INTERNATIONAL STANDARD

ISO 16844-5

First edition
2004-08-01

Road vehicles — Tachograph systems —

Part 5: Secured CAN interface

Véhicules routiers — Systèmes tachygraphes —

Partie 5: Interface CAN sauvegardée

Reference number
ISO 16844-5:2004(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.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 2.

The main task of technical committees is to prepare International Standards. 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 document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16844-5 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 16844 consists of the following parts, under the general title *Road vehicles — Tachograph systems*:

— *Part 1: Electrical connectors*

— *Part 2: Recording unit, electrical interface*

— *Part 3: Motion sensor interface*

— *Part 4: CAN interface*

— *Part 5: Secured CAN interface*

— *Part 6: Diagnostics*

— *Part 7: Parameters*

Introduction

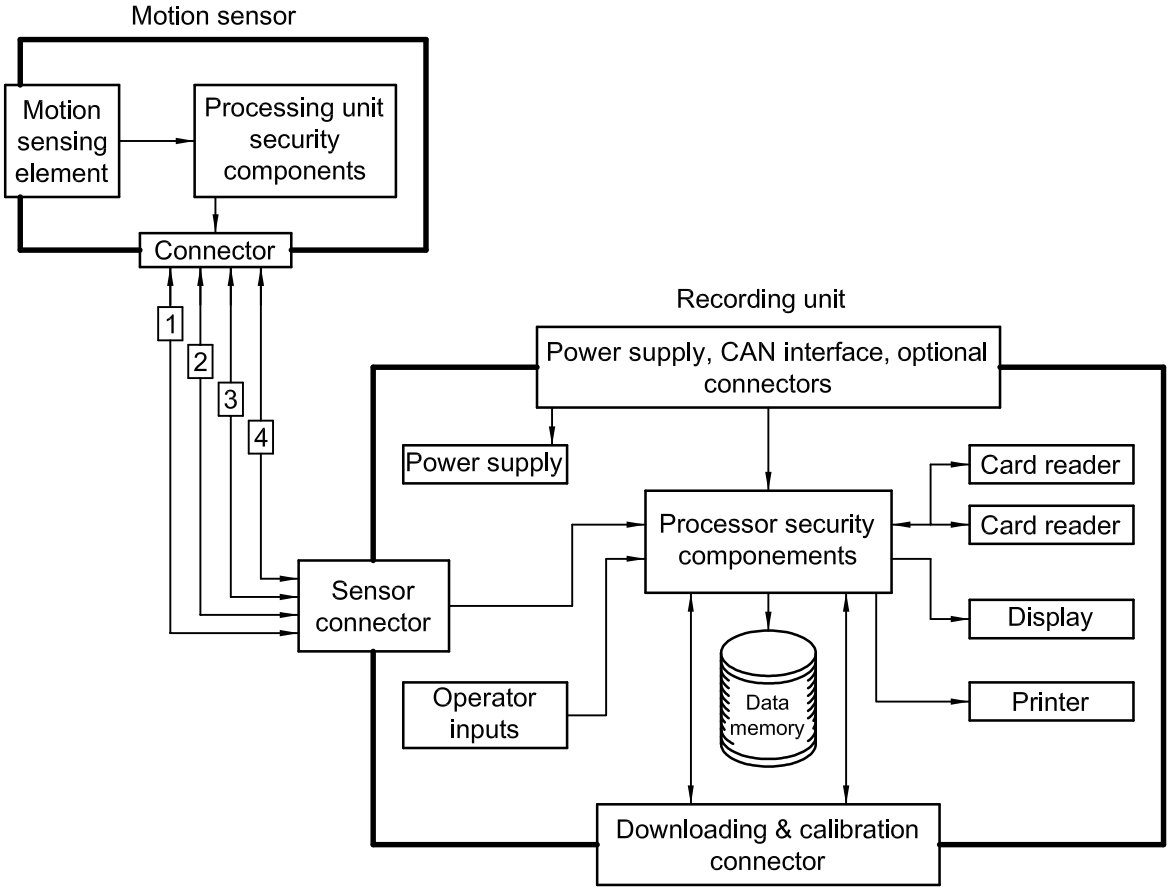
ISO 16844 supports and facilitates the communication between electronic units and a tachograph; the tachograph being based upon Council Regulations (EEC) No. 3820/85 [1] and (EEC) No. 3821/85 [2] and their amendments Council Regulation (EEC) No. 2135/98 [3] and Commission Regulation (EC) No. 1360/2002 (see Clause 2).

Its purpose is to ensure the compatibility of tachographs from various tachograph manufacturers.

The basis of the digital tachograph concept is a recording unit (RU) that stores data related to the activities of the drivers of a vehicle on which it is installed. When the RU is in normal operational status, the data stored in its memory are made accessible to various entities such as drivers, authorities, workshops and transport companies in a variety of ways: they may be displayed on a screen, printed by a printing device or downloaded to an external device. Access to stored data is controlled by a smart card inserted in the tachograph.

In order to prevent manipulation of the tachograph system, the speed signal sender (motion sensor) is provided with an encrypted data link.

A typical tachograph system is shown in Figure 1.



