SAE The Engineering Society For Advancing Mobility Land Sea Air and Space®
INTERNATIONAL
400 Commonwealth Drive, Warrendale, PA 15096-0001

# SURFACE VEHICLE RECOMMENDED PRACTICE

Submitted for recognition as an American National Standard

SAE J2186

Issued 1991-09-16

## E/E DATA LINK SECURITY

### TABLE OF CONTENTS

1. Scope . . . . . 2
2. References . . . . . 2
2.1 Applicable Documents . . . . . 2
2.1.1 SAE Publications . . . . . 2
2.1.2 California Air Resources Board Regulations . . . . . 2
2.2 Related Publications . . . . . 2
2.2.1 SAE Publications . . . . . 2
2.2.2 ISO Publications . . . . . 2
3. Definitions . . . . . 2
4. Technical Requirements . . . . . 3
4.1 Data Link Security Strategy . . . . . 3
4.2 Data Link Access Function Examples . . . . . 3
4.2.1 Unsecured Read Data . . . . . 3
4.2.2 Unsecured Service Alteration . . . . . 3
4.2.3 Unsecured Permanent Alteration . . . . . 4
4.2.4 Secured Read Data . . . . . 4
4.2.5 Secured Service Alteration . . . . . 4
4.2.6 Secured Permanent Alteration . . . . . 4
4.3 Characteristics of Security . . . . . 4
4.4 Functional Requirements . . . . . 4

*1. Scope*—This SAE Recommended Practice establishes a uniform practice for protecting vehicle modules from "unauthorized" intrusion through a vehicle diagnostic data communication link. The security system represents a recommendation for motor vehicle manufacturers and provides flexibility for them to tailor their system to their specific needs. The vehicle modules addressed are those that are capable of having solid-state memory contents altered external to the electronic module through a diagnostic data communication link. Improper memory content alteration could potentially damage the electronics or other vehicle modules; risk the vehicle compliance to government legislated requirements; or risk the vehicle manufacturer's security interests. This document is intended to meet the "tampering protection" provisions of California Air Resources Board OBD II regulations and does not imply that other security measures are not required nor possible.

*2. References*

**2.1 Applicable Documents**—The following publications form a part of this specification to the extent specified herein. The latest issue of SAE publications shall apply.

2.1.1 SAE PUBLICATIONS—Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

J1978 MAR92 OBD II Scan Tool

2.1.2 CALIFORNIA AIR RESOURCES BOARD REGULATIONS—Available from Air Resources Board, Mobile Source Division, 9528 Telstar Avenue, El Monte, CA 91731.

Mail out #91-18 (OBD II)—Title 13, California Code of Regulations, Section 1968.1 Malfunction and Diagnostic System Requirements—1994 and Subsequent Model Year, Passenger Cars, Light Duty Trucks, and Medium-Duty vehicles with Feedback Fuel Control Systems.

**2.2 Related Publications**—The following publications are provided for information purposes only and are not a required part of this document.

2.2.1 SAE PUBLICATIONS—Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

J1850 AUG91—Class B Data Communication Network Interface

J1930 SEP91—Terms, Definitions, Abbreviations and Acronyms

J1979 DEC91—E/E Diagnostic Test Modes

2.2.1.1 The following publications are under development:

J1962 Draft Diagnostic Connector

J2012 Draft Format and Messages for Diagnostic Trouble Codes

J2190 Draft Enhanced E/E Diagnostic Test Modes

J2201 Draft Universal Interface for OBD II Scan Tool

J2205 Draft Expanded Diagnostic Protocol for OBD II Scan Tool

2.2.2 ISO PUBLICATIONS—Available from ANSI, 11 West 42nd Street, New York, NY 10036.

ISO/CD 9141-1 Road vehicles—Diagnostic systems—CARB requirements for April 1991 interchange of digital information.

*3. Definitions*

STANDARD SERVICE TOOL—A service tool providing basic emission related power train diagnostic tool functions, as required by CARB OBD II regulations. This service tool complies with SAE J1978 and is not necessarily limited to only OBD II functions.

