INTERNATIONAL STANDARD

ISO 16844-3

First edition
2004-11-01

Road vehicles — Tachograph systems —

Part 3: Motion sensor interface

Véhicules routiers — Systèmes tachygraphes —

Partie 3: Interface de capteur de mouvement

Reference number
ISO 16844-3:2004(E)

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 16844-3 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

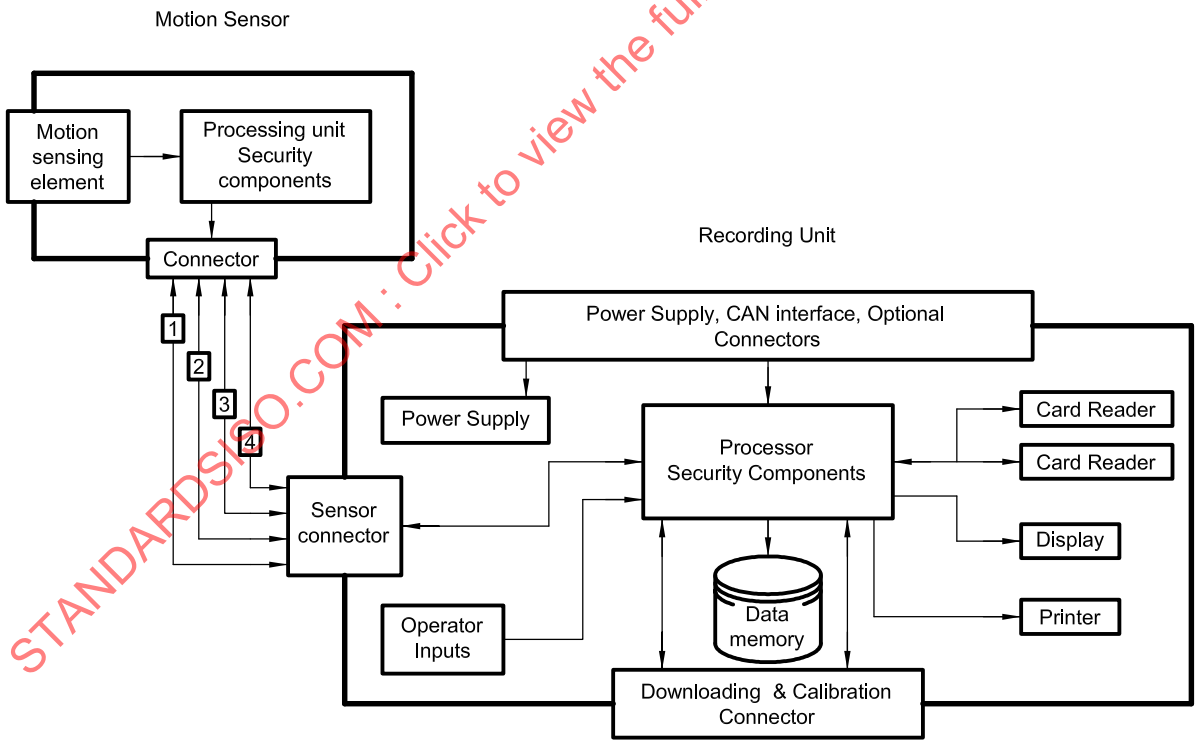
ISO 16844 supports and facilitates the communication between electronic units and a tachograph; the tachograph being based upon Council Regulations (EEC) No. 3820/85 [1] and (EEC) No. 3821/85 [2] and their amendments Council Regulation (EEC) No. 2135/98 [3] and Commission Regulation (EC) No. 1360/2002 [4].

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 3: Motion sensor interface

1 Scope

This part of ISO 16844 specifies the physical and data link layers of the electrical interface connecting a motion sensor to a vehicle unit, used in tachograph systems in road vehicles to perform speed signal transmission and data interchange.

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 15170-1, *Road vehicles — Four-pole electrical connectors with pins and twist lock — Part 1: Dimensions and classes of application*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
check sum
sum (two byte value) of the bytes pointed out at the corresponding location

3.2
direction of movement
bit 6 of byte MF showing whether the vehicle moving direction is forward or reverse

3.3
direction of movement ON
bit 7 of Byte MF showing whether the additional direction information is available or not

3.4
identification key
key necessary for Initialization of a motion sensor, not stored in the sensor memory

NOTE The identification key is derived by adding a constant control vector of the value 48 21 5F 00 03 41 32 $8A_I$ ‖ 00 68 4D 00 CB 21 70 1D hexadecimal on the master key (K_{ID}=K XOR CV).

3.5
inter byte timing
possible pause between two bytes of a message

3.6
header
first four bytes of a message containing sync-byte, target, STX and length of the message

3.7
key
master key
key necessary for Initialization of a motion sensor, not stored in the sensor memory

3.8
pairing key
key only used during the pairing sequence

NOTE Every pairing key is unique to the motion sensor to which it belongs.

3.9
reset
restart of the motion sensor processing unit program

3.10
RxD_in
signal within the motion sensor to the RxD input of the processing unit

3.11
sensor signal
frequency signal proportional to the speed within the motion sensor

3.12
session key
key used for messages to be encrypted

NOTE Every session key is unique to a special motion sensor and the vehicle unit to which it belongs.

3.13
tail
last two bytes of a message containing ETX and LRC

3.14
triple DES
multiple encryption or decryption of plain text or cipher text with different keys

NOTE 1 Encryption: first, the plain text is encrypted using a first key, then it is decrypted using a second key, and then it is encrypted again using a third key.

NOTE 2 Decryption: first, the cipher text is decrypted using the third key, then it is encrypted using the second key, and then it is decrypted again using the first key.

3.15
two-key triple DES
encryption algorithm similar to triple DES where the third key used is equal to the first one

3.16
TxD_out
signal within the motion sensor from the TxD output of the processing unit

3.17
vehicle unit
recording equipment excluding the motion sensor and its connecting cables

NOTE The vehicle unit can either be a single unit or several units distributed in the vehicle, as long as it complies with the security requirements of [1], [2] and [3].

3.18
voltage monitor
hardware function that detects a drop of the supply voltage below a defined level

3.19
K'_P
key derived from the pairing used to encrypt the pairing data

4 Symbols and abbreviated terms

CS	check sum
Cs_{high}	high byte of CS
Cs_{low}	low byte of CS
CV	control vector
CVPI	check value previous instruction
D_A	data for authentication
DES	data encryption standard
D_{Fs}	data of file selected
DON	direction of movement On
DM	direction of movement
D_S	data of sensor (encrypted, i.e. two-key triple DES)
EXT	end of text marker
K	master key
K_{ID}	identification key
K_P	pairing key
K_S	sessions key
LSB	least significant byte
LRC	longitudinal redundancy check
MF	multi function byte
MSB	most significant byte

NARA new audit record available

N_S extended serial number

P_D pairing data

STX start of text

VU vehicle unit

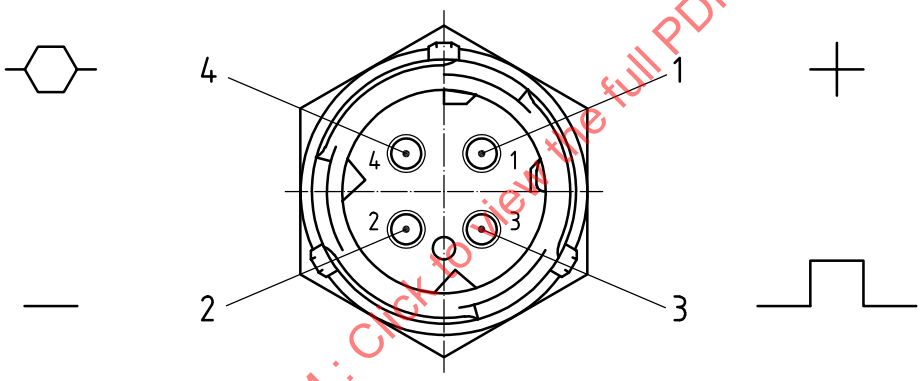
XOR arithmetical exclusive OR

5 Connector

5.1 Dimensions and pin allocation

The connector used (see Figure 2) shall be according to ISO 15170-1, with coding No. 1, application class K3 (contact temperature range −40 °C to +140 °C, max. acceleration of vibrations 300 m/s^2).

