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

VEHICLE UNIT GENERIC SECURITY TARGET

1. Introduction

This document contains a description of the vehicle unit, 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

PIN	Personal identification number
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
Motion data	The data exchanged with the motion sensor, representative of speed and distance travelled
Physically separated parts	Physical components of the VU that are distributed in the vehicle as opposed to physical components gathered into the VU 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	Users are to be understood as human user of the equipment. Normal users of the VU comprise drivers, controllers, workshops and companies
User data	Any data, other than security data, recorded or stored by the VU, required by Chapter III.12.

2.3. References

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991.

3. Product rationale

3.1. Vehicle unit description and method of use

The VU is intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities.

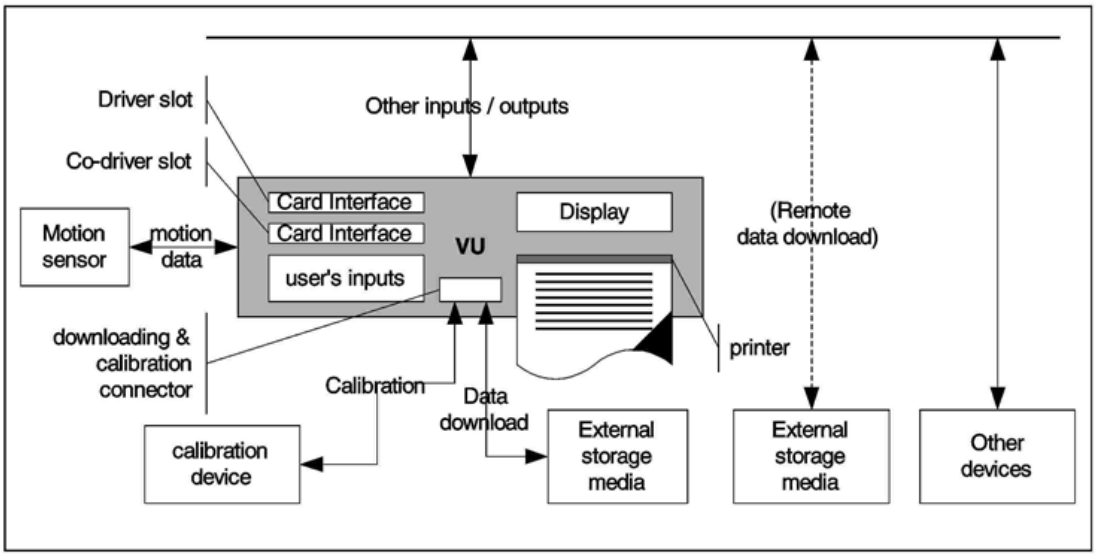
It is connected to a motion sensor with which it exchanges vehicle's motion data.

Users identify themselves to the VU using tachograph cards.

The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards.

The VU outputs data to display, printer and external devices.

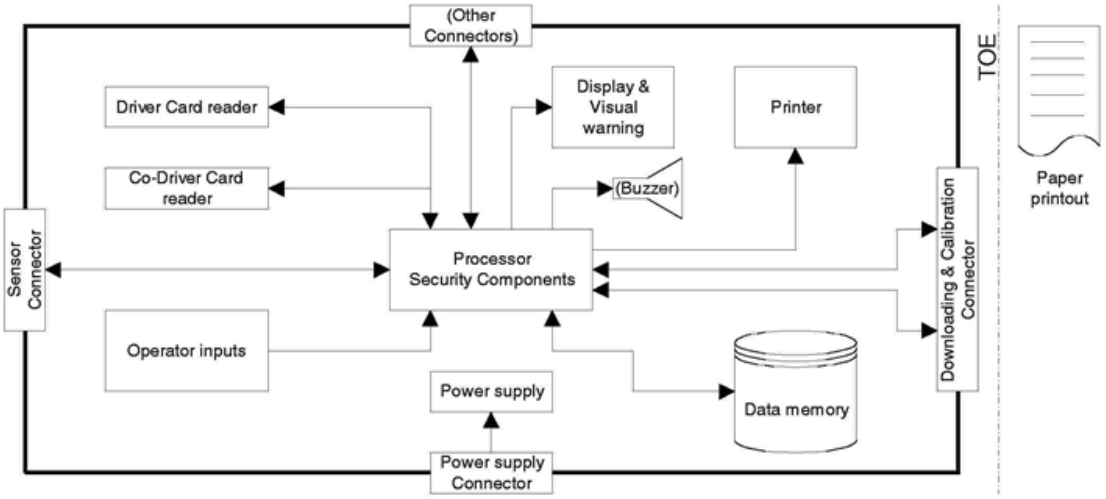
The vehicle unit's operational environment while installed in a vehicle is described in the following figure:



The VU general characteristics, functions and mode of operations are described in Chapter II of Annex I B.

The VU functional requirements are specified in Chapter III of Annex I B.