ENHANCED SERVICE TOOL—A service tool providing expanded emission related power train diagnostic functions in excess of the standard service tool and/or non-power train systems diagnostic tool functions.

SECURED SERVICE TOOL—A service tool containing a feature for accessing secured data link functions. Use of this feature is limited by the vehicle manufacturer.

UNSECURED FUNCTIONS—Standard diagnostic functions that are provided by vehicle manufacturers. These are controlled and protected by the on-vehicle controller. The unsecured capability includes reprogramming of selected items for which the reprogrammer is liable.

SECURED FUNCTIONS—Manufacturer restricted functions that require "Unlocking" the on-vehicle controller to gain access. Typical functions include programming of vehicle emission systems.

READ DATA FUNCTION—Operation which reads parameters and codes via the data link.

SERVICE ALTERATION FUNCTION—Operation which temporarily alters the vehicle control system for the purpose of diagnosing the system's operation.

PERMANENT ALTERATION FUNCTION—Operation which permanently alters the operating characteristics of a vehicle module or system.

SEED—The data value sent from the on-board controller to the secured service tool.

KEY—The data value sent from the secured service tool to the on-board controller.

4. ***Technical Requirements***—Proper "Unlocking" of the controller shall be a prerequisite to access certain critical on-board controller functions; the only access to the on-board controller permitted while in a "Locked" mode is through the product-specific software. This permits the product-specific software to protect itself and the rest of the vehicle control system from unauthorized intrusion.

This document does not attempt to define capability or information that is under security; this is left to the vehicle manufacturer. The security system shall not prevent basic diagnostic communications between the external tool and the on-board controller.

**4.1 Data Link Security Strategy**—As shown in Table 1, the data link access of function is divided into two classifications: Unsecured and Secured. Each of these functions are subclassified as: Read Data, Service Alteration, and Permanent Alteration. These classifications are allocated to three types of service tools: Standard Tools, Enhanced Tools, and Secured Tools. The allocation of access classification by service tool type should provide for normal service capability of the vehicle and protect the vehicle from "unauthorized" intrusion of certain critical functions.

**TABLE 1—SECURITY AUTHORITY ACCESS DATA LINK ACCESS FUNCTION (REFER TO SECTION 4.2)**

| Service Tool Type | Unsecured Read Data (4.2.1) | Unsecured Service Alteration (4.2.2) | Unsecured Permanent Alteration (4.2.3) | Secured Read Data (4.2.4) | Secured Service Alteration (4.2.5) | Secured Permanent Alteration (4.2.6) |
|---|---|---|---|---|---|---|
| Standard (SAE J1978) | X | B | B | NA | NA | NA |
| Enhanced | X | E | E | NA | NA | NA |
| Secured | X | X | X | X | X | X |

X —Function Allowed
NA —Not Allowed
B —Basic Diagnostic Capability Per Vehicle Manufacturer's Specification
E —Enhanced Diagnostic Capability

**4.2 Data Link Access Function Examples**

4.2.1 UNSECURED READ DATA

Read emission related data.

Read emission related trouble codes.

4.2.2 UNSECURED SERVICE ALTERATION

Cycle device on/off.

Substitute sensor value.

4.2.3 UNSECURED PERMANENT ALTERATION

Change vehicle option/configuration data (i.e., tire size).

Reset electronic module.

4.2.4 SECURED READ DATA

Read keyless entry parameters.

Read executable code.

4.2.5 SECURED SERVICE ALTERATION

Vehicle assembly plant verification tests involving parameters not normally used in service.

4.2.6 SECURED PERMANENT ALTERATION

Alteration of a vehicle emission calibration.

Alteration of executable code.

**4.3 Characteristics of Security**—A special communications mode shall be provided to "Unlock" the on-board controllers which have secured or restricted functions. The security system is intended to make the emission related controller more immune to:

a. Unauthorized intrusion into the controller without full control of the product specific software.
b. Unauthorized alteration of the on-board control system or control parameters.

