



Immobilizer Module Manipulation Attack Test

1 Introduction

Note: Nothing in this standard supercedes applicable laws and regulations.

Note: In the event of conflict between the English and domestic language, the English language shall take precedence.

1.1 Purpose. To define the tests which will determine if a vehicle meets the requirements of:

- Canada Motor Vehicle Safety Standard (CMVSS) 114).
- CAN/ULC-S338-98 Standards Council of Canada (SCC) standard.
- ECE 97.01 Regulation, through supplement six (6).
- ECE R116.00 Regulation, through supplement four (4).

1.2 Applicability. This procedure applies to Canadian passenger cars manufactured on or after September 1, 2007. Also, it applies to United States (U.S.) trucks and multipurpose passenger vehicles having a Gross Vehicle Weight Rating (GVWR) of 4536 kg (10 000 lb) or less, manufactured on or after September 1, 1983. Also applies to European derivatives of this regulation.

1.3 Remarks.

1.3.1 Legal Requirements. The CMVSS 114 requirements are found in the GM Global Legal Database, as published by the GM North America Product Development (NAPD) Safety Regulations and Certification department. The GM Global Legal Database contains the most recent statement of CMVSS 114 requirements and supercedes those listed in any test procedure. Guidance for interpreting CMVSS 114 requirements may be obtained from the responsible GM Safety Regulations and Certification contact.

2 References

Note: Only the latest approved standards are applicable unless otherwise specified.

2.1 External Standards/Specifications.

CAN/ULC-S338-98 CMVSS 114 ECE 97.01 ECE R116.00

2.2 GM Standards/Specifications.

None

2.3 Additional References.

- GM Global Legal Database.

3 Resources

3.1 Facilities.

3.1.1 Calibration. The test facilities and equipment shall be in good working order and shall have a valid calibration label.

3.1.2 Alternatives. Alternative test facilities and equipment may also be used. However, all measuring variables as specified in this standard shall be determined correctly with respect to their physical definition.

3.1.3 Electrical bench test lab.

3.2 Equipment.

GM Confidential

© Copyright 2015 General Motors Company All Rights Reserved

May 2015

Page 1 of 9

3.2.1 Vehicle electrical bench and multimeter to measure voltage outputs when Electronic Control Module (ECM) output panel is available.

3.2.2 Scope or multimeter to measure fuel injector activation on bench.

3.2.3 Test tool to read serial communication data.

3.2.4 Strong magnets for test manipulation Method 1.

3.2.5 Stop watch.

3.2.6 Attack Test tools. The tools listed in 4.3.2 may be used in clause 12.16.1 of the CAN/ULC-S338-98.

3.3 Test Vehicle/Test Piece.

3.3.1 Test vehicles and/or system bench equipped with the latest updated Engine Control Module (ECM)/Body Control Module (BCM) modules and software.

3.4 Test Time.

Calendar time: 2 days

Test hours: 16 hours

Coordination hours: 4 hours

3.5 Test Required Information. The Immobilizer system is defined as comprising those modules that support substitution detection in the vehicle.

3.5.1 Instructions on how to equip electrical vehicle bench must be supplied by requesting engineer.

3.6 Personnel/Skills. No special training. Two people may be required for manipulation test Method 1.

4 Procedure

4.1 Preparation. Equip electrical vehicle bench per instruction of requesting engineer. Set bench to demonstrate normal operation, i.e., correct modules, software, etc.

4.2 Conditions.

4.2.1 Environmental Conditions. Not applicable.

4.2.2 Test Conditions. Deviations from the requirements of this standard shall have been agreed upon. Such requirements shall be specified on component drawings, test certificates, reports, etc.

4.3 Instructions. Module manipulation 2.5 minute bench test instructions.

Manipulation of the Immobilizer system modules that support substitution detection will be done through demonstration of four (4) attack procedures. Technician will have 2.5 minutes bench/5 minutes vehicle to start vehicle system.

Set bench for normal operation in "Park" for automatic transmission vehicles or with "Park Brake Active" for manual transmission vehicles. Verify bench is operating properly by observing display telltales or monitoring serial data messages with test tool. If a powertrain simulator is available, start the appropriate models. Remove any and all recognized keys from the effective range of the Immobilizer system and try to start vehicle with an alternate key by activation of ignition. Ensure Immobilizer system is working properly by demonstration of security telltales. Perform the four (4) procedures (see 4.3.1 Procedures) and record the test results on Data Sheet A1 in Appendix A.