The pin allocation shall be in accordance with Table 1.



Key

1 to 4 pin Nos.

Figure 2 — Marking zone at fixed or free connector — Code 1

Table 1 — Pin allocation

Pin No.	Function
1	Positive supply
2	Battery minus
3	Speed signal, real time
4	Data signal, in/out

5.2 Electrical specification

5.2.1 Electrical requirements

The allocated connector function shall be in accordance with Table 2 and valid within the temperature range –40 °C to +135 °C.

Table 2 — Electrical requirements of allocated connector function

Pole No.	Function	Parameter	Electrical requirements			Remark
			min.	typical.	max.	
1	Positive supply	Voltage	6.5 V	—	9 V	Reverse voltage protected[b]
		Current I_S	—	—	15 mA	Total unit current without direction signal current, see Clause 8.
2	Battery minus	—	—	—	—	See ISO 16844-2.
3	Speed signal real time[a]	U_{low}	—	—	0,8 V	I = 250 µA[b]
		U_{high}	$U_{pos\ sply}$ –1,5 V	—	—	I = –150 µA[b]
		Rise time (10 % to 90 %)	—	50 µs	—	Test condition: External pull up resistor 22 kΩ to positive supply ($U_{pos\ sply}$); $U_{pos\ sply}$ = 6,5 V; external capacitor 2 nF to battery minus.
		Fall time (90 % to 10 %)	—	10 µs	—	
		Frequency	—	—	<1,6 kHz	—
4	Data signal in/out [a]	$U_{low\ in}$	—	—	1,2 V	I = –1 mA[b]
		$U_{high\ in}$	5,2 V	—	—	I = –0,5 mA[b]
		$U_{low\ out}$	—	—	1 V	I = 1 mA[b]
		$U_{high\ out}$	5,4 V	—	—	I = –20 µA[b]
		Rise time (10 % to 90 %)	—	110 µs	—	Test condition: External pull up resistor 10 kΩ to positive supply ($U_{pos\ sply}$); $U_{pos\ sply}$ = 6,5 V; external capacitor 5 nF to battery minus.
		Fall time (90 % to 10 %)	—	10 µs	—	
		Baud rate	—	1200 Baud	—	Accuracy ± 3 %

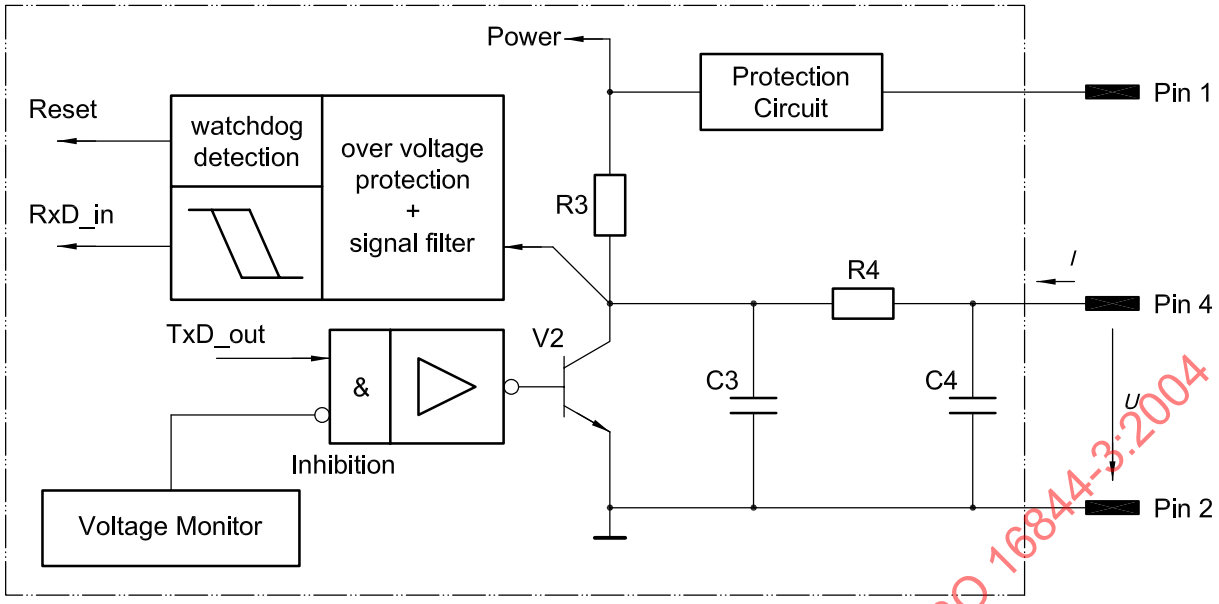
[a] Outputs shall be short circuit protected up to 28V and 1 min.

[b] All values measured relative to pin 2.

5.2.2 Block diagram data signal, in/out

Figure 3 shows a block diagram of the data interface hardware. If no communication takes place, the state of pin 4 shall be high. The incoming signal at pin 4 shall be filtered before it is used as an input signal to the processing unit.

The data TxD_out shall only be transmitted if the voltage monitor shows that the supply voltage is within the specified range. See also 7.5.3.



R3 = 10 kΩ; R4 = 330 Ω; C3 = C4 = 2,2 nF

Figure 3 — Interface data signal — Example

5.2.3 Voltage monitoring and watchdog signal

5.2.3.1 Electrical requirements

The electrical requirements of the voltage monitoring of supply voltage over poles 1 and 2, and the watchdog signal, both submitted via pole 4, shall be in accordance with Table 3.

Table 3 — Requirements of the watchdog signal voltage monitor

Parameter		Electrical requirements			Remark
		Min.	Typical	Max.	
Voltage monitor [a]		5,0 V	—	$U_{pos\ sply}$ 6,5 V	If the supply voltage is below 6,5 V, the sensor may not reply to any request, but if it is below 5,0 V, it does not reply.
Watchdog signal [b]	t_{don}	—	—	1 s	Sensor watchdog reset delay time
	t_{doff}	—	—	1 s	Sensor watchdog recover time
	t_{won}	1 s	—	—	Watchdog on time
	t_{woff}	1 s	—	—	Watchdog off time

