# KITAS 2171 v.1.11
# Digital Tachograph - Motion Sensor

**Autor:** Dr. Marion Grüner (I CVAM TCO LRH)

**Revision:** 1.5

**Status:** Released

**Datei:** 2171.70.014.00_EAD_000_AB.doc
Datei PVCS verwaltet

| Designed by | Date | Department | Released by | Date | Department |
|---|---|---|---|---|---|
| Marion.gruener@continental-corporation.com | 2011-01-10 | I CVAM TTS LRH | Winfried.rogenz@continental-corporation.com | 2011-01-10 | I CVAM TTS LRH |

| | | |
|---|---|---|
| Continental | Designation<br>KITAS 2171<br>KITAS 2171 | Released<br>Rev. 1.5 |
| | Documentkey<br>2171.70.014.00_EAD_000_AB | Pages<br>1 / 42 |
| Continental Automotive GmbH | | |

# 1 History

| Revision | Datum | Autor, Bearbeiter | Anlass |
|---|---|---|---|
| 01.10.00 | 06.10.1999 | SV IC43LM/ZU Winfried Rogenz | Erstausgabe |
| 1.0 | 22.08.2003 | SV I CV PD FF Thomas Grill | Nachtrag 2: Re-Zertifizierung KITAS 2171 - IT-Sicherheitszertifikat<br>Dateiname Security Target für KITAS "Security Target-2171.doc" in 2171.70.014.00_EAD_000_AA.doc geändert.<br>Neue Dokumentenvorlage SV verwendet.<br>DTCO 1380 geändert in DTCO 1381.Änderungen / Ergänzungen zu Objects<br>Referenzliste zu Security Targets Verordnung (EG) 1360/2002 Anhang I B Anlage 10 |
| 1.1 | 19.02.2004 | SV I CV PD TS Thomas Grill | "ISO 16844-3, Clarification proposal" - Definition Pairinginformation ergänzt |
| 1.2 | 16.11.2009 | I CVAM TCO LRH Dr. Marion Grüner | Verwendung der Dokumentenvorlage von<br>Continental<br>Dateiname in 2171.70.014.00_EAD_00_AB.doc geändert<br>Hinzufügen der Änderungshistorie<br>Anpassung des Rationale an die gesetzliche Vorgabe des Anhang 12 der Verordnung (EG) 68/ 2009 |
| 1.3 | 10.12.2009 | I CVAM TCO LRH Dr. Marion Grüner | Änderungen aus Review mit Herrn Rogenz wurden eingearbeitet |
| 1.4 | 27.04.2010 | I CVAM TCO LRH Dr. Marion Grüner | Änderungen aus Review von Hr. Dr. Furgel eingearbeitet, Hinweise von Hr Kocar zum TOE(Punkt 5.2 und Literaturverzeichnis) am 14.12.2010 eingearbeitet( Datum und Revionsstand bleiben erhalten) |
| 1.5 | 10.01.2011 | I CVAM TCO LRH Dr. Marion Grüner | Änderung aus Review von Hr. Kocar (BSI) und Hr. Vollstädt ( T-Systems) vom 10.01.2011:<br>Kapitel „Produkt Rationale“ wird der Satz wie folgt angepasst:<br>The Commission regulation (EU) No.1266/2009 describes new functionality for the motion sen-sor ~~which has no impact on the security functions of the motion sensor~~. |

## 2 List of contents

# 3 Introduction

This document contains a description of the motion sensor KITAS 2171v.1.11, of the threats it must be able to counteract and of the security objectives it must achieve. In the following the KITAS 2171 v.1.11 is mentioned as KITAS 2171. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

This document is based on the Motion Sensor Generic Security Target, which is described in Appendix 10 and Appendix 11 [1] of Annex 1B of the European Regulation (EEC) No 3821/85 [2] amended by the COMMISSION REGULATION (EC) No 1360/2002 [3] .The document states the security functions and assumptions on the environment and describes how they are implemented in the motion sensor KITAS 2171.

Requirements referred to in the document, are those of the body of Annex 1B. For clarity of reading, duplication sometimes arises between Annex 1B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex 1B body requirement referred by this security target requirement, the Annex 1B body requirement shall prevail.

Annex 1B body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

# 4 Abbreviations and definitions

## 4.1 Abbreviations

| | |
|---|---|
| **DTCO** | Digital Tachograph |
| **e** | encrypted |
| **K** | Master key |
| $\mathbf{K_{ID}}$ | derived Master key - identification key |
| $\mathbf{K_p}$ | sensor-specific pairing key |
| $\mathbf{K_s}$ | session key |
| **KITAS** | Kienzle Tachograph Sensor |
| $\mathbf{N_s}$ | Extended Serial-Number |
| **ROM** | Read Only Memory |
| **SEF** | Security Enforcing Function |
| **TBD** | To Be Defined |
| **TOE** | Target Of Evaluation |
| **VU** | Vehicle Unit |

## 4.2 Definitions

Adaptor

“adaptor” means: a part of the recording equipment, providing a signal permanently representative of vehicle speed and/or distance travelled, and which is:

— installed and used only in M1 and N1 type vehicles

(as defined in Annex II to Council Directive 70/156/EEC) put into service for the first time between 1 May 2006 and 31 December 2013,

— installed where it is not mechanically possible to install any other type of existing motion sensor which is otherwise compliant with the provisions of this Annex and its Appendixes 1 to 11,

— installed between the vehicle unit and where the speed/distance impulses are generated by integrated sensors or alternative interfaces.

Digital Tachograph

Recording Equipment

Entity

A device connected to the motion sensor. (specific definition see S1:)

Motion data

The data exchanged with the VU, representative of speed and distance travelled. (specific definition see O1:)

Motion Sensor
Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.

Physically separated parts
Physical components of the motion sensor that are distributed in the vehicle as opposed to physical components gathered into the motion sensor casing.

Recording Equipment
The total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers.

Security data
The specific data needed to support security enforcing functions (e.g. crypto keys). (specific definition see O9:, O11:)

System
Equipment, people or organisations, involved in any way with the recording equipment.

User
A human user of the motion sensor (when not used in the expression “user data”). (specific definition see S2:)

User data
Any data, other than motion or security data, recorded or stored by the motion sensor. (specific definition see O2:, O3:, O4:, O5:, O6:, O7:, O8:)

Vehicle Unit
The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.

# 5 Product rationale

## 5.1 Motion sensor description and method of use

The motion sensor is intended to be installed in road transport vehicles. Its purpose is to provide a VU with secured motion data representative of vehicle's speed and distance travelled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement can be representative of vehicle's speed or distance travelled. It may be located in the vehicle's gear box or in any other part of the vehicle.

In its operational mode, the motion sensor is connected to a VU.

It may also be connected to specific equipment for management purposes. In the case of the KITAS 2171 motion sensor it will only be connected to specific equipment during the manufacturing process to initialise the device. In the field no specific equipment will be connected. Also workshops will not perform any management or repair operations but replace a faulty motion sensor by a new one.

