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

[F1[F2ANNEX I B

REQUIREMENTS FOR CONSTRUCTION, TESTING, INSTALLATION AND INSPECTION

Textual Amendments

F1 Inserted by Council Regulation (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85.

F2 Substituted by Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport (Text with EEA relevance).

Appendix 10

GENERIC SECURITY TARGETS

MOTION SENSOR GENERIC SECURITY TARGET

1. Introduction

This document contains a description of the motion sensor, of the threats it must be able to counteract and of the security objectives it must achieve. 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.

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

Annex I B 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.

2. Abbreviations, definitions and references

2.1. Abbreviations

ROM	Read only Memory
SEF	Security enforcing function
TBD	To be defined
TOE	Target of evaluation
VU	Vehicle unit.

2.2. Definitions

Digital Tachograph	Recording equipment
Entity	A device connected to the motion sensor
Motion data	The data exchanged with the VU, representative of speed and 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
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys)
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’)
User data	Any data, other than motion or security data, recorded or stored by the motion sensor.

2.3. References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.

3. Product rationale

3.1. Motion sensor description and method of use

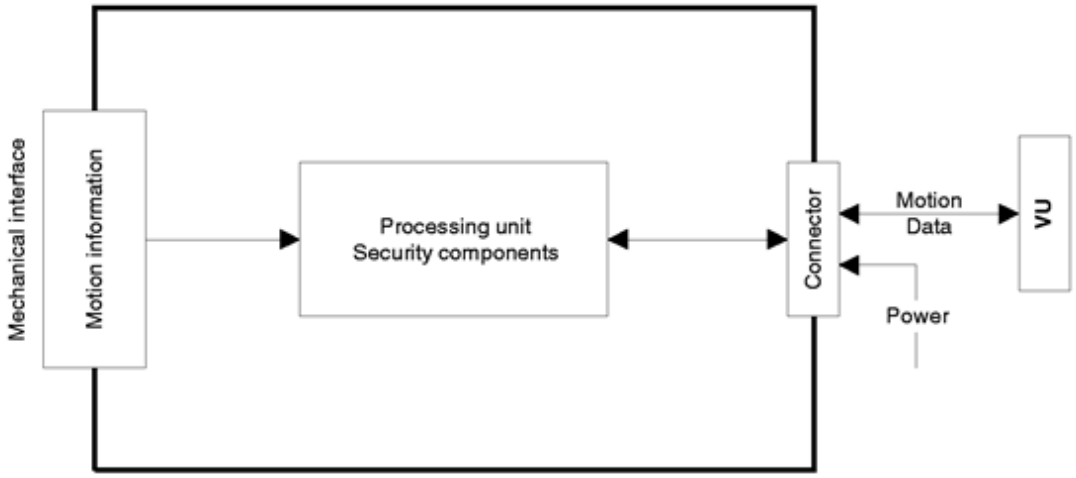
The motion sensor is intended to be installed in road transport vehicles. Its purpose is to provide a VU with secured motion data representative of vehicle's speed and distance travelled.

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.

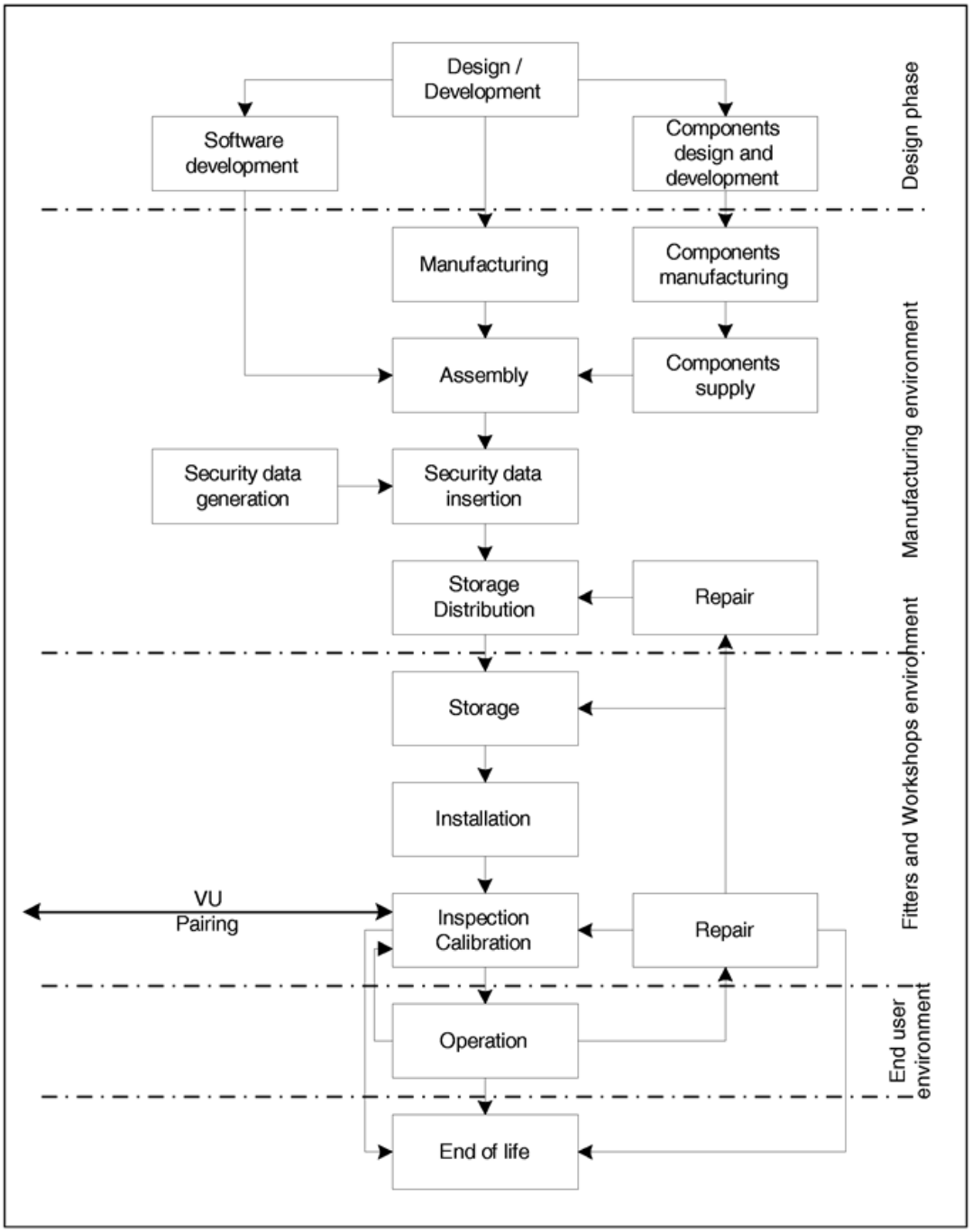
It may also be connected to specific equipment for management purposes (TBD by manufacturer).