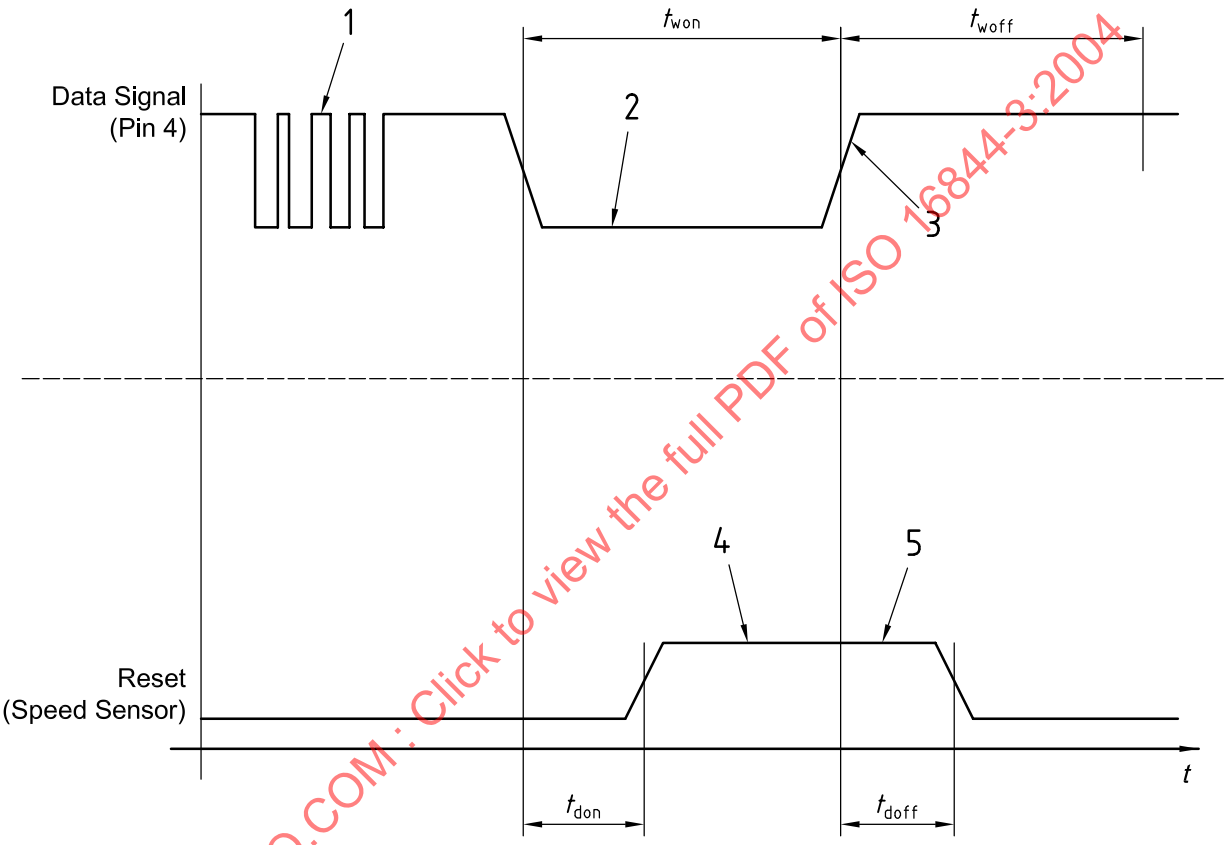
[a] See block diagram of data signal in Figure 3.

[b] See data signal (in) U_{low}, see 5.2.3.2.

5.2.3.2 Timing diagram watchdog signal

If the vehicle unit discovers a time-out of an expected response, it shall be possible to start another attempt or send a watchdog signal to the motion sensor in accordance with Figure 4 and, for voltage levels and timing, in accordance with Table 3. If the motion sensor detects a watchdog signal at pin 4, it shall restart its program (see 7.5.3)

The reset shall not effect the speed real time signal of pin 3.



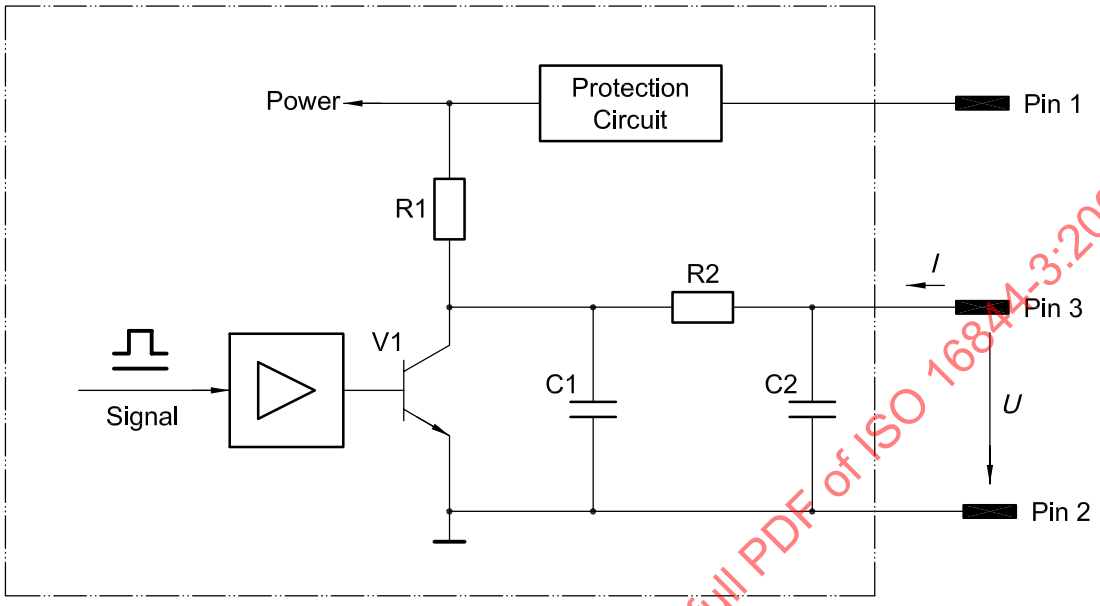
Key

1 normal data signal
2 tachograph sends watchdog signal
3 requirement
4 watchdog detection
5 example

Figure 4 — Timing of watchdog signal

5.2.4 Block diagram of the speed signal, real time

The speed signal, real time is a digital signal with a frequency proportional to the rotary speed of the scanned impulse wheel. Manipulations of this signal shall be of no effect to the messages. Resistance R2 of Figure 5 limits the input current, so it is responsible for overload and short circuit protection.



R1 = 4,7 kΩ; R2 = 1,5 kΩ; C1 = C2 = 1 nF

Figure 5 — Speed signal, real time — Example

6 Cable

The cable for connecting the motion sensor to the vehicle unit shall provide distributed core capacitances of CS < 2,0 nF. The cable impedances depend on parasitic capacitances, inductances, resistances, etc., which influence the transfer characteristic of the cable. The parasitic capacitances (see Figure 6) are of the greatest influence for the frequency range.

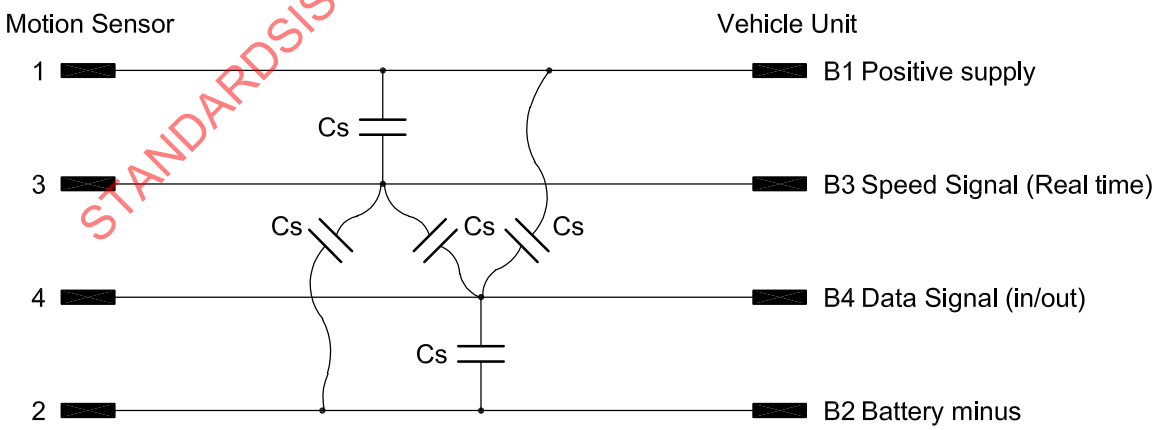


Figure 6 — Equivalent circuit of the cable parasitic capacitances

7 Interface protocol

7.1 Transmission

7.1.1 Data rate and structure of data frame

The transfer of data shall be serial and asynchronous with a baud rate of 1 200 Baud.

The structure of one byte shall be according to Figure 7: 1 start bit, 8 data bits, 1 parity bit (even) and 1 stop bit

	Start	D0	D1	D2	D3	D4	D5	D6	D7	Parity	Stop	

Start bit shall be low state.

Stop bit shall be high state.

Figure 7 — Structure of one data frame message structure

7.1.1.1 Request from vehicle unit to motion sensor

The message structure of a request from the vehicle unit to the motion sensor shall be according to Figure 8.