A type approved motion sensor (according to the provisions of the Annex IB, section VIII – Type approval of recording equipment and tachograph cards) shall be fitted into the adaptor housing, which shall also include a pulse converter device inducing the incoming pulses to the embedded motion sensor. The embedded motion sensor itself shall be connected to the VU, so that the interface between the VU and the adaptor shall be compliant with the requirements set out in ISO 16844-3 (req. ADA_002 of the Council regulation (EC) no. 68/2009).[4]

The adaptor is only intended for those vehicles that are required to be equipped with recording equipment in compliance with this Regulation. It shall be installed and used only in those types of vehicle defined under (rr) [a], where it is not mechanically possible to install any other type of existing motion sensor which is otherwise compliant with the provisions of this Annex and its Appendixes 1 to 11. The adaptor shall not be mechanically interfaced to a moving part of the vehicle, as required by Appendix 10 of Annex IB (section 3.1), but connected to the speed/distance impulses which are generated by integrated sensors or alternative interfaces

The Commission regulation (EU) No.1266/2009 describes new functionality for the motion sensor. [5]

[a] (rr) is the definition for the adaptor. The description is found under point 4.2 definitions of this document.

## 5.2 Delivery of the TOE

| No | Type | Description | Version | Date | Type of delie-very |
|---|---|---|---|---|---|
| 1 | Hardware Motion Sensor | Motion sensor KITAS 2171 Version 1.11 | V1.11 | | Hardware |
| 2 | Software | COP08 | V1.09 | | Software |
| 3 | Software | 2. Microcontroller (with dynamic und static detection of the magnet maniputaion) | V2.0 | | Software |
| 4 | Documentation | KITAS 2171 Weg- und Geschwindigkeitsgeber – Installationsbeschreibung, Version 1.3, Continental Automotive GmbH, 26.03.2010 | V1.3 | | as paper |

The typical motion sensor is described in the following figure:

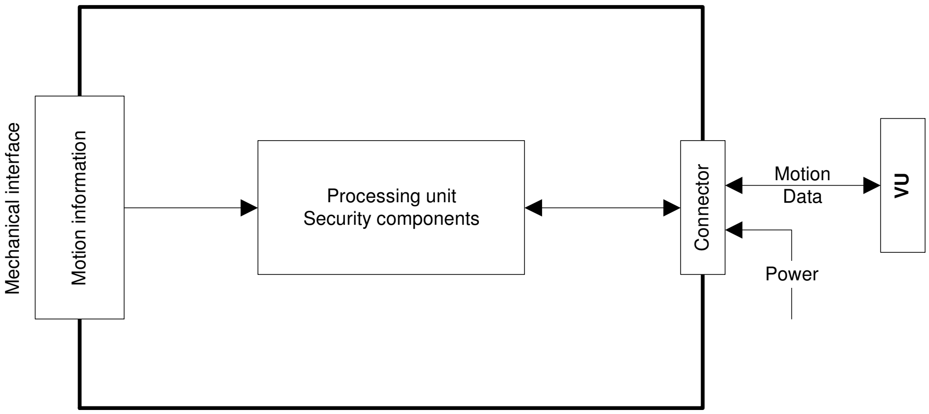

*Figure 1 Typical motion sensor*

The following figure shows the basic architecture of the actual TOE, the motion sensor KITAS 2171 (**KI**enzle **TA**chograph **S**ensor) and of the vehicle unit of the DTCO (**D**igital **T**a**C**h**O**graph).

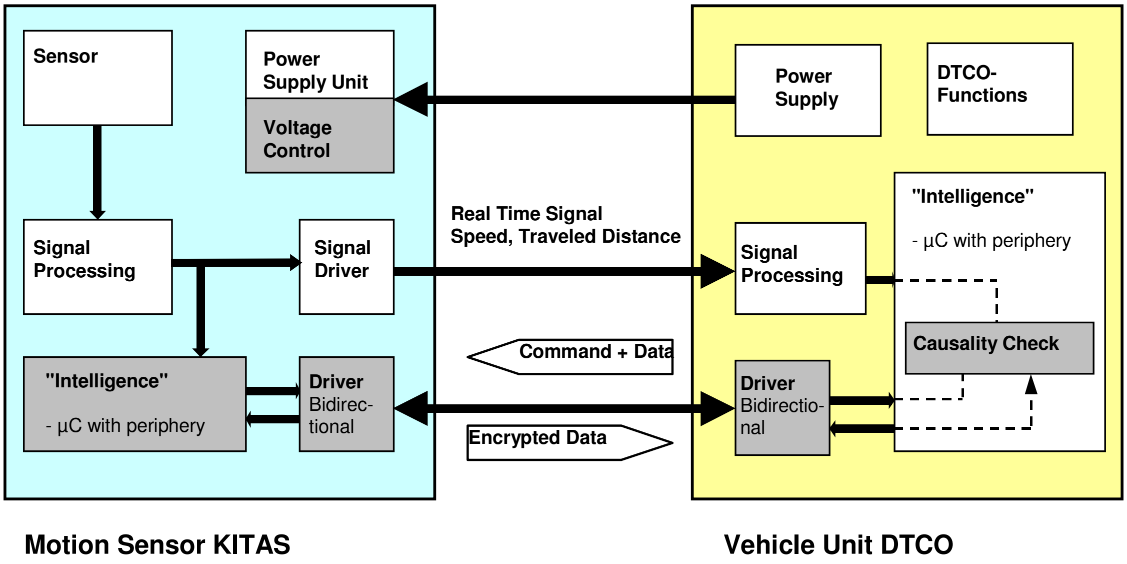

*Figure 2 Actual TOE KITAS 2171.*

There is a microcontroller integrated in the motion sensor KITAS 2171.xx. One of the two signalling channels carries the sensor signal (speed, travelled distance) to the DTCO in real time. The other one acts as a bi-directional channel. The distance signal is added to an impulse counter in both the motion sensor and the DTCO.

The value of the impulse counter in the motion sensor KITAS 2171 is transmitted encrypted on a periodic request of the DTCO. It is decrypted and checked for equality in the DTCO. A deviation is interpreted as manipulation. The DTCO acts as master and controls the integrity/completeness of the plaintext signal.

The KITAS motion sensor has been equipped with cryptographic functions for data transfer. In this context the standardised procedure Triple-DES (Data Encryption Standard) with 2 keys is used.

Authentication information for an unequivocal assignment between the KITAS motion sensor and the DTCO is stored during the initialisation phase. The authenticity of signals transferred over the bi-directional channel is proved with this information.

Cases of manipulation of the power supply or one of the two signalling channels are detected by the system. A substitution of the motion sensor is also detected, since the DTCO and the KITAS motion sensor are unequivocally assigned during the initialisation phase.

The real time signal (speed and travelled distance) itself is being transferred in plaintext, since there are no requirements for confidentiality of the signal itself.