Disclosure of the "Seed/Key" relationship shall be limited to those persons, authorized by the vehicle manufacturer, who are responsible for the production of the secured service tool. The security system shall not prevent basic diagnostic or vehicle communications between external devices and the on-board controller.

There shall be three parameters which control the security access of the on-board controller:

a. The "Seed" and "Key" shall each be a minimum of 2 bytes in length. The relationship between the "Seed" and "Key" is the responsibility of the vehicle manufacturer. Multiple "Seed/Key" relationships may exist for access to different functions within a controller or systems within a vehicle.
b. The Delay Time (DT) shall be a minimum of 10 seconds; the vehicle manufacturer may specify an increased delay time to suit its specific requirements.
c. The Number of False Access Attempts (NFAA) shall be a maximum of two; the vehicle manufacturer may specify a reduced number of false attempts to suit its specific requirements. When the "Key" received by the controller is not correct, it shall be considered as a false access attempt; if access is rejected for any other reason, it shall not be considered a false access attempt.

**4.4 Functional Requirements**—Two request/response communication message pairs (Request #1/Response #1, Request #2/Response #2) shall be used to "Unlock" the on-board controller. The specific message content is not specified by this document and is the responsibility of the vehicle manufacturer.

a. Step 1—The external device shall request the on-board controller to "Unlock" itself by sending Request #1. The controller shall respond by sending a "Seed" using Response #1. A seed value of zero shall indicate that the controller is currently unlocked.
b. Step 2—The external device shall respond by returning a "Key" number back to the controller using Request #2. The controller shall compare this "Key" to one internally determined and issue Response #2.

If the two numbers agree, then the controller shall enable ("Unlock") the external device's access to secured communication modes.

If, upon "NFAA" attempts, the two keys do not compare (false attempt), then the controller shall insert the DT before allowing further attempts. The DT shall also be required at each controller power-on.

Three on-board controller responses shall be decoded by the external device:

a. Accept—The controller has "Unlocked" its access.
b. Invalid Key—The access attempt was rejected because the key was determined to be invalid by the controller; the access attempt was false.
c. Process Error—The access attempt was rejected for reasons other than receiving the wrong key; this shall not be counted as a false access attempt.

Termination of security access, "Locking" the product, shall result after any of the following conditions:

a. Each time the product is "powered up."
b. Upon commanding the product to a normal operational mode.
c. Conditions at the vehicle manufacturers discretion.

If an attempt is made to communicate with a "Locked" on-board controller and access a "Secured" function, the controller may return a special response indicating that the controller is "Locked" and cannot respond as requested.



PREPARED BY THE SAE VEHICLE E/E SYSTEMS DIAGNOSTICS STANDARDS COMMITTEE

**Rationale**—Not applicable.

**Relationship of SAE Standard to ISO Standard**—Not applicable.

**Application**—This document establishes a uniform practice for protecting vehicle modules from "unauthorized" intrusion through a vehicle diagnostic data communication link. The security system represents a recommendation for motor vehicle manufacturers and provides flexibility for them to tailor their system to their specific needs. The vehicle modules addressed are those that are capable of having solid-state memory contents altered external to the electronic module through a diagnostic data communication link. Improper memory content alteration could potentially damage the electronics or other vehicle modules; risk the vehicle compliance to government legislated requirements; or risk the vehicle manufacturer's security interests. This document is intended to meet the "tampering protection" provisions of California Air Resources Board OBD II regulations and does not imply that other security measures are not required nor possible.

**Reference Section**

J1850 AUG91—Class B Data Communication Network Interface
J1930 SEP91—Terms, Definitions, Abbreviations and Acronyms
J1962 Draft—Diagnostic Connector
J1978 MAR92—OBD II Scan Tool
J1979 DEC91—E/E Diagnostic Test Modes
J2012 Draft—Format and Messages for Diagnostic Trouble Codes
J2190 Draft—Enhanced E/E Diagnostic Test Modes
J2201 Draft—Universal Interface for OBK II Scan Tool
J2205 Draft—Expanded Diagnostic Protocol for OBD II Scan Tool

