INTERNATIONAL STANDARD

ISO 16844-3

Second edition
2022-05

Road vehicles — Tachograph systems —

Part 3: Motion sensor communication interface

Véhicules routiers — Systèmes tachygraphes —

Partie 3: Interface de communication pour capteur de mouvement

Reference number
ISO 16844-3:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

This second edition cancels and replaces the first edition (ISO 16844-3:2004), which has been technically revised. It also incorporates the Technical Corrigendum ISO 16844-3:2004/Cor. 1:2006.

The main changes are as follows:

— part 5 of this series (ISO 16844-5) has been removed due to its technical irrelevance,

— correction of the typos and mistakes in the text,

— adoption of the content according to the new version of the ISO guidelines,

— adoption of the content according to the new technical requirements,

— alignment of the content regarding to the referred standards.

A list of all parts in the ISO 16844 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

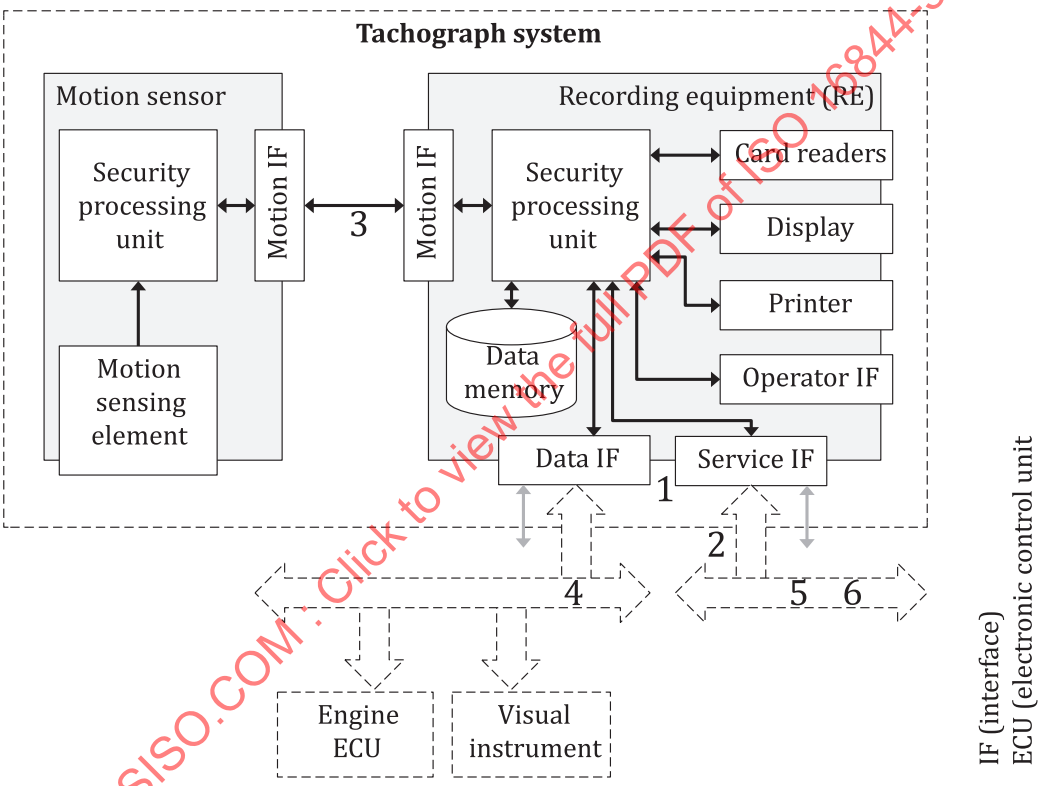
Introduction

This document supports and facilitates the communication between electronic control units (ECUs) and a digital tachograph.

The digital tachograph concept is based upon a recording equipment storing data, related to the activities of the various drivers driving the vehicle, on which it is installed.

During the normal operational status of the recording equipment, data stored in its memory are accessible to different entities (drivers, authorities, workshops, transport companies) in different ways (displayed on a screen, printed by a printing device, downloaded to an external device). Access to stored data is controlled by a smart card inserted in the tachograph.

A typical tachograph system is shown in Figure 1.



Key

1 data and service IF connector standardized in ISO 16844-1

2 electrical data and service IF requirements standardized in ISO 16844-2

3 communication interface between motion sensor and RE standardized in this document

4 CAN-based data IF including parameter groups standardized in ISO 16844-4

5 optional CAN-based service IF standardized in ISO 16884-6

6 data identifier (DID) specification for the optional service IF standardized in ISO 16844-7

Figure 1 — Typical ISO 16844 conformant tachograph system

Road vehicles — Tachograph systems —

Part 3:
Motion sensor communication interface

1 Scope

This document specifies the communication interface between motion sensor and recording equipment. This includes the mechanical, electrical and logical requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 16844-1, *Road vehicles — Tachograph systems — Part 1: Recording equipment data and service connector*

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 16844-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

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 indicating whether the vehicle moving direction is forward or reverse

3.3
direction of movement On
bit 7 of byte MF indicating whether the additional direction information is available or not

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

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

3.8
pairing key
key only used during the pairing sequence

Note 1 to entry: Every pairing key is unique to the motion sensor to which it belongs. All the cryptography uses the AES-based encryptions.