The physical construction of the motion sensor KITAS is of a way that opening the KITAS box isn't possible without destroying it. This way a manipulation gets obvious. Furthermore the motion sensor is sealed at the gearbox.

The transmission protocol is defined and explained in [6, 8].

The commands which are necessary for production, installation in the vehicle, and during operation (transmission of the real time signal and transmission of encrypted data) are included.

## 5.3 Motion sensor life cycle

The life cycle of the motion sensor KITAS 2171 is described in the following figure:

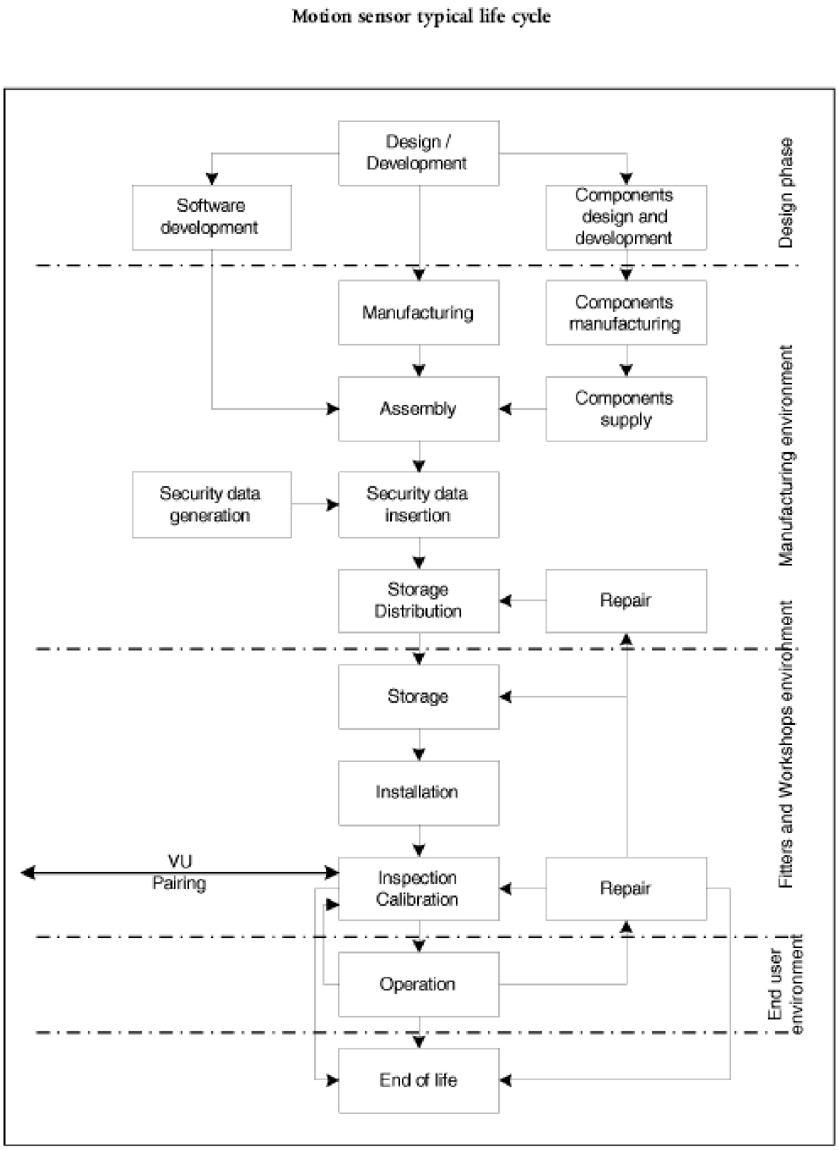

*Figure 3 Motion sensor KITAS 2171 life cycle*

The repair of a motion sensor KITAS 2171 in the field is not possible. The fitters and workshops are only replacing a faulty motion sensor by a functional motion sensor.

## 5.4 Subjects, objects, and access modes/actions

### 5.4.1 Subjects

For the motion sensor KITAS 2171 the following types of **subjects** exist:

**S1: Entities:**

S1.1: Installation device in the manufacturing process for storing objects O3:, O6:, O7:, O8:, O9: in the non volatile memory of the motion sensor

S1.2: vehicle unit in pairing and operational mode with the motion sensor

**S2: Users:**

S2.1: Drivers and co-drivers (in operational mode)

S2.2: Workshop staff , fitters and staff of vehicle manufacturers (in calibration mode)

S2.3: Control officers from national control authorities (in control mode)

S2.4: Staff of the respective haulage company (in company mode)

***Note:*** The human users S2.1: to S2.4: of the recording equipment in road transport vehicles. are subjects of the vehicle unit in the tachograph system and have not direct access to the motion sensor. They will access it indirectly through the vehicle unit only. So any authentication and access control function for those users is performed by the vehicle unit. The motion sensor itself does not need to know which human user currently accessing the system.

### 5.4.2 Objects

For the specification of the security functions of the motion sensor KITAS 2171 the following objects are relevant. Definitions of data objects are provided in the Appendix 1[7] of Annex 1B

**O1: motion data representative of vehicle's speed and distance travelled:**

O1.1: impulses (real time signal)

O1.2: impulse counter

**O2: Data of file No. 0 (Error messages for audit records)**

O2.1: actual random number

O2.2: kind of error (EEPROM error, authentication failure, self testing errors ...) for audit records

**O3: Data of file No. 1 (Operating system identifier)**

O3.1: SensorOSIdentifier (Identifier of the operating system – Firmware version - of the motion sensor)

**O4: Data of file No. 2 (First pairing information)**

O4.1: SensorPairingDateFirst

O4.2: firstVUApprovalNumber

O4.3: firstVUSerialNumber

Note:

Instead of clear text the data of first pairing information are encrypted with the derived key of pairing key XOR concatenated value of extended serial-number and extended serial-number.

The data of first pairing information = $e_{(Kp\ XOR\ (Ns\ ||\ Ns))}$ { Random || SensorPairingDateCurrent || CurrentVUApprovalNumber || CurrentVUSerialNumber}. [8]

**O5: Data of file No. 3 (Current pairing information)**

O5.1: SensorPairingDateCurrent

O5.2: CurrentVUApprovalNumber

O5.3: CurrentVUSerialNumber

Note:

Instead of clear text the data of the current pairing information are encrypted with the derived key of pairing key XOR concatenated value of extended serial-number and extended serial-number.