Header				Data bytes		Tail	
Sync	Target	STX	Length	Instruction No.	Data (depending on the instruction number)	ETX	LRC
LRC = XOR from Sync to ETX							

Figure 8 — Structure of the requests

7.1.1.2 Acknowledge from motion sensor to vehicle unit

The acknowledge from the motion sensor shall be sent as 1 byte, with the instruction number appropriate to the vehicle unit, if a correct request was detected.

7.1.1.3 Break from the vehicle unit

If the vehicle unit receives an incorrect acknowledge from the motion sensor, the vehicle unit may send a break byte as shown in Figure 9.

If the motion sensor detects a break byte, the scheduled reply shall be aborted and the motion sensor shall be ready for a new request. See also 7.1.2.

Value don't care

Figure 9 — Structure of break

7.1.1.4 Reply from the motion sensor to the vehicle unit

The motion sensor shall send the message according to Figure 10 if data have been requested from the vehicle unit.

Header				Data bytes	Tail	
Sync	Target	STX	Length	Data	ETX	LRC
LRC = XOR from Sync to ETX						

Figure 10 — Structure of reply

7.1.1.5 Sync byte

The sync byte shall be a byte of the value 192 decimal, used for controlling the baud rate.

7.1.1.6 Target byte

The target byte shall identify the direction of transmission, where

— logic “0” identifies transmission direction from the vehicle unit to the motion sensor, and

— logic “1” the direction from the motion sensor to the vehicle unit.

7.1.1.7 STX byte

The STX byte shall be a constant byte of the value 2 decimal.

7.1.1.8 Length byte

The length byte specifies the length of the complete message from the sync byte to the LRC; the LRC byte is included.

7.1.1.9 Data bytes

The data bytes shall contain information interchanged between motion sensor and vehicle unit.

7.1.1.10 ETX byte

The ETX byte shall be a constant byte of the value 3 decimal.

7.1.1.11 LRC byte

The LRC byte shall be an arithmetical XOR from Sync until ETX, including ETX.

7.1.1.12 Timing

During normal operation, the timing parameters shall be those according to Figure 11, which shall be in accordance with Table 4.

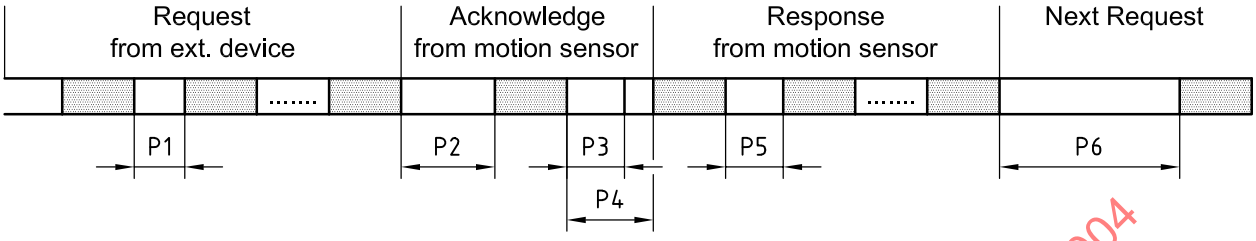


Figure 11 — Structure of timing during normal operation

Table 4 —Timing values

Timing	Value		Description
	min. ms	max. ms	
P1	0	10	Inter byte timing for external request
P2	0	25	Timing between the external request and the acknowledge from motion sensor
P3	0	10	Timing in which the break of an acknowledged request is possible
P4	10	30	Timing between the acknowledge and the motion sensor response
P5	0	10	Inter byte timing for motion sensor response
P6	30 to 25 200 [a]	—	Timing between the motion sensor responses and start of a new external request

[a] Min. and max. timing of period P6 depend on the instruction number.

7.1.2 State diagram — Communication and execution of instructions

Figure 12 shows the execution of the programs within the motion sensor and the vehicle unit and how it is affected by the communication.

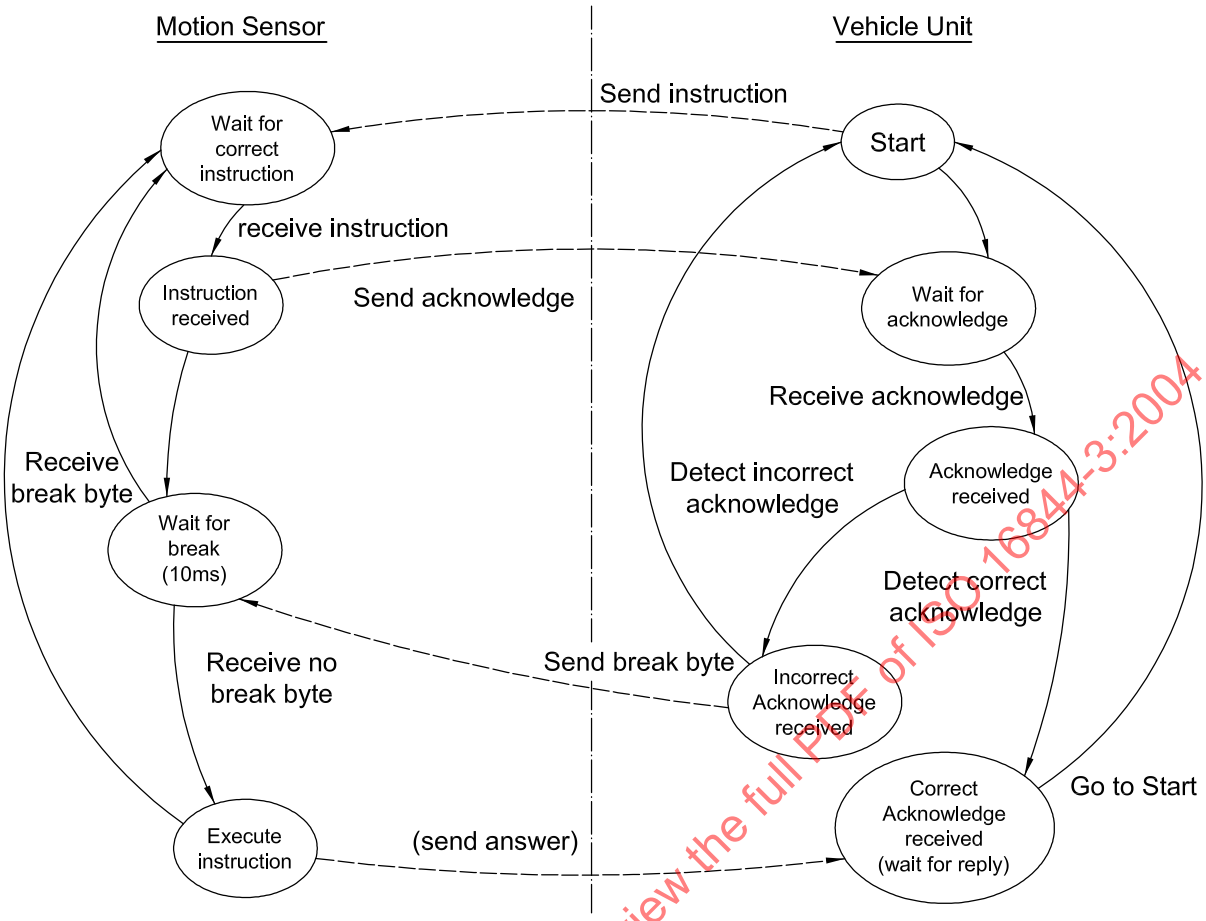


Figure 12 — State diagram of communication and execution of instructions

7.2 Motion sensor state at the end of production

The motion sensor shall be prepared for pairing when it leaves the factory, i.e. the following values shall be stored in its non-volatile memory:

— the extended serial-number of the motion sensor in plain text, N_S, see 7.6.9.6;

— the extended serial-number of the motion sensor encrypted with the identification key, ${}^{e}K_{ID}$ (N_S);

— the pairing key of the motion sensor in plain text, K_P;

— the pairing key of the motion sensor encrypted with master key, e_K (K_P).