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
session key
key used for messages to be encrypted

Note 1 to entry: Every session key is unique to a special motion sensor and the recording equipment to which it belongs.

3.12
tail
last two bytes of a message containing ETX and LRC

3.13
TxD_out
signal within the motion sensor from the TxD output of the processing unit

3.14
voltage monitor
hardware function that detects a drop of the supply voltage below a defined level

4 Symbols and abbreviated terms

For the purposes of this document, the following the following symbols and abbreviated terms apply:

CAN	controller area network
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
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)
$e_{K_x}(A)$	encrypted data A using a particular key K_x
EXT	end of text marker
I_S	current power supply
K	master key
K_{ID}	identification key
K_P	pairing key
K'_P	key derived from the pairing used to encrypt the pairing data
K_S	session key
LSB	least significant byte
LRC	longitudinal redundancy check
MF	multi-function byte
MSB	most significant byte
NARA	new audit record available
n	number of bytes
N_S	extended serial number
P_D	pairing data
$R_{type\_approval\_no}$	type approval number of the recording equipment (VU)
R_{serial_no}	serial number of the recording equipment (VU)
STX	start of text
$t_{pairing}$	date of pairing
U_{low}	speed signal voltage low value
$U_{low\ in}$	input signal voltage low value
$U_{low\ out}$	output signal voltage low value
U_{high}	speed signal voltage high value
$U_{high\ in}$	input signal voltage high value

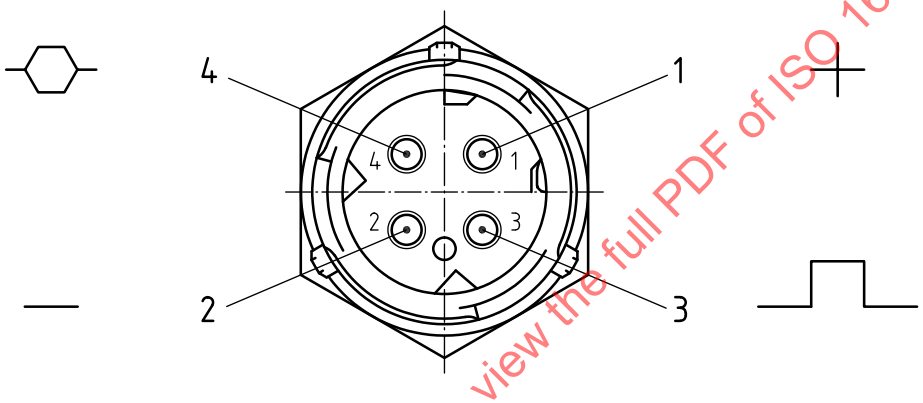
$U_{\text{high out}}$	output signal voltage high value
$U_{\text{pos sply}}$	positive supply voltage
VU	recording equipment
XOR	arithmetical exclusive OR

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, maximum acceleration of vibrations 300 m/s^2).

The pin allocation shall be in accordance with Table 1.



Key

1 to 4 pin numbers

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 shall be 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	—	
		bit rate	—	1 200 bit/s	—	Accuracy ±3 %

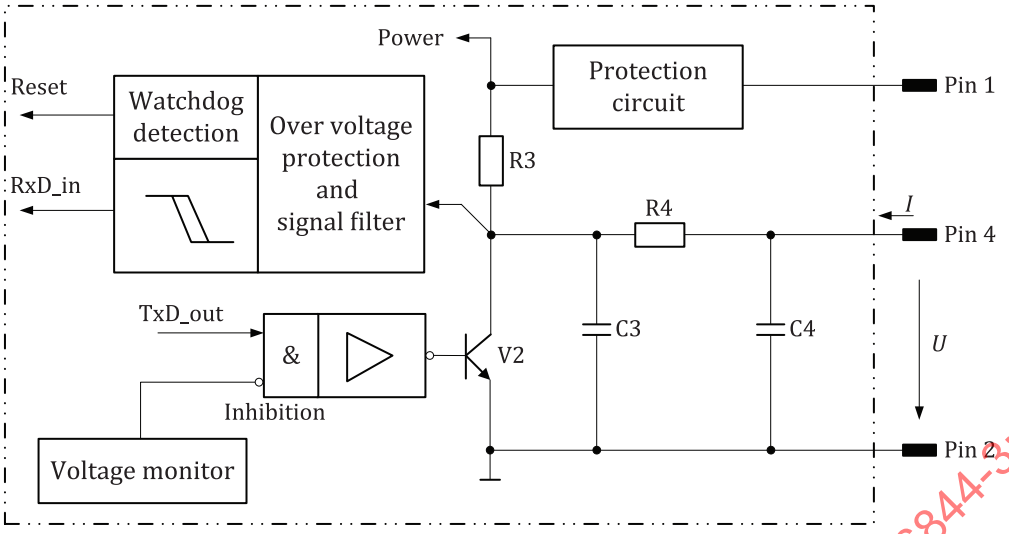
[a] Outputs shall be short-circuit protected up to 28 V for 1 min.