The data of current pairing information = $e_{(Kp\ XOR\ (Ns\ ||\ Ns))}$ { Random || SensorPairingDateCurrent || CurrentVUApprovalNumber || CurrentVUSerialNumber}. [8]

**O6: Data of file No. 4 (Extended serial number $N_s$)**

O6.1: SerialNumber (Serial number for the motion sensor, unique for the manufacturer, the type and the month below)

O6.2: monthYear (Date of production)

O6.3: type (type of the motion sensor)

O6.4: manufacturerCode (numerical code of the manufacturer of the equipment)

**O7: Data of file No. 5 (Security identifier)**

O7.1: SensorSCIdentifier (Identifier of the security component - processor part-type - of the motion sensor)

**O8: Data of file No. 6 (Approval number)**

O8.1: SensorApprovalNumber (type approval number of the sensor)

**O9: Security data to be stored in the motion sensor**

O9.1: $K_p$ (sensor specific pairing key)

O9.2: $e_{KID}$(Ns) (extended serial number of the motion sensor encrypted with the derived Master key – identification key)

O9.3: $e_K(K_p)$ (sensor specific pairing key encrypted with the Master key)

**O10: Security data to generate and to be stored in the motion sensor**

O10.1: $K_s$ (session key)

**O11: Security data not stored in the motion sensor**

O11.1: K (Master key), $K_{ID}$ (derived Master key – identification key) [6]

### 5.4.3 Access modes

Actions and access to objects are only possible when the motion sensor is connected to an entity. Only the entity has access to the motion sensor and provides the communication between both entities. For the entities the following types of actions and access modes exist:

- installation device in the manufacturing process
  - write the motion sensor identification data (O3:, O6:, O7:, O8:) and security data (O9:)
- vehicle unit in pairing mode
  - generate a session key (O10:)
  - write the motion sensor installation data (O4:, O5:)
- vehicle unit in operational mode
  - write/send messages
  - receive/read messages (O1:, O2:)

The Table 1 describes the access rights.

| | **O1:** | **O2:** | **O3:** | **O4:** | **O5:** | **O6:** | **O7:** | **O8:** | **O9:** | **O10:** |
|---|---|---|---|---|---|---|---|---|---|---|
| **S1.1:** | | | **w**<br>**(once)** | | | **w**<br>**(once)** | **w**<br>**(once)** | **w**<br>**(once)** | **w**<br>**(once)** | |
| **S1.2:**<br>pairing mode | | | | **w** **(once)**<br>**/r** | **w/r** | **r** | | | **u** | **g** |
| **S1.2:**<br>operational mode | **r** | **r** | **r** | **r** | **r** | **r** | **r** | **r** | | **u** |

r = read; w = write; g = generate, u = use

*Table 1 Access rights*

### 5.5 Threats

This paragraph describes the threats the motion sensor may face.

#### 5.5.1 Threats to access control policies

T.Access — Users could try to access functions not allowed to them.

#### 5.5.2 Design related threats

T.Faults — Faults in hardware, software, communication procedures could place the motion sensor in unforeseen conditions compromising its security.

T.Tests — The use of non invalidated test modes or of existing back doors could compromise the motion sensor security.

T.Design — Users could try to gain illicit knowledge of design either from manufacturer’s material (through theft, bribery, …) or from reverse engineering.

### 5.5.3 Operation oriented threats

T.Environment Users could compromise the motion sensor security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,…).

T.Hardware Users could try to modify motion sensor hardware.

T.Mechanical_Origin Users could try to manipulate the motion sensor input (e.g. unscrewing from gearbox, …).

T.Motion_Data Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).

T.Power_Supply Users could try to defeat the motion sensor security objectives by modifying (cutting, reducing, increasing) its power supply.

T.Security_Data Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.

T.Software Users could try to modify motion sensor software.

T.Stored_Data Users could try to modify stored data (security or user data).

## 5.6 Security objectives

The main security objective of the digital tachograph system is the following:

O.Main The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

Therefore the security objective of the motion sensor, contributing to the global security objective, is:

O.Sensor_Main The data transmitted by the motion sensor must be available to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance travelled.

## 5.7 Information Technology Security Objectives

The specific IT security objectives of the motion sensor contributing to its main security objective, are the following:

O.Access The motion sensor must control connected entities' access to functions and data.

O.Audit The motion sensor must audit attempts to undermine its security and should trace them to associated entities.

O.Authentication The motion sensor must authenticate connected entities.

O.Processing The motion sensor must ensure that processing of input to derive motion data is accurate.

O.Reliability The motion sensor must provide a reliable service.

O.Secured_Data_Exchange The motion sensor must secure data exchanges with the VU.

## 5.8 Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the motion sensor.

### 5.8.1 Equipment design

M.Development Motion sensor developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

M.Manufacturing Motion sensor manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the motion sensor is protected from physical attacks which might compromise IT security.

### 5.8.2 Equipment delivery

M.Delivery Motion sensor manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor is done in a manner which maintains IT security.

### 5.8.3 Security data generation and delivery

M.Sec_Data_Generation Security data generation algorithms must be accessible to authorised and trusted persons only.

M.Sec_Data_Transport Security data must be generated, transported, and inserted into the motion sensor, in such a way to preserve its appropriate confidentiality and integrity.

### 5.8.4 Recording equipment installation, calibration, and inspection

M.Approved_Workshops Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.

M.Mechanical_Interface Means of detecting physical tampering with the mechanical interface must be provided (e.g. seals)

M.Regular_Inpections Recording equipment must be periodically inspected and calibrated.

### 5.8.5 Law enforcement control

M.Controls Law enforcement controls must be performed regularly and randomly, and must include security audits.

### 5.8.6 Software upgrades

| | |
|---|---|
| M.Software_Upgrade | Software revisions must be granted security certification before they can be implemented in a motion sensor. |

# 6 Security enforcing functions

## 6.1 Identification and authentication

UIA_101 The motion sensor shall be able to establish, for every interaction, the identity of any entity it is connected to.

### *6.1.1 Implementation within the motion sensor KITAS 2171*

<SF1>: The motion sensor KITAS 2171 performs an initial authentication of the VU during the pairing process. Authentication is performed by proofing knowledge of a common secret (O11.1:K (Master key), $K_{ID}$ (derived Master key – identification key)) between the motion sensor and the vehicle unit. During the pairing process a new secret common (O10.1:$K_s$ (session key)) only to the vehicle unit and the motion sensor that performed the pairing is established. This new secret is than used as the encryption key in the communication in the operational mode between the two entities and thereby also is used as the mechanism to authenticate and establish the identity of the vehicle unit to the motion sensor. Any data (motion data (O1.2:) and user data (O2: to O8:) transferred from the motion sensor is thereafter encrypted using this key, so only the authorised vehicle unit is able to decrypt the information, i. e. has access to it. Forging or copying of authentication data is prohibited because they are stored securely in the motion sensor and the vehicle unit and cryptographically protected when they are transferred.

UIA_102 The identity of a connected entity shall consist of:

- an entity group:
  - VU,
  - Management device,
  - Other,
- an entity ID (VU only).

UIA_103 The entity ID of a connected VU shall consist of the VU approval number and the VU serial number.

### *6.1.2 Implementation within the motion sensor KITAS 2171*

<SF2>: The identity ID is exchanged during the pairing process. The entity ID (O5.2:, O5.3:) is stored by the motion sensor in its EEPROM.