Key

1 positive supply
2 battery minus
3 speed signal, real time
4 data signal in/out

Figure 1 — Typical tachograph system

Road vehicles — Tachograph systems —

Part 5:
Secured CAN interface

1 Scope

This part of ISO 16844 specifies the secured interchange of digital information between a road vehicle's tachograph system and vehicle units, and within the tachograph system itself. This type of interchange will be used for CAN communication or diagnostic services on CAN (controller area network), where there is need to protect interchanged parameters against fraud.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14229-1, *Road vehicles — Unified diagnostic services (UDS) — Part 1: Specification and requirements* [1)]

ISO 15764, *Road vehicles — Extended data link security*

ISO 15765-2, *Road vehicles — Diagnostics on Controller Area Networks (CAN) — Part 2: Network layer services*

ISO 16844-4, *Road vehicles — Tachograph systems — Part 4: CAN interface* [1)]

ISO 16844-6:2004, *Road vehicles — Tachograph systems — Part 6: Diagnostics*

ISO 16844-7, *Road vehicles — Tachograph systems — Part 7: Parameters*

Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 15764 and the following apply.

3.1
recording unit
part of the tachograph system that acquires and stores data concerning the vehicle and its driver(s) and their activities

1) To be published.

4 Abbreviated terms

EC	European Commission
EEC	European Economic Community
hex	hexadecimal number
ID	identifier
PDU	protocol data unit
PGN	parameter group number
RU	recording unit
VIN	vehicle identification number
VU	vehicle unit

5 Physical layer

The physical layer shall be implemented according to ISO 16844-4.

6 Data link layer

The data link layer shall be implemented according to ISO 16844-4.

7 Network layer

The network layer shall be implemented according to ISO 15765-2, together with the additional requirements given in ISO 16844-6:2004, 7.1.

8 Application layer

The SecuredDataTransmission (hex 84) service according to ISO 14229-1 shall be used.

9 Security sub-layer

9.1 General

The security sub-layer is inserted between the application layer and the application, as described in ISO 14229-1.

It shall be implemented according to ISO 15764, based on the settings according to ISO 14229-1, giving additional tachograph requirements.

The RU shall act as the server according to ISO 15764.

9.2 Security sub-layer service request parameters

9.2.1 Server identifier

The server identifier shall be the unique identifier of the RU. If the identifier is less than 8 bytes, it will be padded with hex FF.

For a tachograph designed in accordance with Council Regulations (EEC) No. 3820/85 [1] and No. 3821/85 [2], last amended by Council Regulation (EC) 1360/2002, the identifier shall be the 8 byte key identifier of the VU in accordance with Council Regulation (EC) 1360/2002, Annex 1B Appendix 11, Section 3.3.1.

9.2.2 Secured mode service type

The RU will only accept the secured mode service types according to Table 1. In all other cases it will send a negative response with error code hex 31 (requestOutOfRange).

Table 1 — Supported secured mode service types

securedModeServiceType value	Service type
1	Diagnostic service according to ISO 14229-1
3	Tachograph service according to ISO 16844-4 and ISO 16844-7

In case of securedModeServiceType 1 the settings of ISO 16844-6 apply for the diagnostic service to be executed in the secured mode.

In case of securedModeServiceType 3 the security sub-layer of the RU shall accept a request PGN also for information that is broadcast periodically (see ISO 16844-4), and on reception of a request PGN shall respond without verifying the certificate of the client (see ISO 15764).

NOTE The client will send the request in the secured mode to get an authenticated response from the RU. As the messages are available for any client in non-secured mode as well, neither authentication of the client towards the RU nor protection against eavesdropping is needed.

9.2.3 Secured mode service identifier

In the case of securedModeServiceType 1, the securedModeServiceIdentifier shall be the 1 byte service identifier (see ISO 14229-1) for the service request of the diagnostic service to be executed in the secured mode.

In the case of securedModeServiceType 3, the securedModeServiceIdentifier shall be the PDU format field of the PGN (see ISO 16844-4) of the message to be sent in the secured mode. The RU will only accept values of the PDU format field between 0 and 239 (PDU 1 format). In all other cases, it will send a negative response with error code hex 31 (requestOutOfRange).

NOTE It is not possible to send the Electronic Engine Controller #1 message to the RU in the secured mode.

9.2.4 Security profile

The RU shall only accept security profiles containing the value 0 in the bit number 13 (meaning that the response has to include no user ID). If this bit is set to 1, the RU shall send a negative response with error code hex 40 (auditTrailInformationNotAvailable, see ISO 15764).

9.2.5 Audit trail information

If the audit trail information of the service request contains the VIN, the RU shall verify it and send a negative response with error code hex 31 (requestOutOfRange), in case it doesn't fit with the VIN stored in the RU.

No other audit trail information contained in the service request shall be verified by the RU.

9.3 Security sub-layer service response parameters

In the case of securedModeServiceType 1 in the corresponding service indication, the securedModeServiceIdentifier shall be the 1-byte service identifier (see ISO 14229-1) for the service response of the diagnostic service to be executed in the secured mode.

In the case of securedModeServiceType 3 in the corresponding service indication, the securedModeServiceIdentifier shall be the PDU specific field of the PGN (see ISO 16844-4) of the message to be sent in the secured mode. If no specific response message was requested, the RU will send the acknowledge message in response to the request message.

Bibliography

[1] Council Regulation (EEC) No. 3820/85 of 20 December 1985 on the harmonization of certain social legislation relating to road transport

[2] Council Regulation (EEC) No. 3821/85 of 20 December 1985 on recording equipment in road transport

[3] Council Regulation (EEC) No. 2135/98 of 24 September 1998 amending Regulation (EEC) No. 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Council Regulations (EEC) No. 3820/85 and (EEC) No. 3821/85

ICS 43.040.10

Price based on 5 pages