[b] Values are measured relatively 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 U_{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 7.5.3.1.



Key

R3	10 kΩ
R4	330 Ω
C3, C4	2,2 nF
V2	npn transistor

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 pins 1 and 2, and the watchdog signal, both submitted via pin 4, shall be in accordance with Table 3. If the supply voltage is below 6,5 V, the motion sensor may reply to requests; but if it is below 5,0 V, it shall not reply.

Table 3 — Requirements of the watchdog signal voltage monitor

Parameter		Electrical requirements			Remark
		Min.	Typical	Max.	
Voltage monitor [a]		5,0 V	—	$U_{\text{pos sply}}$ 6,5 V	No remark
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

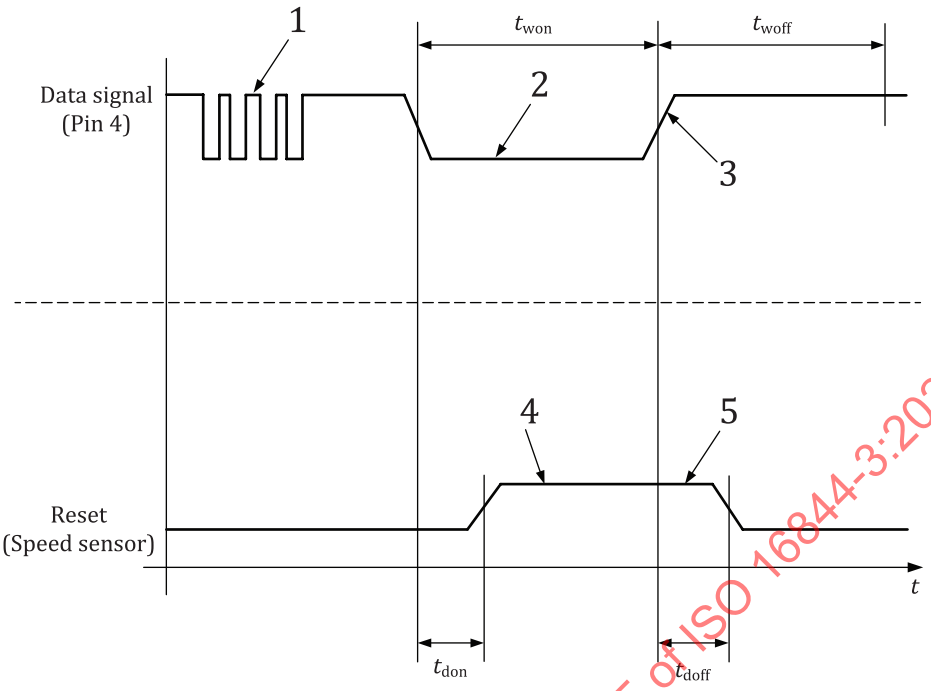
[a] See block diagram of data signal in Figure 3.

[b] Voltage level: see data signal in/out (in) $U_{\text{low in}}$, see 5.2.3.2.

5.2.3.2 Timing diagram watchdog signal

If the recording equipment 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 7.5.3.6).

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



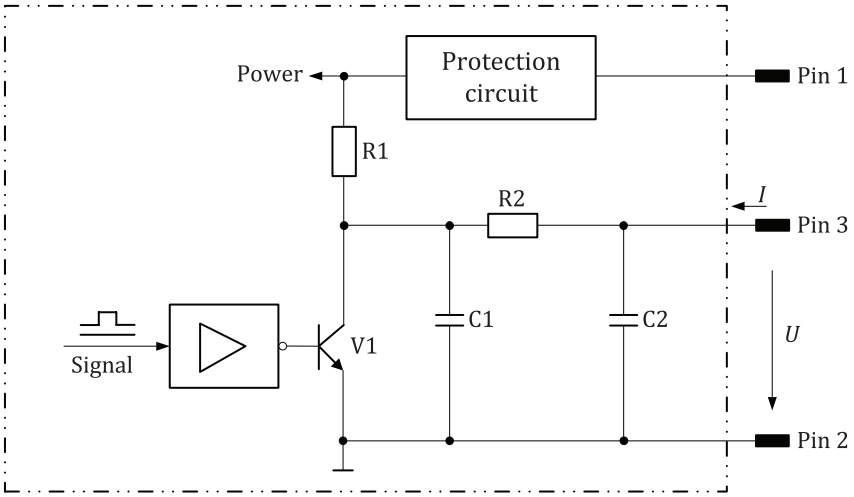
Key

1	normal data signal	4	watchdog detection
2, 3	tachograph sends watchdog signal	5	sensor watchdog recover time

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.