The master key and identification key shall not be stored in the non-volatile memory of the motion sensor. The pairing key shall be unique to each motion sensor. The pairing key is only used to pair the motion sensor and the vehicle unit. The two 64 bit halves of the pairing key are distinct. A unique session key is generated during the pairing. The session key is different from the pairing key.

The master key shall not be stored completely within the vehicle unit memory. The identification key shall not be stored within the vehicle unit memory and shall be derived by adding a constant control vector of the value 48 21 5F 00 03 41 32 8A|| 00 68 4D 00 CB 21 70 1D hexadecimal on the master key (K_{ID}=K XOR CV).

The following information shall also be stored in the non-volatile memory of the motion sensor when it is shipped:

— motion sensor type in plain text;

— date of production of the motion sensor in plain text;

— operating system identifier of the motion sensor in plain text;

— security identifier of the motion sensor (type of processor used) in plain text;

— type approval number of the motion sensor in plain text;

— name of the motion sensor manufacturer in plain text.

7.3 Instructions

Instructions numbers shall be in accordance with Table 5.

Table 5 — Instruction numbers

Instruction-number	Vehicle unit request				Motion sensor					Timing to next instruction
						Reply				
	Header Bytes	Instruction Bytes	Data Bytes	Tail Bytes	Acknowledge bytes	Header Bytes	Instruction Bytes	Data Bytes	Tail Bytes	ms
10	4	1	8 [b]	2	1	a	a	a	a	12 600 to 21 000 depending on the file number [d]
11	4	1	0	2	1	4	0	e	2	30
40	4	1	0	2	1	4	0	8 [c]	2	30
41	4	1	8 [b]	2	1	4	0	16 [b]	2	30
42	4	1	16 [b]	2	1	a	a	a	a	8 400
43	4	1	24 [b]	2	1	a	a	a	a	25 200
50	4	1	0	2	1	4	0	24 [b]	2	200
70	4	1	8 [b]	2	1	a	a	a	a	8 400
80	4	1	0	2	1	4	0	8 [b]	2	30

[a] There will no response to the request except the acknowledge.

[b] The data bytes of the concerned instruction will be transmitted encrypted.

[c] The data bytes shall not be encrypted.

[d] See Table 9.

[e] See Tables 10 and 11.

7.4 Initialization of communication between motion sensor and vehicle unit

7.4.1 General

The motion sensor shall be matched with the vehicle unit by the interchange of pairing data.

7.4.2 Necessary sequence of instruction for pairing

7.4.2.1 Overview

Table 6 details the sequence of instruction numbers necessary for pairing.

Table 6 — Sequence of instructions for pairing

Vehicle unit	Direction of data transfer	Motion sensor	Remark
40	→		Initializes pairing
	←	Acknowledge	See 7.1.2.
	←	Response	The motion sensor sends its serial number N_S.
41	→		The vehicle unit sends the extended serial number of the sensor encrypted with identification key.
	←	Acknowledge	See 7.1.2.
	←	Response	If the vehicle unit is authorised, the sensor returns the pairing key encrypted with master key.
42	→		The vehicle unit sends the session key, encrypted with pairing key.
	←	Acknowledge	See 7.1.2.
43	→		The vehicle unit sends the pairing information, encrypted with pairing key.
	←	Acknowledge	See 7.1.2.
50	→		Request for authentication
	←	Acknowledge	See 7.1.2.
	←	Response	The sensor sends the pairing information encrypted with session key.

7.4.3 Pairing initialization of vehicle unit and motion sensor

7.4.3.1 General

The timing between transmission of the initializing instruction and the next instruction shall be at least thirty milliseconds (P6 = 30 ms min.).

7.4.3.2 Initialization message

The vehicle unit shall initialize the pairing by transmitting instruction No. 40 to the motion sensor (see Figure 13).

Sync	Target	STX	Length	Instruction No.	ETX	LRC
192	0	2	7	40	3	238

Figure 13 — Structure of instruction 40 for pairing Initialization

7.4.3.3 Response from the motion sensor to the vehicle unit

The extended serial-number of the motion sensor as shown in Figure 14 shall be sent to the vehicle unit in plain text as response to received instruction No. 40.

The content of data bytes on the data line shall be N_S.

Sync	Target	STX	Length	Extended serial-number of motion sensor								ETX	LRC
192	1	2	14	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	3	x

Figure 14 — Structure of response to instruction 40

7.4.4 Transmission of encrypted serial number of motion sensor

7.4.4.1 General

The encrypted serial number of the motion sensor shall be transmitted from vehicle unit to motion sensor. The timing between transmission of this instruction and the next instruction shall be at least thirty milliseconds (P6 = 30 ms min.).

7.4.4.2 Request

The vehicle unit shall encrypt the extended serial number of the motion sensor, using the identification key and transmit it as an eight (8) byte block to the motion sensor with instruction No. 41 as shown in Figure 15. The content of data bytes on the data line shall be $e_{K_{ID}}(N_S)$.

Sync	Target	STX	Length	Instruction No.	Extended serial number of motion sensor encrypted with identification key								ETX	LRC
192	0	2	15	41	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	3	x

Figure 15 — Structure of instruction 41 — Transmission of encrypted extended serial number of motion sensor

7.4.4.3 Response

The motion sensor then compares the received data with the stored encrypted extended serial number. If they are equal, it is assumed that the authentication of the vehicle unit to the motion sensor is correct. In this case the motion sensor transmits a pairing key which is encrypted with the master key to the vehicle unit. The content of data bytes on the data line, as shown in Figure 16, shall be $e_K(K_P)$.

Sync	Target	STX	Length	Pairing key encrypted with master key														ETX	LRC
192	1	2	22	Byte 0	Byte 1	Byte 2	Byte 3		...	...	...	...	...		Byte 12	Byte 13	Byte 14	Byte 15	3	x

Figure 16 — Structure of response to instruction 41 — Transmission of pairing key to the vehicle unit

7.4.5 Transmission of session key from vehicle unit to motion sensor

7.4.5.1 General

The timing between transmission of this instruction and the next instruction shall be at least eight thousand four hundred milliseconds (P6 = 8400 ms min.).

7.4.5.2 Request

The vehicle unit checks that the two 64 bit halves of the pairing key are distinct. Then, subject to this condition, the vehicle unit shall send the session key encrypted with the pairing key (see Figure 17) and shall transmit it with instruction No. 42 as a sixteen (16) byte block to the motion sensor. As the session key is 16 bytes long, it is necessary to start the encryption procedure twice.

The session key is decrypted with the pairing key and stored permanently in the non-volatile memory of the motion sensor. It shall be changed by every initialization. The content of data bytes on the data line shall be $e_{Kp}(K_S)$.

Sync	Target	STX	Length	Instruction No.	Session key encrypted with pairing key																ETX	LRC
192	0	2	23	42	Byte 0	Byte 1	Byte 2	Byte 3		...	...	...	...	...	...		Byte 12	Byte 13	Byte 14	Byte 5	3	x

Figure 17 — Structure of instruction 42 — Transmission of session key to motion sensor

7.4.6 Transmission of pairing information from vehicle unit to motion sensor

7.4.6.1 General

The timing between transmission of this instruction and the next instruction shall be at least twenty-five thousand, two-hundred milliseconds (P6 = 25 200 ms min.).

7.4.6.2 Request

The vehicle unit encrypts the pairing information with the pairing key using two-key triple DES and shall transmit it with the instruction No. 43 as a twenty-four (24) byte block to the motion sensor (see Figure 18). As the pairing information is 24 bytes long, it is necessary to start the encryption procedure three times.

The motion sensor decrypts the pairing information with the pairing key using two key triple DES and stores it permanently in the non-volatile memory of the motion sensor. The pairing information shall be found at two locations in the non-volatile memory: at the location for the first pairing and the location for the last pairing. While the pairing information of the first pairing shall never be overwritten, the pairing information of the last pairing changes with every pairing.