The typical motion sensor is described in the following figure:



3.2. Motion sensor life cycle

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



3.3. Threats

This paragraph describes the threats the motion sensor may face.

3.3.1. Threats to access control policies

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

3.3.2. 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.

3.3.3. 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).

3.4. 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.

3.5. 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.

3.6. Physical, personnel or procedural means

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

3.6.1. 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.

3.6.2. 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.

3.6.3. 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.

3.6.4. 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.

3.6.5. Law enforcement control

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

3.6.6. Software upgrades

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

4. Security enforcing functions

4.1. Identification and authentication

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

The identity of a connected entity shall consist of:

— an entity group:
  — VU,
  — Management device,
  — Other,

— an entity ID (VU only).

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

The motion sensor shall be able to authenticate any VU or management device it is connected to:
— at entity connection,
— at power supply recovery.

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

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

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.

4.2. Access control

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

4.2.1. Access control policy

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

4.2.2. Data access rights

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

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

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

4.2.3. File structure and access conditions

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

4.3. Accountability

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

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

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

4.4. Audit

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

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.

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).

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.

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.

4.5. Accuracy

4.5.1. Information flow control policy

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

4.5.2. Internal data transfers

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

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

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.

4.5.3. Stored data integrity

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

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

4.6. Reliability of service

4.6.1 Tests

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.

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).

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

4.6.2. Software

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

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

4.6.3. Physical protection

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).

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

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

4.6.4. Power supply interruptions

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

4.6.5. Reset conditions

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.

4.6.6. Data availability

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

4.6.7. Multiple applications

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.

4.7. Data exchange

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.

4.8. Cryptographic support

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

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

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

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

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

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

5. Definition of security mechanisms

The security mechanisms, fulfilling the motion sensor security enforcing functions, are defined by the motion sensor manufacturers.

6. Minimum strength of security mechanisms

The minimum strength of the motion sensor security mechanisms is High, as defined in (ITSEC).

7. Level of assurance

The target level of assurance for the motion sensor is ITSEC level E3, as defined in (ITSEC).

8. 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	**Fault**	**Tests**	**Design**	**Envi**	**Hard**	**Mat**	**Mat**	**Init**	**Phy**	**Orig**	**Sup**	**Data**	**Acc**	**Data**	**Auth**	**Prov**	**Int**	**Int**	**Secured_Data_Exchan**
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							
Security Enforcing Functions																	
Identification and authentication																	
UIA_x101 Entities identification						x					x		x			x	
UIA_x102 Entities identity											x		x				
UIA_103 VU identity												x					
UIA_x104 Entities authentication						x					x		x			x	
UIA_x105 re-authentication						x					x		x			x	
UIA_x106 Unforgeable authentication						x					x		x				
UIA_107 Authentication failure						x						x			x		
Access control																	
ACCx101 Access control policy								x		x	x						
ACC_102 Motion sensor ID										x	x						
ACC_103 User data										x	x						
ACC_104 Security Data								x		x	x						
ACCx105 File structure and								x		x	x						

access conditions																	
Accountability																	
ACT_101 Motion sensor ID data													x				
ACT_102 Pairing data													x				
ACT_103 Accountability data													x				
Audit																	
AUD_101 Audit records													x				
AUDx_102 Audit events list			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
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]]	

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, MOTION SENSOR GENERIC SECURITY TARGET.