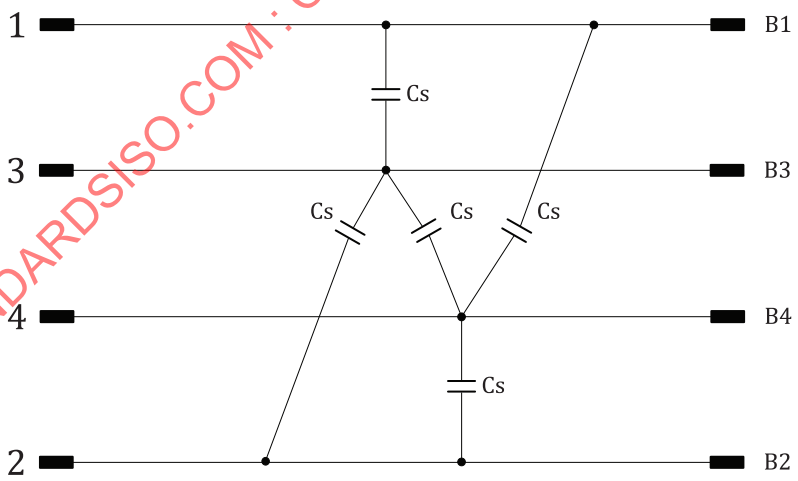
Key

R1	4,7 kΩ
R2	1,5 kΩ
C1, C2	1 nF
V1	npn transitor

Figure 5 — Speed signal, real-time — Example

6 Cable

The cable for connecting the motion sensor to the recording equipment 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.



Key

1 – 4	connector motion sensor
B1 – B4	connector vehicle unit
Cs	see text

Figure 6 — Equivalent circuit of the cable parasitic capacitances

7 Interface protocol

7.1 Transmission

7.1.1 Bit rate and frame structure

The transfer of data shall be serial and asynchronous with a bit rate of 1 200 bit per second.

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

1	Start	D0	D1	D2	D3	D4	D5	D6	D7	Parity	Stop	1

Key

1	don't care
D0	least significant bit
D7	most significant bit
Start	bit at low state
Stop	bit at high state

Figure 7 — Transmission of one byte

7.1.2 Frame specification

7.1.2.1 Request frame from recording equipment to motion sensor

The request frame from the recording equipment to the motion sensor shall be according to Table 4.

Table 4 — Structure of the request frame

Header				Data bytes		Tail	
Sync	Target	STX	Length	Instruction number	Data (depend on the instruction number)	ETX	LRC[a]

[a] LRC = XOR from Sync to ETX.

7.1.2.2 Acknowledge frame from motion sensor to recording equipment

The acknowledge from the motion sensor shall be sent as single byte, with the instruction number appropriate to the recording equipment, if a correct request is detected.

7.1.2.3 Break frame from the recording equipment

If the recording equipment receives an incorrect acknowledge from the motion sensor, the recording equipment may send a break frame "single byte - value doesn't care".

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

7.1.2.4 Reply frame from the motion sensor to the recording equipment

The motion sensor shall send the reply frame according to Table 5 if motion sensor data have been requested from the recording equipment.

Table 5 — Structure of reply frame

Header				Data bytes	Tail	
Sync	Target	STX	Length	Data	ETX	LRC[a]
[a] LRC = XOR from Sync to ETX.						

7.1.2.5 Sync byte

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

7.1.2.6 Target byte

The target byte shall identify the direction of transmission, where

— logic "0" identifies transmission direction from the recording equipment to the motion sensor, and

— logic "1" the direction from the motion sensor to the recording equipment.

7.1.2.7 STX byte

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

7.1.2.8 Length byte

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

7.1.2.9 Data bytes

The data bytes shall contain information interchanged between motion sensor and recording equipment.

The data bytes shall be sent as MSB first, LSB last.

7.1.2.10 ETX byte

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

7.1.2.11 LRC byte

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

7.1.2.12 Timing

During normal operation, the timing parameters shall be those according to Figure 8, which shall be in accordance with Table 6.

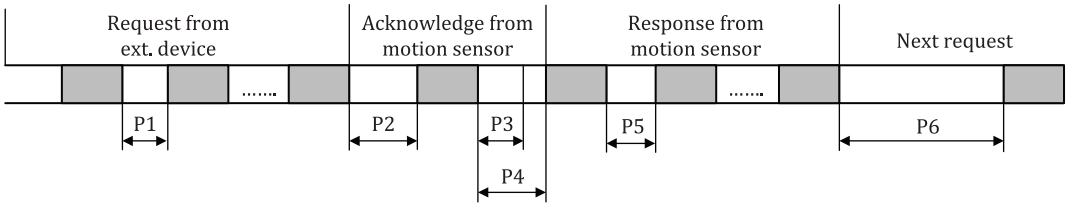


Figure 8 — Structure of timing during normal operation

Table 6 — Timing values

Timing	Value		Description
	min. ms	max. ms	
P1	0	10	Inter byte timing for the 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 the motion sensor response
P6	30 to 25 200[a]	—	Timing between the motion sensor responses and start of a new external request

[a] Minimum timing of period P6 depend on the instruction number, as specified in Table 5.