The content of data bytes on the data line shall be $e_{Kp}(P_D)$.

Sync	Target	STX	Length	Instruction No.	Pairing Information (encrypted with pairing key)															ETX	LRC
192	0	2	31	43	Byte 0	Byte 1	Byte 2	Byte 3		...	...	...	...	...	...		Byte 20	Byte 21	Byte 22	Byte 23	3	x

Figure 18 — Transmission of pairing information to motion sensor

7.4.7 Request from vehicle unit for pairing information and authentication to motion sensor

7.4.7.1 Request

The vehicle unit shall request the motion sensor for pairing information and authentication using instruction No. 50 to the motion sensor as shown in Figure 19.

Sync	Target.	STX	Length	Instruction No.	ETX	LRC
192	0	2	7	50	3	244

Figure 19 — Request for authentication to motion sensor

The vehicle unit shall decrypt the data bytes with the session key and compare the decrypted data with the pairing information of the current pairing. If they are equal, it is assumed that the authentication of the motion sensor to the vehicle unit is correct and that the motion sensor is using the correct session key.

7.4.7.2 Response from motion sensor to vehicle unit

The motion sensor shall respond by submitting the pairing information as shown in Figure 20. The contents of data bytes on the data line shall be $e_{Ks}(P_D)$.

Sync	Target	STX	Length	Pairing Information (encrypted with session key)															ETX	LRC
192	1	2	30	Byte 0	Byte 1	Byte 2	Byte 3		...	...	...	...	...		Byte 20	Byte 21	Byte 22	Byte 23	3	x

Figure 20 — Structure of response to instruction 50 — Request for authentication to motion sensor

7.5 Communication of motion sensor and vehicle unit in normal use

7.5.1 Necessary sequence of instruction Nos. for communication in normal use

The necessary sequence of instruction Nos. for communication in normal use shall be in accordance with Table 7.

Table 7 — Sequence of instruction Nos. for communication in normal use

Vehicle unit	Direction of data transfer	Motion sensor	Remark
70	→		The vehicle unit sends authentication data to the motion sensor.
	←	Acknowledge	See 7.1.2.
80	→		The vehicle unit sends request for response to the motion sensor.
	←	Acknowledge	See 7.1.2.
	←	Response	If the vehicle unit is authorized, the motion sensor sends authentication and sensor data to the vehicle unit.

7.5.2 Latch of counter value and encrypt data

7.5.2.1 General

The timing between this instruction and the next instruction shall be at least eight-thousand, four-hundred milliseconds (P6 = 8400 ms min.).

7.5.2.2 Request

The request for latch counter value and encrypted data shall be transmitted with the instruction No. 70 from the vehicle unit to the motion sensor using a thirty-two (32) bit random number encrypted with the session key.

7.5.2.3 Latch timing

The counter value of a 16 bit counter shall be latched in the moment when the transmitter becomes empty of the acknowledgement of instruction No. 70. The content of data bytes on the data line, as shown in Figure 21, shall be $e_{Ks}(D_A)$.

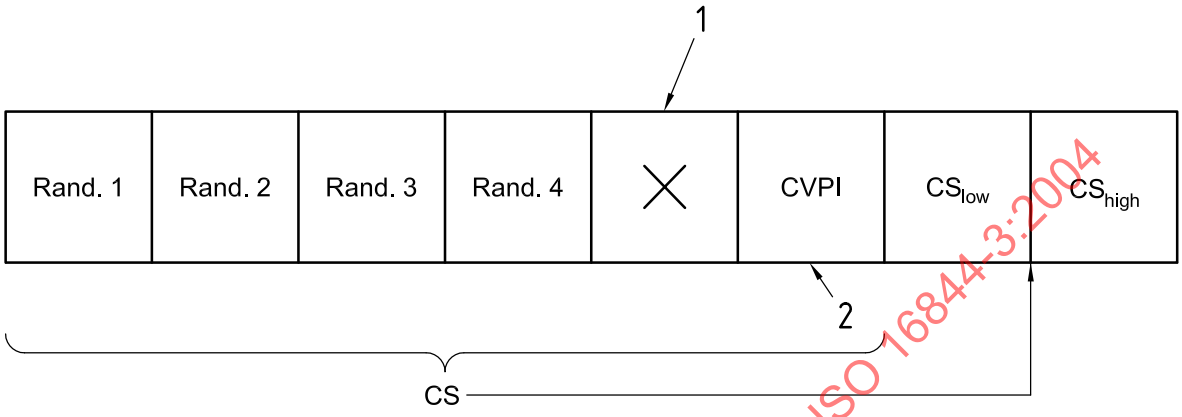
Sync	Target.	STX	Length	Instruction No.	Authentication data 8 bytes (4 bytes random number and 4 bytes control information)[a] encrypted with session key								ETX	LRC
192	0	2	15	70	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	3	x

[a] See Figure 22.

Figure 21 — Latch counter value and encrypt data

7.5.2.4 Authentication data after decryption

The motion sensor may check that no information was lost since the reception of the last instruction by means of the check value CVPI (see Figure 22). The authentication is correct if the checksum from byte 0 to byte 5 is equal to the value of byte 6 and byte 7. Value CVPI shall be set to 0 by the vehicle unit when the communication is started the very first time after pairing of vehicle and sensor unit.



Key

1 In the case of instruction No.10, the file number shall be found at this position; in the case of instruction No. 70, this byte is left unspecified.

2 Instruction No.10 or No. 70: XORed with the low byte of the actually latched counter value.

Figure 22 — Structure of authentication data after decryption

7.5.3 Transmission of encrypted data

7.5.3.1 General

The timing between this instruction and the next instruction shall be at least thirty milliseconds (P6 = 30 ms min.).

7.5.3.2 Request

The request from the vehicle unit to the motion sensor shall be as shown in Figure 23 with instruction No. 80.

Sync	Target	STX	Length	Instruction No.	ETX	LRC
192	0	2	7	80	3	150

Figure 23 — Structure of instruction 80 — Transmission of encrypted data

7.5.3.3 Response

The response to instruction No. 80 submitted from the motion sensor to the vehicle unit shall be as shown in Figure 24.

The data (see Figure 24) shall be transmitted encrypted with the session key. Only Sync, Target, STX, Length, ETX and LRC shall be transmitted in plain text. The meaning of encrypted data shall be as shown in Figure 25. The contents of data bytes on the data line shall be $e_{Ks}(D_S)$.

Sync	Target	STX	Length	Encrypted data								ETX	LRC
192	1	2	14	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	3	x

Figure 24 — Structure of response to instruction 80

7.5.3.4 Encrypted data after decryption

The structure of encrypted data after decryption shall be as shown in Figure 25.

Duty cycle	Random number from instruction No. 70 XOR Serial-number of the motion sensor				Counter value of the motion sensor		Additional information
DC	Rand.1 ⊕ Serno.1	Rand.2 ⊕ Serno.2	Rand.3 ⊕ Serno.3	Rand.4 ⊕ Serno.4	LSB	MSB	MF

Figure 25 — Structure of data after decryption

7.5.3.5 MF byte

The MF byte, as shown in Figure 26, shall contain a bit reserved for NARA set to logic “1” if available. The bit shall automatically be cleared when the motion sensor detects that the vehicle unit has received its response to the instruction 11 file number 0. The mechanism of detection shall be as shown in Figure 22, where byte CVPI shows that the authenticated vehicle unit had accepted the message.

Additional direction information [a]		New audit record available					
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
DON [b]	DM	NARA	c	c	c	c	c

[a] See 8.1.

[b] Fixed by the manufacturer.

[c] The meaning of these bits is undefined.

Figure 26 — Structure of byte MF after decryption

7.5.3.6 Counter value

The 16 bit counter in the motion sensor shall be decremented with each pulse of the speed signal.