The data related to the first (O4:) and the current (O5:) pairing are stored in the files with the numbers 2 and 3. Pairing data includes the date and time of the pairing as well as the VU approval number and the VU serial number (the entity ID).

A management device and other devices do not exist for the motion sensor KITAS 2171 and so only the entity group VU is available.

UIA_104 The motion sensor shall be able to authenticate any VU or management device it is connected to:

- at entity connection,
- at power supply recovery

*6.1.3 Implementation within the motion sensor KITAS 2171*

<SF3>: At entity connection it is necessary to start the pairing process. The actions for authentication are described in section 6.1.1. At power supply recovery a reset is indicated to the VU and a synchronisation process between motion sensor KITAS 2171 and VU is initiated. The authentication is performed as described in section 6.1.4.

UIA_105 The motion sensor shall be able to periodically re-authenticate the VU it is connected to.

UIA_106 The motion sensor shall detect and prevent use of authentication data that has been copied and replayed.

*6.1.4 Implementation within the motion sensor KITAS 2171*

<SF4>: Every request to the motion sensor KITAS 2171 contains a check with authentication data. This authentication data consists of an encrypted field (with O10.1:$K_s$ (session key)) that contains a random number and a check sum of this random number. The entity is authenticated only if this data has been formatted correctly. The authentication data consists further of an check_value of the previous instruction, which depends on the latched impulscounter O1.2 and the authentication data of the previous instruction.

<SF5>: Every motion sensor KITAS 2171 has only one authorised entity (VU) at a given time.

UIA_107 After (*TBD by manufacturer and not more than 20*) consecutive unsuccessful authentication attempts have been detected, the SEF shall:

- Generate an audit record of the event,
- warn the entity,
- continue to export motion data in a non secured mode.

*6.1.5 Implementation within the motion sensor KITAS 2171*

<SF6>: The authentication process is based on symmetric encryption.

Unsuccessful authentication attempts are handled in the following way:

- the respective entity request isn’t performed;
- an error code for failed entity authentication is generated and stored in the respective data file;
- the vehicle unit is informed about the error.

## 6.2 Access control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

### 6.2.1 Access control policy

ACC_101 The motion sensor shall control access rights to function and data.

Implementation within the motion sensor KITAS 2171

<SF7>: Since there is only one authorised entity (VU) of the motion sensor at a given time there is no need differentiate between the access rights of different entities. Access control is performed on the basis of the commands that the vehicle unit is allowed to submit to the motion sensor. The motion sensor checks that the command code submitted corresponds to a valid command.

### 6.2.2 Data access rights

ACC_102 The motion sensor shall ensure that motion sensor identification data can be written once only (requirement 078).

requirement 078 of Annex 1B:

Motion sensor identification data are recorded and stored once and for all in the motion sensor, by the motion sensor manufacturer.

ACC_103 The motion sensor shall accept and/or store user data from authenticated entities only.

ACC_104 The motion sensor shall enforce appropriate read and write access rights to security data.

Implementation within the motion sensor KITAS 2171

<SF8>: The motion sensor KITAS 2171 complies data access rights to motion data, security data and user data in the way as defined in Table 1 Access rights.

The motion sensor identification data (O3:, O6:, O7: ,O8:) are written at the manufacturers site into the storage of the motion sensor KITAS 2171 and can not be changed by any entity.
There is no additional user data where the vehicle unit has access to.

### 6.2.3 File structure and access conditions

ACC_105 Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

Implementation within the motion sensor KITAS 2171

<SF9>: The file structure is defined by the control program within the TOE. So it is set up during the production process. Neither the file structure nor the access rights can altered afterwards.

<SF10>:File structure and access rights have been defined and are initialised during the manufacturing process. The file structure can not be changed hereafter.

## 6.3 Accountability

ACT_101 The motion sensor shall hold in its memory motion sensor identification data (requirement 077).

requirement 077 of Annex 1B:

The motion sensor shall be able to store in its memory the following identification data:

- name of the manufacturer,
- part number,
- serial number,
- approval number,
- embedded security component identifier (e.g. internal chip/processor part number),
- operating system identifier (e.g. software version number).

ACT_102 The motion sensor shall store in its memory installation data (requirement 099).

requirement 099 of Annex 1B:

The motion sensor shall record and store in its memory the following motion sensor installation data:

- first pairing with a VU (date, time, VU approval number, VU serial number),
- current pairing with a VU (date, time, VU approval number, VU serial number).

ACT_103 The motion sensor shall have a capability to output accountability data to authenticated entities at their request.

Implementation within the motion sensor KITAS 2171

<SF11>:The motion sensor identification data (O3:O6:O7:O8:) and installation data (O4:O5:) are stored in the EEPROM of the motion sensor. There is no function to alter the motion sensor identification data. The identifiers stored there are:

Authorised entities (VU) can read motion sensor identification data (O3:O6:O7:O8:) by issuing command No. 10 and 11 and select file No. 1,4,5 and 6.

Authorised entities (VU) can submit a request to read the motion data (O1:) with command No. 70 and 80. The motion data will then be submitted to the vehicle unit in encrypted form. The motion data is also available to the vehicle unit as well as to any unauthorised entity through the pulse lines directly connected to the vehicle unit.

Authorised entities (VU) can read motion sensor installation data (O4:O5:) related to the first and current pairing. The vehicle unit can read the pairing data by submitting command No. 10 and 11 with a request to read file No. 2 (for the data of the first pairing) or file No. 3 (for the data of the last pairing).

### 6.4 Audit

AUD_101 The motion sensor shall, for events impairing its security, generate audit records of the events.

AUD_102 The events affecting the security of the motion sensor are the following:

- security breach attempts:
  - authentication failure,

- stored data integrity error,
- internal data transfer error,
- unauthorised case opening,
- hardware sabotage.

- Sensor fault,

AUD_103 Audit records shall include the following data:

- date and time of the event,
- type of event,
- connected entity identity.

when required data is not available, an appropriate default indication shall be given (*TBD by manufacturer*).

Implementation within the motion sensor KITAS 2171

<SF12>:The motion sensor has reserved file No. 0 to collect data for audit records related to events affecting its security. These are described in Table 2 Events affecting the security

| Byte | Class of error | Event affecting the security | related SEF |
|---|---|---|---|
| 0 | NON VOLATILE MEMORY | stored data integrity error | <SF17>: |
| 1 | Controller RAM | sensor fault | <SF18>: |
| 2 | Controller-Instruction | sensor fault | <SF18>: |
| 4 | Communication | sensor fault | <SF18>: |
| 4 | Authentication (instructions 10 and 70) | authentication failure | <SF6>: |
| 5 | | | |
| 6 | Sensor Element | optional | |
| 7 | Overtemperature | optional | |

*Table 2 Events affecting the security*

An indicator for the event impairing the security of the motion sensor KITAS 2171 is stored together with event specific data. No date and time is stored because the motion sensor has no clock. The vehicle unit can submit a request to transmit the error file and than add the date and time of the event can be added to the audit log of the vehicle unit.

