INTERNATIONAL STANDARD

ISO 15031-7

First edition
2001-03-15

Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics —

Part 7: Data link security

Véhicules routiers — Communications entre un véhicule et un équipement externe pour le diagnostic relatif aux émissions —

Partie 7: Sécurité de la liaison de données

Reference number
ISO 15031-7:2001(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO 15031 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 15031-7 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 15031 consists of the following parts, under the general title *Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics*:

— *Part 1: General information*

— *Part 2: Terms, definitions, abbreviations and acronyms*

— *Part 3: Diagnostic connector and related electrical circuits, specification and use*

— *Part 4: External test equipment*

— *Part 5: Emissions-related diagnostic services*

— *Part 6: Diagnostic trouble code definitions*

— *Part 7: Data link security*

Introduction

The various parts of ISO 15031, when taken together, provide a coherent, self-consistent set of specifications for facilitating emissions-related diagnostics. Parts 2 through 7 of ISO 15031 are based on recommended practices of the society of automotive engineers (SAE). This part of ISO 15031 is based on SAE J2186:1996, *E/E Data Link Security*.

Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics —

Part 7: Data link security

1 Scope

This part of ISO 15031 gives guidelines for the protection of road vehicle modules from unauthorized intrusion through a vehicle diagnostic data link. These security measures offer vehicle manufacturers the flexibility to tailor their security to their own specific needs, and do not exclude other, additional measures.

This part of ISO 15031 applies to vehicle modules whose solid-state memory contents are able to be altered from outside the electronic module through a diagnostic data communication link. Such alteration could potentially damage a vehicle's electronics or other components, placing at risk its compliance with government legislation or the vehicle manufacturer's interests in respect of security.

2 Normative reference

The following normative document contains provisions which, through reference in this text, constitute provisions of this part of ISO 15031. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 15031 are encouraged to investigate the possibility of applying the most recent edition of the normative document indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/TR 15031-2:—[1)], *Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 2: Terms, definitions, abbreviations and acronyms.*

3 Terms and definitions

For the purposes of this part of ISO 15031, the terms and definitions given in ISO/TR 15031-2 and the following apply.

3.1
unsecured functions
standard diagnostic functions provided by the vehicle manufacturer and controlled and protected by the on-board controller

EXAMPLE Reprogramming of selected items such as the clearing of fault codes.

1) To be published.

3.2
secured functions
restricted functions whose access requires unlocking the on-board controller

EXAMPLE Programming of vehicle emission systems such as fuel/ignition maps, anti-theft systems and odometer.

3.3
seed
pseudo-random data value sent from the on-board controller to the external test equipment and processed by the security algorithm to produce the key

3.4
key
data value giving access to the secured functions sent from the external test equipment to the on-board controller in response to the seed

3.5
false access attempt
FAA
incorrect key received by the on-board controller

3.6
delay time
DT
time period inserted between access attempts

4 Technical requirements

4.1 General

The unlocking of the on-board controller shall be a prerequisite for accessing certain critical on-board control functions.

NOTE This part of ISO 15031 does not specify the functions or information to be secured, leaving this to the vehicle manufacturer.

The only access permitted the on-board controller when a function is locked shall be through the product-specific software, thus permitting the software to protect itself and the rest of the vehicle control system from unauthorized intrusion. Different on-board functions may be protected by separate seed–key combinations.

The security measures shall not prevent normal diagnostic communications between the external device and the on-board controller.

4.2 Security characteristics

These security measures may be incorporated in any communications protocol. Special commands shall be provided via the diagnostics communication link for unlocking the on-board controller.

The following three parameters shall determine security access to the on-board controller and the secured function.

a) The seed and key shall each be a minimum of two bytes in length, the selection of a minimum number of bytes providing a minimum security level. Four or more bytes should be used when higher levels of security are required. The relationship between seed and key shall be the responsibility of the vehicle manufacturer. Multiple seed–key relationships may exist for accessing different controller functions or systems in a vehicle.

b) There shall be a maximum number of two false access attempts (FAA) before the delay time (DT) is inserted; the vehicle manufacturer may specify a reduced number of FAAs to suit specific requirements. When the key

received by the controller is incorrect, it shall be considered as an FAA, but if access is denied for any other reason, it shall not be considered as such.

c) The DT shall be a minimum of 10 s; the vehicle manufacturer may specify a longer DT to suit specific requirements, including a DT that increases with the number of FAAs.

Disclosure of the seed–key relationship shall be limited to persons authorized by the vehicle manufacturer.

CAUTION — Care should be taken when selecting the value of each of the parameters since their combination determines the robustness of the overall security of an application or a system.

4.3 Functional requirements

Two request/response communication message pairs shall be used to unlock the secured function.

NOTE This part of ISO 15031 does not specify message content, leaving this to the vehicle manufacturer.

— **Request 1/Response 1.** The external device shall request the on-board controller to unlock the desired secured function 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.

— **Request 2/Response 2.** The external device shall respond by returning a key number 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, the controller shall enable (unlock) the external device's access to the secured function. If the allowed number of FAAs is reached without the key numbers matching (false attempt), the controller shall insert the DT before allowing any further attempts.

The DT shall also be inserted at each controller and function power-up.

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

The following three on-board controller responses shall be decoded by the external device.

a) Accept: the controller has unlocked and enabled 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 (FAA).

c) Process error: the access attempt was rejected for reasons other than receipt of the wrong key; this shall not be counted as an FAA.

Termination of security access and locking of the secured function shall result under any of the following conditions:

— each time the controller is powered up;

— upon a command to go to a normal operational mode;

— other conditions at the vehicle manufacturer's discretion.

If an attempt is made to communicate with a locked on-board controller in order to access a secured function, the controller may return a special response indicating that it is locked and cannot respond as requested.

ICS 13.040.50; 43.040.10

Price based on 3 pages