7.1.3 State diagram — Communication and execution of instructions

Figure 9 shows the execution of the programs within the motion sensor and the recording equipment and how it is affected by the communication.

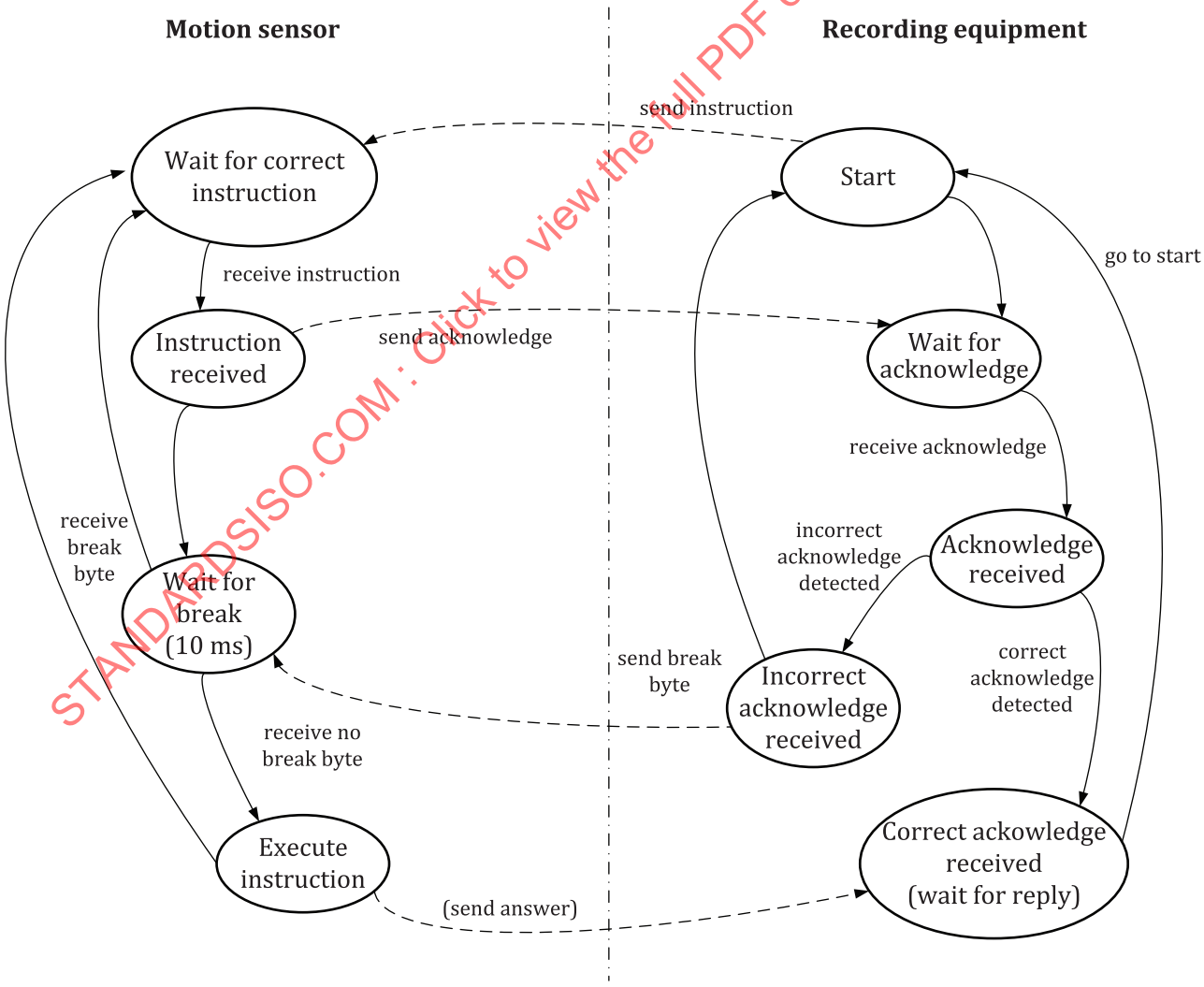


Figure 9 — State diagram of communication and execution of instructions

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 is not encrypted, N_S, see 7.6.5.6;

— the extended serial-number of the motion sensor encrypted with the identification key, $e_{K_{ID}}$ (N_S) and all relevant versions of $e_{K_{ID}}$ (N_S)[1)];

— all relevant pairing keys of the motion sensor are not encrypted, K_P[1)];

— all relevant versions of e_K (K_P), encrypted with the master key of the related version[1)].

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 recording equipment. A unique session key is generated during the pairing. The session key is different from the pairing key.