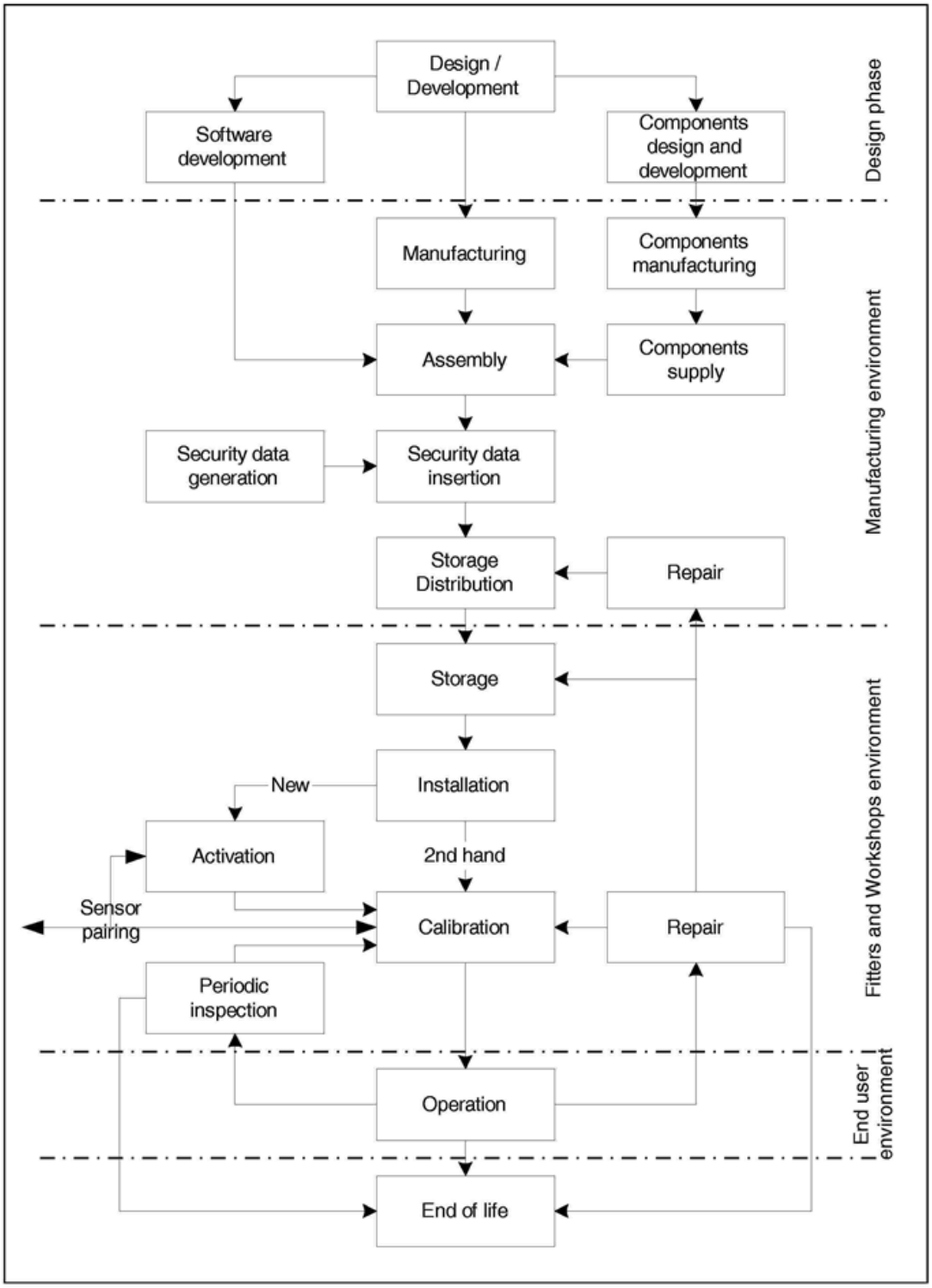
The typical VU is described in the following figure:



It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

3.2. Vehicle unit life cycle

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



3.3. Threats

This paragraph describes the threats the VU may face.

3.3.1. Threats to identification and access control policies

T.Access	Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function)
T.Identification	Users could try to use several identifications or no identification.

3.3.2. Design related threats

T.Faults	Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security
T.Tests	The use of non invalidated test modes or of existing back doors could compromise the VU 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.Calibration_Parameters	Users could try to use mis-calibrated equipment (through calibration data modification, or through organisational weaknesses)
T.Card_Data_Exchange	Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal)
T.Clock	Users could try to modify internal clock
T.Environment	Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, …)
T.Fake_Devices	Users could try to connect fake devices (motion sensor, smart cards) to the VU
T.Hardware	Users could try to modify VU hardware
T.Motion_Data	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal)
T.Non_Activated	Users could use non activated equipment
T.Output_Data	Users could try to modify data output (print, display or download)
T.Power_Supply	Users could try to defeat the VU 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 VU 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 objectives of the VU, contributing to the global security objective, are the following:

O.VU_Main	The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed
O.VU_Export	The VU must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity.