4.3.1 Procedures.

4.3.1.1 Procedure 1. Activation of system outputs through the application of magnets.

Monitor starter motor outputs as well as fuel injection activation. Activation On output is when voltage needed to start starter goes high and when scope on fuel injection system shows a Pulse Width Modulation (PWM) signal or when appropriate indicator state goes active on simulator. This will be done at the Immobilizer system module.

Record name of module to be tested. Record the description of engine start output being activated and the description of fuel injection output being monitored on bench. Apply magnets to module for 2.5 minutes bench/5 minutes vehicle while trying to start system with alternate key in ignition, if applicable. Record whether outputs were activated.

GM Confidential

© Copyright 2015 General Motors Company All Rights Reserved

May 2015

Page 2 of 9

AVA Documents
Document Sharing Hub

4.3.1.2 Procedure 2. Assessment of system wiring mechanizations to identify any possible circuits which could be affected by shorts to battery or ground. Short Immobilizer outputs for engine start control. Test to comprehend applying battery or ground as identified in the assessment.

Record name of module to be tested and engine start output on bench being shorted to positive (+) and negative (-). Describe engine output and fuel injection output being monitored on bench. After shorting module output to first positive for 2.5 minutes bench/5 minutes vehicle, record output results. Then short module output to negative for 2.5 minutes bench/5 minutes vehicle and record output results on Data Sheet A1 in Appendix A.

4.3.1.3 Procedure 3. Attempt to put Immobilizer system module into abnormal or service state by disconnection/application of power or ground.

Record name of module to be tested and serial data output description from bench. If vehicle has multiple serial data systems or high-speed/low-speed systems, test all applicable communication systems. Record description of engine start and fuel injection output being monitored. Repeatedly short module serial data output to battery positive (+) for 2.5 minutes bench/5 minutes vehicle while trying to start ignition. Record results of engine output and fuel injection output. Repeat for 2.5 minutes bench/5 minutes vehicle shorting to ground, recording results on Data Sheet A1 in Appendix A.

4.3.1.4 Procedure 4. Pull fuses for Immobilizer system module individually and together while attempting to start vehicle.

Record name of module. Record description of engine start and fuel injection output from bench. For 2.5 minutes bench/5 minutes vehicle pull/apply module fuse while trying to start ignition. Record the results of engine start and fuel injection outputs on Data Sheet A1 in Appendix A. Pull/apply module fuses for Immobilizer modules for 2.5 minutes bench/5 minutes vehicle. Record the results of engine start and fuel injection outputs for Immobilizer system on Data Sheet A1 in Appendix A.

4.3.2 Attack Test Tools. The following listed tools may be used in clause 12.16.1 of the CAN/ULC-S338-98.

- Common hand tools (i.e., hammer, chisel, slide hammer, punch, wrench, screwdriver, and pliers).
- Steel rod/spike.
- Hacksaw.
- Portable battery drill, High Speed Steel (HSS) bits, maximum 13 mm diameter, and hole cutters.
- Portable battery angle grinder.
- Portable battery jigsaw.

In addition to the preceding list, special purpose tools are permissible. Tools are limited to what the attacker can carry on their person and in an average size tool bag, and can carry with one hand.

Note: Clause 12.16.1 permits the attack test to be performed either on the modules as installed on the vehicle or bench-tested outside the vehicle. GMW15372 utilizes the “bench-tested outside the vehicle” method for verification of this requirement; so only the reference to special purpose tools is applicable.

5 Data

5.1 Calculations. Not applicable.

5.2 Interpretation of Results. Not applicable.

5.3 Test Documentation. Record pertinent test results on the data sheets supplied in Appendix A.

6 Safety

This standard may involve hazardous materials, operations, and equipment. This standard does not propose to address all the safety problems associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.

7 Notes

7.1 Glossary.

Illegitimate Key: Key without transponder circuit but activates lock cylinder.

GM Confidential

© Copyright 2015 General Motors Company All Rights Reserved

May 2015

Page 3 of 9

AVA Documents
Document Sharing Hub