfalls or errors that can jeopardize forensic findings and Court credibility, because existing practices and procedures often do not cover methods of electronic data recovery and documentation.

SYNOPSIS: This presentation discusses methods and considerations for the examination and interrogation of non-volatile memory data in evidentiary vehicle electronic control units (ECUs) that may have been involved in an event or incident that may be reasonably expected to be the subject of litigation. This practice is intended to become applicable when it is determined that examination or interpretation of such non-volatile memory data may produce probative evidence. These methods are being considered for a new *Practice for the Investigation of Non-Volatile Memory Data in Evidentiary Vehicle Electronic Control Units*, currently being considered by ASTM committee E30.05 on Forensic Engineering.

LEARNING OBJECTIVES: By observing the elements of this proposed protocol, the attendee will learn several methods for conducting an examination for the controlled interrogation of the data in a subject vehicle electronic control unit (ECU). Such data may be saved in ROM, EPROM, EEPROM[1] or flash-memory, all of which are non-volatile forms of memory. The retrieval of such data is commonly referred to as a download of information from the subject device[2].

A further objective of this proposed protocol is to retrieve any such data with the highest assurance of not changing or disturbing that data, either by erasure or overwriting. Such a download is referred to as a *forensically neutral*[3] download. A forensically neutral download can be accomplished with a load box/interface containing proper electrical loads and interfaces, or by using an exemplar vehicle for the same purpose. An example of a nonforensically neutral download is shown in Figure 1, and an example of a forensically neutral download is shown in Figure 2.

Figure 1

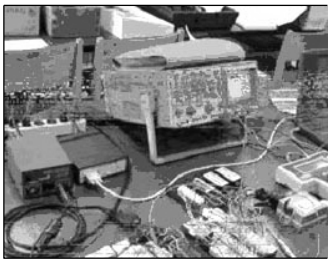

Figure 2

Certain commonly used commercial interrogating tools are not forensically neutral when used in a direct umbilical mode to interrogate SRS ECUs (i.e., a direct connection to the SRS ECU). In that mode, certain external fault codes will be added (or re-detected) because there is no provision for proper dummy-load resistors in the tool cabling. If the data of interest is not changed (e.g., crash data parameters), then a non-forensically-neutral interrogation may be acceptable. If certain fault codes are of interest, then a non-forensically-neutral interrogation may not be acceptable. If a potential DTC data change is not acceptable, other test equipment, laboratory breadboards and/or the use of an exemplar vehicle can avoid this problem. In general, it is expected that the test conductor will have a proper test fixture, and a proper exemplar component to demonstrate that his/her test bed is forensically neutral.

If the subject component is considered as evidence in litigation, and the manufacturer or supplier of the subject ECU is, or may be, a party to that litigation, it shall be considered standard practice to give the opportunity of first (qualified, non-destructive, non-intrusive, non-altering) download to the manufacturer or supplier of the ECU, with all adverse parties observing. This does not apply to exploratory interrogations or analyses of ECU components, which may be considered exemplar components.

THEORY OF THE ANALYSIS: Electronic data within any ECU is an encoded representation of information, constants and variables used to govern the function of an electronic control unit, as well as to

describe and document the version and level of such data. Such data are normally saved in a binary bit format. In order to create a concise representation of such data, it is usually represented by eight binary bit values, and these values are commonly represented as bytes of data, each byte having a specific memory address. Although most of the data referenced in this practice are saved in EEPROM, certain other data can be saved in ROM, EPROM or flash memory.

In general, the test conductor should perform two test series, with two devices under test (DUT). The first series should involve an exemplar device (to provide a baseline verification of the test fixture) and the second series should involve the subject ECU.

A. Power off test fixture (can include optional use of subject/exemplar vehicle as test fixture).
B. Select DUT.
C. Install DUT. DUT installation should include physical stability integrity if there is any chance that physical movement during the interrogation cycle will change the data within the DUT.
D. Power on test fixture with DUT installed. Observe MIL codes and other-indicator status. Visually record.
E. As appropriate, interrogate DUT with standard scan tool to observe scanner data (DTCs & PIDs). Save data as appropriate (photographically, computer data file, hardcopy, etc.)
F. Interrogate DUT with interrogation tool to download EEPROM and/or selected PID information (RAM, ROM, EAROM, EEPROM). Save data as appropriate (photographically, computer data file, hardcopy, etc.)
G. Re-interrogate with standard scan tool to record scanner data (DTCs & PIDs). Save data as appropriate (photographically, computer data file, hardcopy, etc.)
H. If no exceptions, power down and remove DUT.
I. Select next DUT as applicable and repeat steps 1-8. (For subject DUT, repeat EEPROM download procedure twice.)
J. End test operations.

[1] EEPROM = Electrically Erasable Programmable Read-Only Memory. EEPROM is made by using a special semiconductor construction that allows it to retain previously stored data even when the battery is disconnected. Flash-memory has similar characteristics to EEPROM, and that technology is also commonly used to save music or digital camera images in other commercial devices.

[2] Common usage identifies “download” as the process of interrogating an on-vehicle ECU and recording that data on an external diagnostic ECU (laptop computer), and that common usage is preserved herein. When requesting PID information that usage is reasonably applicable. However, strictly speaking, SAE J2190:4.23 identifies that the process of requesting the transfer of data from an on-vehicle ECU to an external ECU (Mode $35) is called an upload request, whereas the process of requesting the transfer of data from an external ECU to an on-vehicle ECU to an (Mode $34) is called an download request. Again, to avoid confusion, common usage is preserved herein.

[3] Not all electronic data interrogation processes are *forensically neutral*. A *forensically neutral* interrogation is one that will neither add or subtract error codes (DTCs) or crash data information from any ECU under interrogation. This applies to in-vehicle and bench top interrogation processes, including ECUs interrogated via direct umbilicals while still mounted in a vehicle. To be *forensically neutral*, such a unit must include provisions for actuator (squib, solenoid, etc.) dummy loads, sensor detection loads, MIL loads, serial feedback or for seatbelt switch status, so that any ECU undergoing such test-via-umbilical-interrogation will see only a correct operating environment during power-on and continuous loop checks.

Electronic Data Recorders, Forensic Neutrality, EDR Protocol

 ** Presenting Author*