The security breach attempt "internal data transfer" does not apply for the motion sensor KITAS 2171, because it does not makes use of physically separated parts (see 6.5.2)

The security breach attempt "unauthorised case opening" does not apply for the motion sensor KITAS 2171, because it is not designed to be openable. (see <SF21>:).

The security breach attempt "hardware sabotage” does not apply for the motion sensor KITAS 2171 (see <SF22>:).

AUD_104 The motion sensor shall send the generated audit records to the VU at the moment of their generation, and may also store them in its memory.

AUD_105 In the case where the motion sensor stores audit records, it shall ensure that 20 audit records will be maintained independent of audit storage exhaustion, and shall have a capability to output stored audit records to authenticated entities at their request.

Implementation within the motion sensor KITAS 2171

<SF13>:An accounted error causes an entry in the motion sensors error file. The motion sensors indicates the presence of this error to the vehicle unit in the next instance of communication.

The actual TOE doesn't store audit records. This is expected to be done in the vehicle unit.

<SF14>:Since there is only one  entity at a given time all actions can be automatically related to this entity.

<SF15>:There is only room for one audit event within the TOE. The data is transferred upon request of the vehicle unit.

## 6.5 Accuracy

### 6.5.1 Information flow control policy

ACR_101 The motion sensor shall ensure that motion data may only been processed and derived from sensor mechanical input.

Implementation within the motion sensor KITAS 2171

<SF16>:The sensor, the signal processing and the "intelligence" ( see Figure 2) of the motion sensor KITAS 2171 are installed in a box designed to be not openable. The TOE is a sealed device.

### 6.5.2 Internal data transfers

The requirements of this paragraph apply only if the motion sensor makes use of physically separated parts.

ACR_102 If data are transferred between physically separated parts of the motion sensor, the data shall be protected from modification.

ACR_103 Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

Implementation within the motion sensor KITAS 2171

Since the TOE is a single protected entity, this requirements do not apply for the KITAS motion sensor.

### 6.5.3 Stored data integrity

ACR_104 The motion sensor shall check user data stored in its memory for integrity errors.

ACR_105 Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

Implementation within the motion sensor KITAS 2171

<SF17>:Active stored data integrity checks are performed within the TOE for the integrity of stored data in the RAM and EEPROM devices.

## 6.6 Reliability of service

### 6.6.1 Tests

RLB_101 All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase. It shall not be possible to restore them for later use.

RLB_102 The motion sensor shall run self-tests, during initial start-up, and during normal operation to verify its correct operation. The motion sensor self-tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).

RLB_103 Upon detection of an internal fault during self-test, the SEF shall generate an audit record (sensor fault).

Implementation within the motion sensor KITAS 2171

<SF18>:Self testing of the TOE is performed for the accuracy of arithmetic operations and for the integrity of stored data in the RAM and EEPROM devices (see <SF17>:). TOE self tests are performed during start-up, after reset, and on request (with command No. 70 and 80). Upon detection of an fault during the self test the TOE generates an error (Table 2 Events affecting the security).

There are no functions for testing purpose in the operational system. Testing is performed in the production environment and all functions related to testing are removed from the TOE.

### 6.6.2 Software

RLB_104 There shall be no way to analyse or debug the motion sensor software in the field.

RLB_105 Inputs from external sources shall not be accepted as executable code.

Implementation within the motion sensor KITAS 2171

<SF19>:The design of the KITAS software prohibits pre-emption by external commands or signals.

<SF20>:A software upgrade is performed only with the installation of a new motion sensor in the vehicle. After this a new pairing has to be done.

### 6.6.3 Physical protection

RLB_106 If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of 6 months. In such a case, the SEF shall generate an audit record of the event (It is acceptable that the audit record is generated and stored after power supply reconnection).

If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).

RLB_107 The motion sensor shall detect specified (*TBD by manufacturer*) hardware sabotage.

RLB_108 In the case described above, the SEF shall generate an audit record and the motion sensor shall: (*TBD by manufacturer*).

Implementation within the motion sensor KITAS 2171

<SF21>:The TOE is not designed to be openable. It is a sealed device and any attempt to open the device can be detected through visual inspection.

<SF22>:There are no software functions to detect hardware sabotage. The hardware is sealed so any attempt to tamper with the hardware can be detected by visual inspection.

### 6.6.4 Power supply interruptions

RLB_109 The motion sensor shall preserve a secure state during power supply cut-off or variations.

Implementation within the motion sensor KITAS 2171

<SF23>:The motion sensor KITAS 2171 contains a separated power supply unit that controls the voltage and smoothness of the power input. The internal memory and processing elements are supplied with either proper energy or are inactive. The TOE is designed in a way that each power cut-off or variation results in a reset which provides a secure state in each instance. The occurrence of a reset is indicated to the vehicle unit.

### 6.6.5 Reset conditions

RLB_110 In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the motion sensor shall be reset cleanly.

Implementation within the motion sensor KITAS 2171

<SF24>:After power reset a synchronisation process between motion sensor KITAS 2171 and vehicle unit is initiated.

### 6.6.6 Data availability

RLB_111 The motion sensor shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

Implementation within the motion sensor KITAS 2171

<SF25>:All tasks started by the TOE are initiated by request from the vehicle unit and are immediately started. The response will be generated as fast as the underlying hardware is able to execute. There are no other tasks on the system that are able to slow down the execution.

### 6.6.7 Multiple applications

RLB_112 If the motion sensor provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.

Implementation within the motion sensor KITAS 2171

The TOE does not provide any additional application other than the tachograph application when it leaves the manufactory. Functions which are used with the same product hardware but in a different environment are deactivated by the first pairing of the motion sensor KITAS 2171 with a vehicle unit.

### 6.7 Data exchange

DEX_101 The motion sensor shall export motion data to the VU with associated security attributes, such that the VU will be able to verify its integrity and authenticity.

Implementation within the motion sensor KITAS 2171

<SF26>:The TOE protects the data objects (O1:, O2:, O3:, O4:, O5:, O6:, O7:, O8:) transmitted to the VU or received from the VU by means of encryption. This prohibits read access to the data objects by unauthorised entities. Checksums as part of the encrypted data items and tests if the value of data items are within their defined ranges are used to detect unauthorised modifications during transmission. This verifies the validity of the information. The originator (vehicle unit) is authenticated by the key (i. e. only the vehicle unit knows the session key (O10.1:).

<SF27>:Evidence of origin is generated by the session key (O10.1:) that is used for encryption. Since only two parties (the motion sensor and the vehicle unit that performed the current pairing with the motion sensor KITAS 2171) know this session key, either party can authenticate the other by verifying that the correct session key has been used.

<SF28>:The motion sensor KITAS 2171 generates an acknowledgement message for each receipt command. This acknowledgement message contains an indication of the last receipt command.

