SAE International™

SURFACE VEHICLE RECOMMENDED PRACTICE

SAE J2186

REAF. JUN2005

Issued 1991-09
Reaffirmed 2005-06

Superseding J2186 OCT1996

E/E Data Link Security

TABLE OF CONTENTS

1. ***Scope***—This SAE Recommended Practice establishes a uniform practice for protecting vehicle components from "unauthorized" access through a vehicle data link connector (DLC). The document defines a security system for motor vehicle and tool manufacturers. It will provide flexibility to tailor systems to the security needs of the vehicle manufacturer. The vehicle modules addressed are those that are capable of having solid state memory contents accessed or altered through the data link connector. 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 does not imply that other security measures are not required nor possible.

1.1 **Rationale**—This document has been reaffirmed to comply with the SAE 5-Year Review policy.

2. ***References***

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

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

SAE J2190—Enhanced E/E Diagnostic Test Modes

TO PLACE A DOCUMENT ORDER:
Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: custsvc@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE 100 Leading Our World In Motion

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.

SAE J1850—Class B Data Communication Network Interface
SAE J1930—Terms, Definitions, Abbreviations, and Acronyms

2.2.2 ISO PUBLICATIONS—Available from ANSI, 25 West 43rd Street, New York, NY 10036-8002.

ISO 9141-2—Road vehicles—Diagnostic systems—CARB requirements for interchange of digital information
ISO/DIS 14230—Road vehicles—Diagnostic systems—Keyword protocol 2000

3. Definitions

3.1 Unsecured Functions—Standard diagnostic functions that are provided by vehicle manufacturers such as read data parameters, diagnostic trouble codes, etc. These are controlled and protected by the on-vehicle controller. The unsecured capability may include reprogramming of selected items for which the reprogrammer is liable.

3.2 Secured Functions—Functions that require "Unlocking" the on-vehicle controller to gain access. Typical functions include programming of vehicle emission systems, vehicle theft, and odometer.

3.3 Seed—The data value sent from the on-board controller to the access tool.

3.4 Key—The data value sent from the access tool to the on-board controller.

***4. Technical Requirements*—**Provide a method to access secured vehicle controller functions. Provide a protection method for the seed/key algorithms in the access tool. "Unlocking" of the controller shall be a prerequisite to access secured on-board controller functions. This permits the product software to protect itself and the rest of the vehicle control system from unauthorized access. Different on-board functions may be protected by separate seed/key relationships.

This document does not attempt to define capability or information that is secured. The security system shall not prevent access to unsecured functions between the external device and the on-board controller.

4.1 Characteristics of Security—This security technique can be incorporated in any communications protocol. Special commands shall be provided via the DCL to "Unlock" the on-board controller secured functions.

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

a. The "Seed" and "Key" shall each be a minimum of 2 bytes in length. Selection of the minimum number of bytes will result in a minimum security level. Use of 4 or more bytes are suggested when higher levels of security are required.
   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. As an example, refer to SAE J2190 mode $27.
b. The Delay Time (DT) shall be a minimum of 10 s. The vehicle manufacturer may specify an increased delay time to suit its specific requirements.