**Committee Composition**

**Developed by the SAE Vehicle E/E Systems Diagnostics Standards Committee**

R. R. Smisek, General Motors Corporation, Romulus, MI—Chairman
L. S. Tedesco, Ford Motor Company, Dearborn, MI—Vice Chairman
J. R. Boldt, Chrysler Motors Corporation, Highland Park, MI—Secretary
J. M. Allderige, Zeller Corporation, Defiance, OH
E. Alon, Computer Aided Service Inc., San Jose, CA
T. L. Andrix, SPX Corporation, Farmington Hills, MI
R. Barker, Chrysler Motors Corporation, Center Line, MI
C. J. Booms, Chrysler Corporation, Highland Park, MI
J. M. Bordato, SPX Corporation, Farmington Hills, MI
T. Braun, General Motors Corporation, Kokomo, IN
R. C. Breitzman, Ford Motor Company, Dearborn, MI
G. J. Broniak, Chrysler Motors Corporation, Center Line, MI
J. A. Brouse, Cuyahoga Community College, Parma, OH
M. J. Buchanan, ITT Cannon, Auburn Hills, MI
J. M. Burke, American Honda Motor Company Inc., Torrance, CA
T. R. Calkins, Vetronix Corporation, Santa Barbara, CA
J. L. Camp, Cirmount Circuits Inc., Farmington Hills, MI

**Developed by the SAE Vehicle E/E Systems Diagnostics Standards Committee (Continued)**

J. A. Chaney, Chrysler Motors Corporation, Center Line, MI
B. E. Chapman, AMP Inc., Harrisburg, PA
W. B. Clemmens, Environmental Protection Agency, Ann Arbor, MI
R. J. Colvin, Allen Group Inc., Kalamazoo, MI
M. C. Cwiek, Chrysler Motors Corporation, Auburn Hills, MI
M. Dinn, Chrysler Motors Corporation, Center Line, MI
R. E. Donnelson, Mitsubishi Motor Sales of America Inc., Fountain Valley, CA
J. Eichhorn, General Motors Corporation, Flint, MI
G. P. Esmer, Alps Electric (USA) Inc., Auburn Hills, MI
B. C. Fodor, Nissan, Gardena, CA
Y. Fujii, Nippondenso Technical Center USA Inc., Southfield, MI
G. G. Giek, American Automobile Association, Heathrow, FL
L. W. Gilpin, Ford Motor Company, Dearborn, MI
G. M. Gianert, Chrysler Motors Corporation, Center Line, MI
R. L. Gonzales, Purdue University, Hammond, IN
S. K. Hansen, Brunswick Corporation, Fond du Lac, WI
T. M. Hanson, General Motors Corporation, Romulus, MI
K. Hellgren, Volvo Car Corporation, Gothenburg, Sweden
M. Hesse, Chrysler Motors Corporation, Center Line, MI
J. B. Heyler, Jr., Los Angeles, CA
A. R. Hinkle, Brighton, MI
P. S. Hlavinka, SPX Corporation, Owatonna, MN
R. J. Hooper, RDT Services Inc., Houston, TX
D. P. Hostetler, Computer Aided Services, San Jose, CA
W. L. Kampmann II, Ypsilanti, MI
D. A. Kasper, Chrysler Motors Corporation, Center Line, MI
P. Kenyon, Chrysler Motors Corporation, Warren, MI
S. A. Kidder, Automotive Information Systems, St. Paul, MN
P. King, King's Garage (ASC), Farmington, MI
A. Kishore, Nissan Motor Company, Ann Arbor, MI
D. L. Koch, Chrysler Motors Corporation, Auburn Hills, MI
J. M. Kotzan, General Motors Corporation, Milford, MI
M. Kristofik, Chrysler Motors Corporation, Center Line, MI
D. R. LaRue, Ford Motor Company, Dearborn, MI
G. Lancaster, Jaguar Cars Ltd., Coventry W. Mids, England
A. Leese, ATI, Redford, MI
J. J. Luyckx, SPX Corporation, Warren, MI
T. M. Lyden, SPX Corporation, Owatonna, MN