### 6.8 Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer’s solutions.

CSP_101 Any cryptographic operation performed by the motion sensor shall be in accordance with a specified algorithm and a specified key size.

CSP_102 If the motion sensor generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes.

Implementation within the motion sensor KITAS 2171

<SF29>:The TOE uses Triple-DES (with 2 keys) for en- and decryption. No other cryptographic algorithms are currently implemented within the TOE.

The TOE does not generate keys. The session key (O10.1:) used for communication with the vehicle unit is generated by the vehicle unit and then distributed in a secure and authenticated way to the motion sensor.

CSP_103 If the motion sensor distributes cryptographic keys, it shall be in accordance with specified key distribution methods.

Implementation within the motion sensor KITAS 2171

<SF30>:The TOE uses the key distribution method described in the architectural design documents.

CSP_104 If the motion sensor accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.

Implementation within the motion sensor KITAS 2171

<SF31>:Cryptographic keys are stored in the motion sensors internal EEPROM. Access to these keys is possible only via the motion sensors internal micro controller. Key can be overwritten by authorised commands only.

CSP_105 If the motion sensor destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.

Implementation within the motion sensor KITAS 2171

<SF32>:Keys are destroyed by overwriting them with new ones. Only session keys (O10.1:) are destroyed when the TOE performs a new pairing with another vehicle unit.

# 7 Definition of Security Mechanisms

The TOE provides the following security mechanisms to its entity:

<SM1> Symmetric cryptographic encryption algorithm, 2-key Triple-DES in ECB mode using 112 bits key length. This security mechanism is employed in accordance with international standardisation.

<SM2> Common secret between the motion sensor and the vehicle unit.

<SM3> Authentication. The motion sensor checks authentication data. The authentication data consists of an encrypted field that contains a random number and a check sum of this random number. The authentication data consists further of an check_value of the previous instruction, which depends on the latched impulscounter O1.2 and the authentication data of the previous instruction

<SM4> Reaction on authentication failures. Rejection of the request and generation of an error message.

<SM5> Storage of identity of connected entity.

<SM6> Entity-subject binding. The motion sensor KITAS 2171 is bound to one VU as an authorised entity at a given time.

<SM7> Access Control. The motion sensor checks that the command code submitted corresponds to a valid command.

<SM8> Data access rights. The motion sensor KITAS 2171 employs data access rights as described in section 0.0.0.

<SM9> Fixed file structure. The file structure of the motion sensor KITAS 2171 can’t be altered during operation.

<SM10> Defined access rights before activation. All file and data access rights are defined before activation.

<SM11> Controlled software update: A software upgrade is performed only with the installation of a new motion sensor KITAS 2171 in the vehicle.

<SM12> Definition of error conditions.

<SM13> Motion sensor identification and installation data. The Motion sensor identification data and installation data are stored in the EEPROM of the motion sensor. There is no function to alter the motion sensor identification data.

<SM14> Audit record storage.

<SM15> Audit record forwarding.

<SM16> Self testing. The first action of the motion sensor KITAS 2171 after receiving proper power supply is a self test. The self test can be also initiated by the authorised entity.

<SM17> Stored data integrity check. During start-up, after a reset, and on request an integrity check based on a checksum over permanently stored data is performed.

<SM18> Physical protection: The  motion sensor KITAS 2171 is a sealed device and any attempt to open the device can be detected through visual inspection.

<SM19> Power supply: The  motion sensor KITAS 2171 includes a separated power supply unit that controls the voltage and smoothness of the power input.

<SM20> Pre-emption prohibition.

<SM21> Secure reset. After power reset a synchronisation process between motion sensor and vehicle unit is initiated.

<SM22> Protected processing: The  motion sensor KITAS 2171 checks the construction and length of incoming commands.

<SM23> Immediate reaction on all  entity requests.

<SM24> Confirmation. The  motion sensor KITAS 2171 generates an acknowledgement message for each receipt command.

<SM25> Key distribution. Cryptographic keys are distributed in accordance with specified cryptographic key distribution methods.

<SM26> Restricted access to cryptographic keys.

<SM27> Cryptographic key destruction. Cryptographic key are destroyed in accordance with specified cryptographic key destruction methods

# 8 Minimum strength of security mechanisms

The minimum strength of the motion sensor security mechanisms is **High**, as defined in ITSEC [9].

# 9 Level of assurance

The target level of assurance for the motion sensor is ITSEC level **E3**, as defined in ITSEC [9].

Observe
Protection marks for restricting the use of documents and products
(DIN 34: 1998-01)

# 10 Rationale

The following matrixes give a rationale for the SEFs by showing:

- which SEFs or means counteract which threats,
- which SEFs fulfil which IT security objectives.

| | Threats | | | | | | | | | | | | IT Objectives | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Access** | **Faults** | **Tests** | **Design** | **Environment** | **Hardware** | **Mechanical_Origin** | **Motion_Data** | **Power_Supply** | **Security_Data** | **Software** | **Stored_Data** | **Access** | **Audit** | **Authentication** | **Processing** | **Reliability** | **Secured_Data_Exchange** |
| **Physical Personnel Procedural means** | | | | | | | | | | | | | | | | | | |
| Development | | x | x | x | | | | | | | | | | | | | | |
| Manufacturing | | | x | x | | | | | | | | | | | | | | |
| Delivery | | | | | | x | | | | | x | x | | | | | | |
| Security Data Generation | | | | | | | | | | x | | | | | | | | |
| Security Data Transport | | | | | | | | | | x | | | | | | | | |
| Approved Workshops | | | | | | | x | | | | | | | | | | | |
| Mechanical interface | | | | | | | x | | | | | | | | | | | |
| Regular Inspection | | | | | | x | x | | x | | x | | | | | | | |
| Law enforcement controls | | | | | x | x | x | | x | x | x | | | | | | | |
| Software Upgrades | | | | | | | | | | | x | | | | | | | |

| | Threats | | | | | | | | | | | | IT Objectives | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access | Faults | Tests | Design | Environment | Hardware | Mechanical_Origin | Motion_Data | Power_Supply | Security_Data | Software | Stored_Data | Access | Audit | Authentication | Processing | Reliability | Secured_Data_Exchange |
| **Security Enforcing Functions** | | | | | | | | | | | | | | | | | | |
| Identification and authentication | | | | | | | | | | | | | | | | | | |
| UIA_101 Entities identification | x | | | | | | | x | | | | | x | | x | | | x |
| UIA_102 Entities identity | x | | | | | | | | | | | | x | | x | | | |
| UIA_103 VU identity | | | | | | | | | | | | | | x | | | | |
| UIA_104 Entities authentication | x | | | | | | | x | | | | | x | | x | | | x |
| UIA_105 re-authentication | x | | | | | | | x | | | | | x | | x | | | x |
| UIA_106 Unforgeable authentication | x | | | | | | | x | | | | | x | | x | | | |
| UIA_107 Authentication failure | | | | | | | | x | | | | | | x | | | x | |
| Access control | | | | | | | | | | | | | | | | | | |
| ACC_101 Access control policy | x | | | | | | | | | x | | x | x | | | | | |
| ACC_102 Motion sensor ID | | | | | | | | | | | | x | x | | | | | |
| ACC_103 User data | | | | | | | | | | | | x | x | | | | | |
| ACC_104 Security Data | | | | | | | | | | x | | x | x | | | | | |
| ACC_105 File structure and access conditions | x | | | | | | | | | x | | x | x | | | | | |
| Accountability | | | | | | | | | | | | | | | | | | |
| ACT_101 Motion sensor ID data | | | | | | | | | | | | | | x | | | | |
| ACT_102 Pairing data | | | | | | | | | | | | | | x | | | | |
| ACT_103 Accountability data | | | | | | | | | | | | | | x | | | | |