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

— motion sensor type is not encrypted;

— date of production of the motion sensor is not encrypted;

— operating system identifier of the motion sensor is not encrypted;

— security identifier of the motion sensor (type of processor used) is not encrypted;

— type approval number of the motion sensor is not encrypted;

— name of the motion sensor manufacturer is not encrypted.

7.3 Instructions

Instruction numbers shall be in accordance with Table 7.

Table 7 — Instruction numbers

Instruction-number	Recording equipment 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

[a] No response to the request except the acknowledge is awaited.

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

[c] The data bytes shall not be encrypted.

[d] See Table 17.

[e] See Table 29 and Table 30.

Key

x motion sensor manufacturer specific

1) For the implementation further specification is needed, which is not in the scope of this document.

Table 7 *(continued)*

Instruction-number	Recording equipment 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
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
51 to 59	4	1	x	2	1	x	x	x	x	x
70	4	1	8 [b]	2	1	[a]	[a]	[a]	[a]	8 400
71 to 79	4	1	x	2	1	x	x	x	x	x
80	4	1	0	2	1	4	0	8 [b]	2	30
130 to 159	4	1	x	2	1	x	x	x	x	x

[a] No response to the request except the acknowledge is awaited.

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

[c] The data bytes shall not be encrypted.

[d] See Table 17.

[e] See Table 29 and Table 30.

Key

x motion sensor manufacturer specific

7.4 Initialisation of communication between motion sensor and recording equipment

7.4.1 General

The recording equipment initiates a pairing process, and the motion sensor responds to the recording equipment by the interchange of pairing data.

7.4.2 Necessary sequence of instruction for pairing

7.4.2.1 Overview

Table 8 specifies the details of the sequence of the instruction necessary for pairing.

Table 8 — Sequence of instructions for pairing

Recording equipment instructions	Direction of data transfer	Motion sensor	Remark
40	→		Initialises pairing
	←	Acknowledge	See 7.1.2.2.
	←	Response	The motion sensor sends its serial number N_S.
41	→		The recording equipment sends the extended serial number of the sensor encrypted with the identification key.
	←	Acknowledge	See 7.1.2.2.
	←	Response	If the recording equipment is authorised, the sensor returns the pairing key encrypted with the master key.
42	→		The recording equipment sends the session key, encrypted with the pairing key.

Table 8 *(continued)*

Recording equipment instructions	Direction of data transfer	Motion sensor	Remark
	←	Acknowledge	See 7.1.2.2.
43	→		The recording equipment sends the pairing information, encrypted with the pairing key.
	←	Acknowledge	See 7.1.2.2.
50	→		Request for authentication
	←	Acknowledge	See 7.1.2.2.
	←	Response	The sensor sends the pairing information encrypted with the session key.

7.4.3 Pairing initialisation of recording equipment and motion sensor

7.4.3.1 Initialisation message

The recording equipment shall initialise the pairing by transmitting instruction No. 40 to the motion sensor (see Table 9).

Table 9 — Initialisation message

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

7.4.3.2 Response message from the motion sensor to the recording equipment

On receiving the instruction No. 40 message, the motion sensor shall send the extended serial-number of the motion sensor as shown in Table 10 as not encrypted response message.

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

Table 10 — Structure of response message to instruction No. 40

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

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 recording equipment to motion sensor.

7.4.4.2 Request message

The recording equipment shall encrypt the extended serial number of the motion sensor, using the identification key and transmit it to the motion sensor with instruction No. 41 as shown in Table 11. The content of data bytes on the data line shall be $e_{K_{ID}}$ (N_S).

Table 11 — Message "Instruction No. 41 — Transmission of encrypted extended serial number"

Sync	Target	STX	Length	Instruction No.	Extended serial number of motion sensor encrypted with identification key			ETX	LRC
192	0	2	23	41	Byte 0	.....	Byte *n*-1	3	x

7.4.4.3 Response message

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 recording equipment 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 recording equipment. The content of data bytes on the data line, as shown in Table 12, shall be e_K (K_P).

NOTE For the implementation further specification is needed, which is not in the scope of this document.

Table 12 — Response message "Instruction No. 41 — Transmission of pairing key to the recording equipment"

Sync	Target	STX	Length	Session key encrypted with master key						ETX	LRC
192	1	2	N[a]	Byte 0	Byte 1	Byte 2	Byte 3	.....	Byte *n*-1	3	x

[a] Variable length, depending on the used cypher suite (session key length).

7.4.5 Transmission of session key from recording equipment to motion sensor

7.4.5.1 Request

The recording equipment shall send the session key encrypted with the pairing key (see Table 13) and shall transmit it with instruction No. 42 to the motion sensor.

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 initialisation. The content of data bytes on the data line shall be e_{K_P} (K_S).

NOTE For the implementation further specification is needed, which is not in the scope of this document.

Table 13 — Structure of instruction No. 42 — Transmission of session key to motion sensor

Sync	Target	STX	Length	Instruction No.	Session key encrypted with pairing key						ETX	LRC
192	0	2	N[a]	42	Byte 0	Byte 1	Byte 2	Byte 3	.....	Byte *n*-1	3	x

[a] Variable length, depending on the used cypher suite (session key length).