7.5.3.7 Duty cycle

The structure of the duty cycle shall be as shown in Figure 27, where

a) the motion sensor is measuring, as a percentage, the duty cycle of the real-time speed signal, and

b) the reset bit shows the occurrence of a system reset and shall be set after reset and automatically cleared when byte CVPI indicates that the message has been accepted by the authenticated vehicle unit (see, too, Figure 22).

Reset	Duty cycle of the real time speed signal %						
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Figure 27 — Structure of byte duty cycle

7.6 Read information

7.6.1 Necessary sequence of instruction for reading information

The necessary sequence of the instruction for reading information shall be in accordance with Table 8.

Table 8 — Sequence of instruction for reading information

Vehicle unit	Direction	Motion sensor	Remark
10	→		The vehicle unit sends authentication data and the number of the requested file to the motion sensor.
	←	Acknowledge	See 7.1.2.
11	→		The vehicle unit sends request for response to the motion sensor.
	←	Acknowledge	See 7.1.2.
	←	Response	If the vehicle unit is authorised, the motion sensor sends authentication and requested data to the vehicle unit.

7.6.2 Request

7.6.2.1 General

The timing between this instruction and the next depends on the number of the requested file and shall be in accordance with Table 9, i.e. lasting between twelve-thousand, six-hundred milliseconds and twenty-one thousand milliseconds (12 600 ms $\leqslant$ P6 $\leqslant$ 21 000 ms).

Table 9 — Timing P6

Number of file(s)		0	1	2	3	4	5	6
Time P6	ms	12 600	12 600	21 000	21 000	12 600	12 600	12 600

7.6.2.2 Request

The request for selected data by the vehicle unit to the motion sensor shall be as shown in Figure 28.

Sync	Target	STX	Length	Instruction No.	Authentication data 8 bytes (4 bytes random number and 4 bytes control information) encrypted with session key								ETX	LRC
192	0	2	15	10	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	3	x

Figure 28 — Structure of instruction 10 — Request for motion sensor information

7.6.2.3 Preparation and response

The selected data shall be prepared after instruction No. 10 has been received, and shall be transmitted after reception of instruction No. 11.

Instructions 10 and 11 may be sent to the motion sensor, for example, if bit NARAC was set in the response to instruction 80.

The error message shall be updated whenever an error occurs. An error message shall be overwritten if a new error occurs.

The content of data bytes on the data line shall be $e_{Ks}(D_A)$.

7.6.3 General message structures

7.6.3.1 General

The timing between this instruction and the next instruction shall be at least thirty milliseconds (P6 = 30 ms min.).

7.6.3.2 Request

A request of the vehicle unit to the motion sensor shall be as shown in Figure 29 with instruction No. 11.

Sync	Target	STX	Length	Instruction No.	ETX	LRC
192	0	2	7	11	3	205

Figure 29 — Structure of instruction 11

7.6.3.3 Response

A response to instruction No. 11 of the motion sensor to the vehicle unit shall be as shown in Figure 30.

Sync	Target	STX	Length	Data for authentication Number of Selected File checksum over all data				Data of Selected File[a]									ETX	LRC
192	1	2	a	Byte 0	Byte 1	…	Byte 6	Byte 7	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	…	3	x

[a] For number of bytes, see Table 10.

Figure 30 — Structure of a response to instruction 11

The meaning of the several files and how to read them is explained in Tables 10 and 11. The sequence of instruction Nos. 10 and 11 gives the vehicle unit not only the possibility to read error messages, but also to get additional information (see Table 10).

The content of data bytes on the data line shall be $e_{Ks}(D_{Fs})$.

See Figure 31.

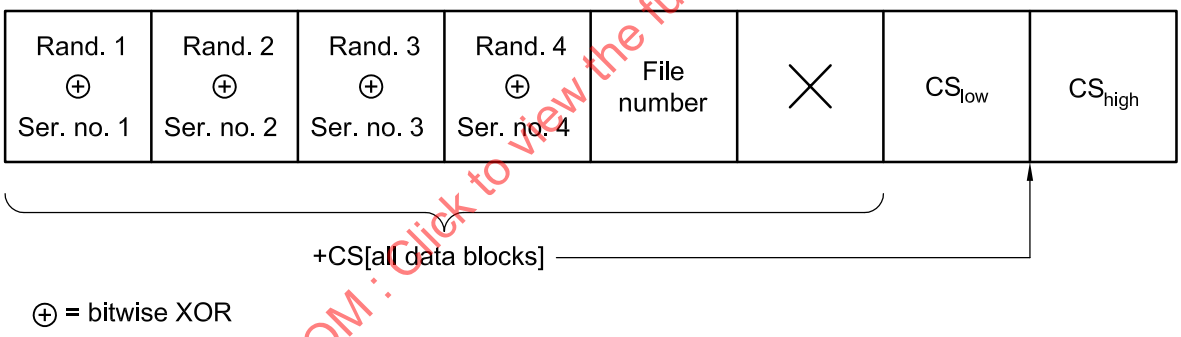


Figure 31 — Structure of data for authentication — Response from motion sensor

7.6.4 Data block chaining

The chaining operation of data blocks shown in Figures 32 to 35 makes the cipher text blocks dependent on current and all preceding plain text blocks — therefore, rearranging cipher text blocks shall not result in a rearranging of the corresponding plain text blocks. The use of different start values prevents the same plain text enciphering to the same cipher text. The use of chaining makes the output feedback more invulnerable to active attacks.

7.6.5 Encryption with two data blocks

Encryption with two data blocks (file number 0, 1, 4, 5, 6) shall be performed as shown in Figure 32. See, also, ISO/IEC 10116.

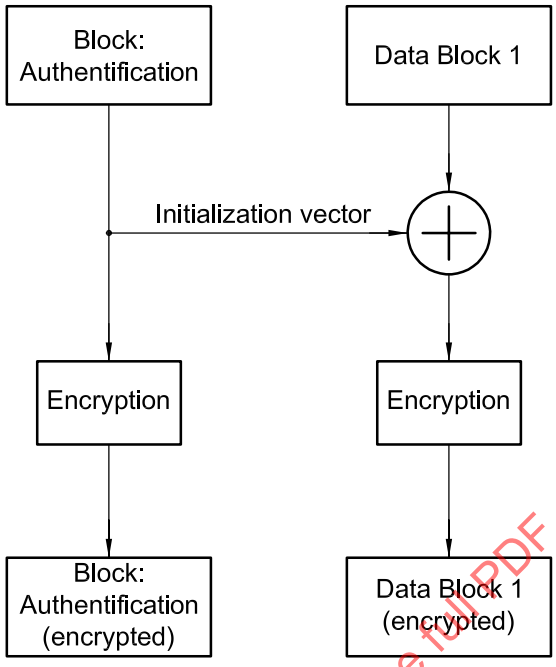


Figure 32 — Data block chaining — Encryption with two data blocks

7.6.6 Encryption with three data blocks

Encryption with three data blocks (file Nos. 2, 3) shall be performed as shown in Figure 33. See, also, ISO/IEC 10116.