| | Threats | | | | | | | | | | | | IT Objectives | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access | Faults | Tests | Design | Environment | Hardware | Mechanical_Origin | Motion_Data | Power_Supply | Security_Data | Software | Stored_Data | Access | Audit | Authentication | Processing | Reliability | Secured_Data_Exchange |
| Audit | | | | | | | | | | | | | | | | | | |
| AUD_101 Audit records | | | | | | | | | | | | | | x | | | | |
| AUD_102 Audit events list | x | | | | x | x | | | | | | x | | x | | | | |
| AUD_103 Audit data | | | | | | | | | | | | | | x | | | | |
| AUD_104 Audit tools | | | | | | | | | | | | | | x | | | | |
| AUD_105 Audit records storage | | | | | | | | | | | | | | x | | | | |
| Accuracy | | | | | | | | | | | | | | | | | | |
| ACR_101 Information flow control policy | | | | | | | | x | | | | | | | | x | x | |
| ACR_102 Internal transfers | | | | | | | | | | | | | | | | x | x | |
| ACR_103 Internal transfers | | | | | | | | | | | | | | x | | | | |
| ACR_104 Stored data integrity | | | | | | | | | | | | x | | | | | x | |
| ACR_105 Stored data integrity | | | | | | | | | | | | x | | x | | | | |
| Reliability | | | | | | | | | | | | | | | | | | |
| RLB_101 Manufacturing tests | | | x | x | | | | | | | | | | | | | x | |
| RLB_102 Self tests | | x | | | | x | | | x | | x | | | | | | x | |
| RLB_103 Self tests | | | | | | x | | | x | | x | | | x | | | | |
| RLB_104 Software analysis | | | | x | | | | | | | x | | | | | | x | |
| RLB_105 Software input | | | | | | | | | | | x | | | | | x | x | |
| RLB_106 Case opening | | | | x | x | x | | | | x | x | x | | | | | x | |
| RLB_107 Hardware sabotage | | | | | | x | | | | | | | | | | | x | |
| RLB_108 Hardware sabotage | | | | | | x | | | | | | | | x | | | | |
| RLB_109 Power supply interruptions | | | | | | | | | x | | | | | | | | x | |

| | Threats | | | | | | | | | | | | IT Objectives | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access | Faults | Tests | Design | Environment | Hardware | Mechanical_Origin | Motion_Data | Power_Supply | Security_Data | Software | Stored_Data | Access | Audit | Authentication | Processing | Reliability | Secured_Data_Exchange |
| RLB_110 Reset | | x | | | | | | | | | | | | | | | x | |
| RLB_111 Data Availability | | | | | | | | | | | | | | | | x | x | |
| RLB_112 Multiple Applications | | | | | | | | | | | | | | | | | x | |
| Data exchange | | | | | | | | | | | | | | | | | | |
| DEX_101 Secured motion data export | | | | | | | | x | | | | | | | | | | x |
| Cryptographic support | | | | | | | | | | | | | | | | | | |
| CSP_101 Algorithms | | | | | | | | | | | | | | | | | x | x |
| CSP_102 key generation | | | | | | | | | | | | | | | | | x | x |
| CSP_103 key distribution | | | | | | | | | | | | | | | | | x | x |
| CSP_104 key access | | | | | | | | | | | | | | | | | x | x |
| CSP_105 key destruction | | | | | | | | | | | | | | | | | x | x |

# 11 Matrix SEF's vs. SM's

Security enforcing functions versus security mechanisms cross reference matrix

| **Security Enforcing Function** | **Security Mechanism** |
|---|---|
| <SF1>: | <SM1>,<SM2> |
| <SF2>: | <SM5> |
| <SF3>: | <SM2>, <SM6>, <SM19>,<SM21> |
| <SF4>: | <SM1>,<SM3> |
| <SF5>: | <SM6> |
| <SF6>: | <SM4> |
| <SF7>: | <SM7> |
| <SF8>: | <SM8> |
| <SF9>: | <SM9> |
| <SF10>: | <SM9>, <SM10> |
| <SF11>: | <SM13> |
| <SF12>: | <SM12> |
| <SF13>: | <SM14> |
| <SF14>: | <SM6> |
| <SF15>: | <SM15> |
| <SF16>: | <SM18> |
| <SF17>: | <SM17> |
| <SF18>: | <SM16>, <SM17> |
| <SF19>: | <SM20> |
| <SF20>: | <SM11> |
| <SF21>: | <SM18> |
| <SF22>: | <SM18> |
| <SF23>: | <SM19> |
| <SF24>: | <SM21> |
| <SF25>: | <SM23> |
| <SF26>: | <SM1>, <SM3>, <SM22> |

| | |
|---|---|
| <SF27>: | <SM1>,<SM2> |
| <SF28>: | <SM24> |
| <SF29>: | <SM1> |
| <SF30>: | <SM25> |
| <SF31>: | <SM26> |
| <SF32>: | <SM27> |

# 12 References

[1] **Appendix 10 and Appendix 11** of Annex 1B of COMMISION REGULATION (EC) No 1360/2002 of 13 June 2002

[2] **Council Regulation (EEC) No. 3821/85** of the 20 December 1985 on recording equipment in road transport. amended by Council Regulation (EC) No. 69/2009 and last amended by CR (EU)

No. 1266/2009 on recording equipment in road transport

[3] **COMMISION REGULATION (EC) No 1360/2002 of 13 June 2002** amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/84 and (EEC) No 3821/85

[4] **Council Regulation (EC) No. 68/2009** of 23 January 2009 adapting for the ninth time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport

[5] **Commission Regulation (EU) No 1266/2009** of 16 December 2009 adapting for the tenth time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport

[6] ISO 16844-3 Motion Sensor Interface, 1.11.2004

[7] **Appendix 1** of Annex 1B of COMMISION REGULATION (EC) No 1360/2002 of 13 June 2002

[8] **ISO 16844-3** „Motion sensor interface", 1.11.2004 und ISO 16844-3: 2004 Technical corrigendum 1, veröffentlicht 1.03.2006

[9] **ITSEC** Information Technology Security Evaluation Criteria 1991