7.4.6 Transmission of pairing information from recording equipment to motion sensor

7.4.6.1 Request

The recording equipment encrypts the pairing information with the pairing key and shall transmit it with the instruction No. 43 to the motion sensor (see Table 14).

The motion sensor decrypts the pairing information 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_{K_P} (P_D).

Table 14 — Transmission of pairing information to motion sensor

Sync	Target	STX	Length	Instruction No.	Pairing information encrypted with pairing key					ETX	LRC
192	0	2	39	43	Byte 0	Byte 1	Byte 2	Byte 3	.....	3	x

7.4.7 Request from recording equipment for pairing information and authentication to motion sensor

7.4.7.1 Request message

The recording equipment shall request the motion sensor for pairing information and authentication using instruction No. 50 to the motion sensor as shown in Table 15.

Table 15 — Request message for authentication to motion sensor

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

The recording equipment 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 recording equipment is correct and that the motion sensor is using the correct session key.

7.4.7.2 Response message from motion sensor to recording equipment

The motion sensor shall respond by submitting the pairing information as shown in Table 16. The contents of data bytes on the data line shall be e_{K_S} (P_D).

Table 16 — Response message "Instruction No. 50 — Request for authentication to motion sensor"

Sync	Target	STX	Length	Paring information encrypted with the session key					ETX	LRC
192	1	2	38	Byte 0	Byte 1	Byte 2	Byte 3	.....	3	x

7.5 Communication of motion sensor and recording equipment in regular use

7.5.1 Sequence of instruction for communication in regular use

Table 17 specifies the communication in regular use and the sequence of the instruction numbers.

Table 17 — Sequence of instruction numbers for communication in normal use

Recording equipment	Direction of data transfer	Motion sensor	Remark
70	→		The recording equipment sends authentication data to the motion sensor.
	←	Acknowledge	See 7.1.3.
80	→		The recording equipment sends request for response to the motion sensor.

Table 17 *(continued)*

Recording equipment	Direction of data transfer	Motion sensor	Remark
	←	Acknowledge	See 7.1.3.
	←	Response	If the recording equipment is authorized, the motion sensor sends authentication and sensor data to the recording equipment.

7.5.2 Latch of counter value and encrypt data

7.5.2.1 Request message

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

7.5.2.2 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 specified in Table 18, shall be e_{K_S} (D_A).

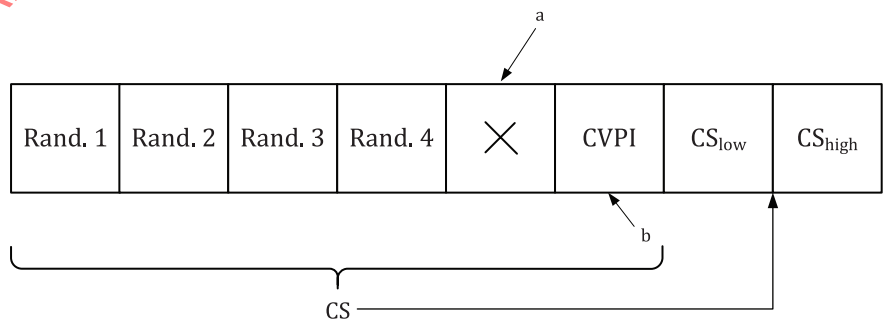
Table 18 — Latch counter value and encrypt data

Sync	Target	STX	Length	Instruction No.	Authentication data 8 byte (4 byte random number and 4 byte control information)[a] encrypted with session key					ETX	LRC
192	0	2	23	70	Byte 0	Byte 1	Byte 2	Byte 3	..... Byte *n*-1	3	x

[a] See Figure 10.

7.5.2.3 Authentication data after decryption

The motion sensor may check that no information is lost since the reception of the last instruction by means of the check value CVPI, as specified in Figure 10. 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 recording equipment when the communication is started the very first time after pairing of recording equipment and motion sensor.



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

[b] Instruction No.10 or No. 70: CVPI shall be set to the CS_{low} of the previous instruction (instruction No. 10 or No. 70) XORed with the low byte of the latched counter value (previously latched counter value of the last command 70).

Figure 10 — Structure of authentication data after decryption

7.5.3 Transmission of encrypted data

7.5.3.1 Request

The request from the recording equipment to the motion sensor shall be as shown in Table 19 with instruction No. 80.

Table 19 — Initialisation message

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

7.5.3.2 Response

The response to instruction No. 80 submitted from the motion sensor to the recording equipment shall be as shown in Table 20.

The data (see Table 20) shall be transmitted encrypted with the session key. Only Sync, Target, STX, Length, ETX and LRC shall be transmitted as not encrypted. The meaning of encrypted data shall be as shown in Table 20. The contents of data bytes on the data line shall be e_{K_S} (D_S).

