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

SURFACE VEHICLE RECOMMENDED PRACTICE

SAE J2186 | REV. OCT96

Issued 1991-09
Revised 1996-10

Superseding J2186 SEP91

Submitted for recognition as an American National Standard

(R) 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.

2. References

2.1 Applicable Document—The following publication forms 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.

QUESTIONS REGARDING THIS DOCUMENT: (412) 772-8512 FAX: (412) 776-0243
TO PLACE A DOCUMENT ORDER: (412) 776-4970 FAX: (412) 776-0790

SAE J2190—Enhanced E/E Diagnostic Test Modes

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 DOCUMENTS—Available from ANSI, 11 West 42nd 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.

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.

Disclosure of the "Seed/Key" relationship shall be limited to those persons as authorized by the vehicle manufacturer.

CAUTION—Care should be taken when selecting the values of all the parameters since their combination determines the robustness of the security for an application or a system.

4.2 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 a “seed” from the on-board controller 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 and the tool shall insert the "DT" time delay before allowing further attempts. The "DT" time delay shall also be required at each controller and tool power-on.

The tool shall automatically insert the delay time (DT) prior to requesting a new seed for any reason.

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 controller 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.

5. Notes

5.1 Marginal Indicia—The (R) is for the convenience of the user in locating areas where technical changes have been made to the previous issue of the report. If the symbol is next to the report title, it indicates a complete revision of the report.

PREPARED BY THE SAE VEHICLE E/E DIAGNOSTICS STANDARDS COMMITTEE

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

SURFACE VEHICLE RECOMMENDED PRACTICE

SAE J2186 | REV. OCT96

Issued 1991-09
Revised 1996-10

Superseding J2186 SEP91

Submitted for recognition as an American National Standard

(R) 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.

2. References

2.1 Applicable Document—The following publication forms 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.

QUESTIONS REGARDING THIS DOCUMENT: (412) 772-8512 FAX: (412) 776-0243
TO PLACE A DOCUMENT ORDER: (412) 776-4970 FAX: (412) 776-0790

SAE J2190—Enhanced E/E Diagnostic Test Modes

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 DOCUMENTS—Available from ANSI, 11 West 42nd 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.

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.

Disclosure of the "Seed/Key" relationship shall be limited to those persons as authorized by the vehicle manufacturer.

CAUTION—Care should be taken when selecting the values of all the parameters since their combination determines the robustness of the security for an application or a system.

4.2 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 a “seed” from the on-board controller 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 and the tool shall insert the "DT" time delay before allowing further attempts. The "DT" time delay shall also be required at each controller and tool power-on.

The tool shall automatically insert the delay time (DT) prior to requesting a new seed for any reason.

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 controller 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.

5. Notes

5.1 Marginal Indicia—The (R) is for the convenience of the user in locating areas where technical changes have been made to the previous issue of the report. If the symbol is next to the report title, it indicates a complete revision of the report.

PREPARED BY THE SAE VEHICLE E/E DIAGNOSTICS STANDARDS COMMITTEE