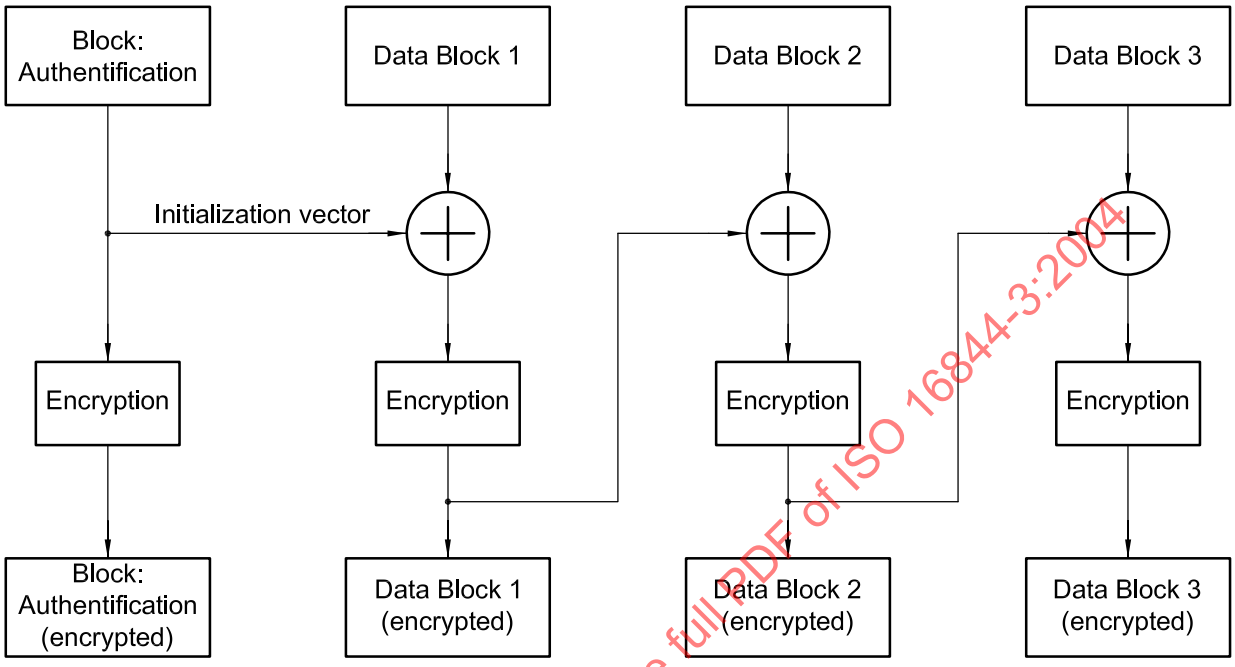


Figure 33 — Data block chaining — Encryption with three data blocks

7.6.7 Decryption with two data blocks

Decryption with two data blocks (file Nos. 0, 1, 4, 5, 6) shall be performed as shown in Figure 34. See, also, ISO/IEC 10116.

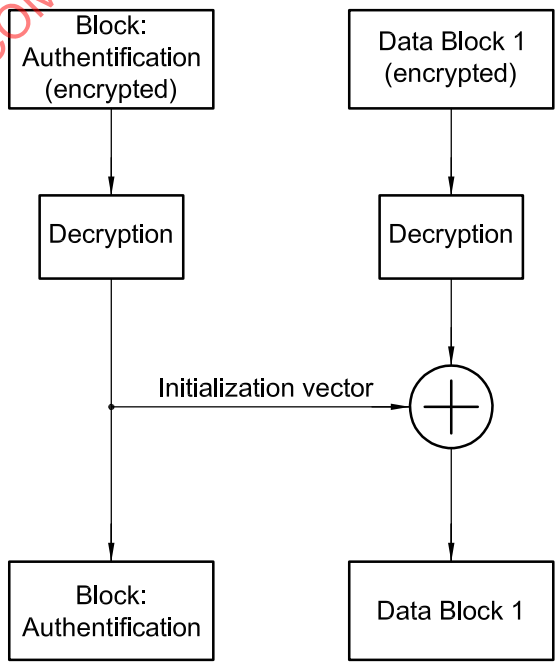


Figure 34 — Data block chaining — Decryption with two data blocks

7.6.8 Decryption with three data blocks

Decryption with three data blocks (File Nos. 2, 3) shall be performed according to Figure 35. See, also, ISO/IEC 10116.

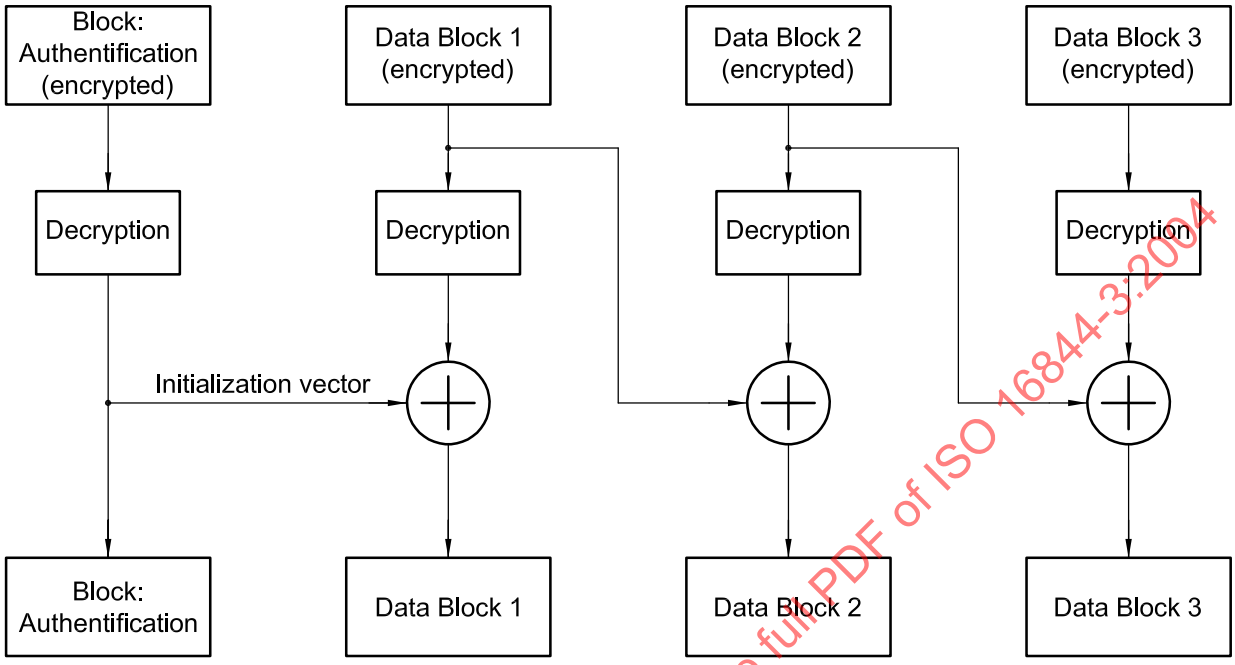


Figure 35 — Data block chaining — Decryption with three data blocks

7.6.9 Structures of selected data

7.6.9.1 Guide to the data bytes

Table 10 specifies the data bytes depending on the number of the files which may be involved. All information shall be encrypted with the session key.

Table 10 — Guide to the data bytes

Identification File No.	Number of data bytes [a] Data for authentication	 Data of selected file	Length	Description
0	8	8	22	Error message: Actual random number (transmitted with the previous instruction, No. 70) when the error is detected, kind of error (see Table 11).
1	8	8	22	The operating system identifier of the motion sensor (see Table 12).
2	8	24	38	The pairing information of the first pairing motion sensor (see Table 13).
3	8	24	38	The pairing information of last pairing of the motion sensor (see Table 14).
4	8	8	22	The extended serial number of the motion sensor (see Table 15).
5	8	8	22	The security identifier of the motion sensor (see Table 16).
6	8	8	22	The type approval number of the motion sensor (see Table 17).
NOTE More information about the meaning of the data depending on the selected file is given in Tables 11 to 17.				
[a] See Figure 30.				

7.6.9.2 Structures of error messages

Error messages shall be transmitted as data of file number 0.

The structure of error messages shall be in accordance with Table 11, showing the explanation of the error messages (see, also, Table 10).

Table 11 — Guide to audit record data

Date (actual random number) 4 Bytes	Class of error 1 Byte	Status1 1 Byte	Unused 2 Bytes	Remark (all bits active high)
XXXX	20 non volatile memory	Address of memory location		The start address of the memory block in which an error has been detected is transmitted to the vehicle unit.
XXXX	21 controller RAM			
XXXX	22 controller-instruction			
XXXX	23 communication			
XXXX	24 authentication (instructions 10 and 70)			
XXXX	25			Reserved for future use
XXXX	26 sensor element			Optional
XXXX	27 over temperature			Optional