Table 20 — Structure of response to instruction No. 80

Sync	Target	STX	Length	Paring information encrypted with the session key						ETX	LRC
192	1	2	22	Byte 0	Byte 1	Byte 2	Byte 3	.....	Byte 16	3	x

7.5.3.3 Encrypted data after decryption

The structure of encrypted data after decryption shall be as shown in Table 21.

Table 21 — Structure of data after decryption

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 $\oplus^a$ Serno. 1	Rand. 2 $\oplus$ Serno. 2	Rand. 3 $\oplus$ Serno. 3	Rand. 4 $\oplus$ Serno. 4	LSB	MSB	MF

[a] Bitwise XOR.

7.5.3.4 MF byte

The MF byte, as shown in Table 22, 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 recording equipment has received its response to the instruction 11 file number 0. The mechanism of detection shall be as shown in Figure 10, where byte CVPI shows that the authenticated recording equipment had accepted the message.

Table 22 — Structure of data after decryption

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.

7.5.3.5 Counter value

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

7.5.3.6 Duty cycle

The structure of the duty cycle shall be as shown in Table 23, 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 recording equipment (see, too, Figure 10).

Table 23 — Structure of byte duty cycle

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

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 24.

Table 24 — Sequence of instruction for reading information

Recording equipment	Direction	Motion sensor	Remark
10	→		The recording equipment sends authentication data and the number of the requested file to the motion sensor.
	←	Acknowledge	See 7.1.2.2.
11	→		The recording equipment sends request for response to the motion sensor.
	←	Acknowledge	See 7.1.2.2.
	←	Response	If the recording equipment is authorised, the motion sensor sends authentication and requested data to the recording equipment.

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 25.

Table 25 — Timing P6

File no.		0	1	2	3	4	5	6	7 to 19 [a]
Time P6	ms	12 600	12 600	21 000	21 000	12 600	12 600	12 600	[a]
[a] Motion sensor manufacturer specific.									

7.6.2.2 Request

The request for selected data by the recording equipment to the motion sensor shall be as shown in Table 26.

Table 26 — Structure of instruction No. 10 — Request for motion sensor information

Sync	Target	STX	Length	Instruction No.	Authentication data 8 byte (4 byte random number and 4 byte control information)[a] encrypted with session key						ETX	LRC
192	0	2	23	10	Byte 0	Byte 1	Byte 2	Byte 3	.....	Byte 16	3	x
[a] See Figure 10.												

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 NARA is 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_{K_S} (D_A).

7.6.3 General message structures

7.6.3.1 Request

A request of the recording equipment to the motion sensor shall be as shown in Table 27 with instruction No. 11.

Table 27 — Structure of instruction No. 11

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

7.6.3.2 Response

A response to instruction No. 11 of the motion sensor to the recording equipment shall be as shown in Table 28.

Table 28 — Structure of a response to instruction No. 11

Sync	Target	STX	Length	Data for authentication number for selected file checksum over all data					Data of selected file[a]									ETX	LRC
192	1	2	a	B0[b]	B1	...	B6	B7	B0	B1	B2	B3	B4	B5	B6	B7	...	3	x

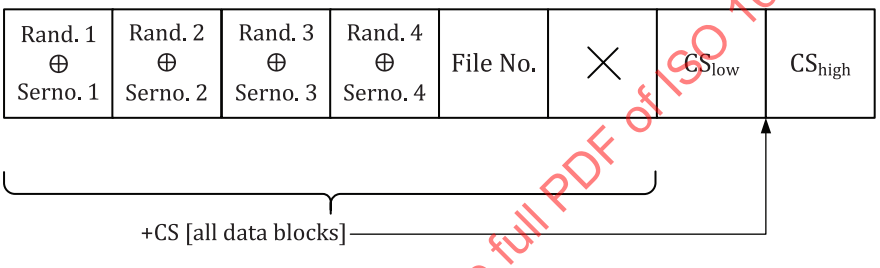
[a] For number of bytes see Table 29.

[b] Byte x.

The meaning of the several files and how to read them is explained in Table 29 and Table 30. The sequence of instruction Nos. 10 and 11 gives the recording equipment not only the possibility to read error messages, but also to get additional information (see Table 29).

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

See Figure 11.



Key

⊕ Bitwise XOR

Figure 11 — Structure of data for authentication — Response from motion sensor

7.6.4 Data block chaining

NOTE For the implementation further specification is needed, which is not in the scope of this document.

7.6.5 Structures of selected data

7.6.5.1 Guide to the data bytes

Table 29 specifies the data bytes depending on the number of the files which are involved. All information shall be encrypted with the session key.

Table 29 — Guide to the data bytes

Identification File No.	Number of data bytes [a]		Length	Description
	Data for authentication	Data of selected file		
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 30)
1	8	8	22	The operating system identifier of the motion sensor (see Table 31)

NOTE More information about the meaning of the data depending on the selected file is given in Tables 30 to 36.

[a] See Table 28.

[b] Motion sensor manufacturer specific.