3.5. Information technology security objectives

The specific IT security objectives of the VU contributing to its main security objectives, are the following:

O.Access	The VU must control user access to functions and data
O.Accountability	The VU must collect accurate accountability data
O.Audit	The VU must audit attempts to undermine system security and should trace them to associated users
O.Authentication	The VU should authenticate users and connected entities (when a trusted path needs to be established between entities)
O.Integrity	The VU must maintain stored data integrity
O.Output	The VU must ensure that data output reflects accurately data measured or stored
O.Processing	The VU must ensure that processing of inputs to derive user data is accurate
O.Reliability	The VU must provide a reliable service
O.Secured_Data_Exchange	The VU must secure data exchanges with the motion sensor and with tachograph cards.

3.6. Physical, personnel or procedural means

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

3.6.1. Equipment design

M.Development	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security
M.Manufacturing	VU 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 VU is protected from physical attacks which might compromise IT security.

3.6.2. Equipment delivery and activation

M.Delivery	VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of non activated VUs is done in a manner which maintains VU security
M.Activation	Vehicle manufacturers and fitters or workshops must activate the VU after its installation before the vehicle leaves the premises where installation took place.

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 VU, in such a way to preserve its appropriate confidentiality and integrity.

3.6.4. Cards delivery

M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only
M.Driver_Card_Uniqueness	Drivers must possess, at one time, *one* valid driver card only
M.Card_Traceability	Card delivery must be traceable (white lists, black lists), and black lists must be used during security audits.

3.6.5. 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.Regular_Inpections	Recording equipment must be periodically inspected and calibrated
M.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.

3.6.6. Equipment operation

M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, …).

3.6.7. Law enforcement control

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

3.6.8. Software upgrades

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

4. Security enforcing functions

4.1. Identification and authentication

4.1.1. Motion sensor identification and authentication

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

The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.

The VU shall authenticate the motion sensor it is connected to:

— at motion sensor connection,

— at each calibration of the recording equipment,

— at power supply recovery.

Authentication shall be mutual and triggered by the VU.

The VU shall periodically (period TBD by manufacturer and more frequently than once per hour) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.

The VU 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, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the SEF shall:

— generate an audit record of the event,

— warn the user,

— continue to accept and use non secured motion data sent by the motion sensor.

4.1.2. User identification and authentication

The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.

The user identity shall consist of:

— a user group:
  — DRIVER (driver card),
  — CONTROLLER (control card),
  — WORKSHOP (workshop card),
  — COMPANY (company card),
  — UNKNOWN (no card inserted),
— a user ID, composed of:
  — the card issuing Member State code and of the card number,
  — UNKNOWN if user group is UNKNOWN.

UNKNOWN identities may be implicitly or explicitly known.

The VU shall authenticate its users at card insertion.

The VU shall re-authenticate its users:

— at power supply recovery,
— periodically or after occurrence of specific events (TBD by manufacturers and more frequently than once per day).

Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.

In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long.

Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.

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

After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall:

— generate an audit record of the event,
— warn the user,
— assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007).

4.1.3. Remotely connected company identification and authentication

Company remote connection capability is optional. This paragraph therefore applies only if this feature is implemented.

For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.

The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.

The VU shall successfully authenticate the remotely connected company before allowing any data export to it.

Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.

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

After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:

— warn the remotely connected company.

4.1.4. Management device identification and authentication

VU manufacturers may foresee dedicated devices for additional VU management functions (e.g. Software upgrading, security data reloading, …). This paragraph therefore applies only if this feature is implemented.

For every interaction with a management device, the VU shall be able to establish the device identity.

Before allowing any further interaction, the VU shall successfully authenticate the management device.

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

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.

It must be noted that the user data recorded by the VU, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011) is not the subject of a security enforcing function.

4.2.1. Access control policy

The VU shall manage and check access control rights to functions and to data.

4.2.2. Access rights to functions

The VU shall enforce the mode of operation selection rules (requirements 006 to 009).

The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).

4.2.3. Access rights to data

The VU shall enforce the VU identification data write access rules (requirement 076)

The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)

After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).

After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).

After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).

After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).

The VU shall enforce appropriate read and write access rights to security data (requirement 080).

4.2.4. 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 VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087, 105a, 105b, 109 and 109a).

The VU shall hold permanent identification data (requirement 075).

The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).

The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).

The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).

The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.

The VU shall ensure that it does not modify data already stored in a tachograph card (requirements 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1 Note.

4.4. Audit

Audit capabilities are required only for events that may indicate a manipulation or a security breach attempt. It is not required for the normal exercising of rights even if relevant to security.

The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).

The events affecting the security of the VU are the following:

- Security breach attempts,
  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorised change of motion sensor,
  - card data input integrity error,
  - stored user data integrity error,
  - internal data transfer error,
  - unauthorised case opening,
  - hardware sabotage,
- last card session not correctly closed,
- motion data error event,
- power supply interruption event,
- VU internal fault.

The VU shall enforce audit records storage rules (requirement 094 and 096).

The VU shall store audit records generated by the motion sensor in its data memory.

It shall be possible to print, display and download audit records.

4.5. Object re-use

The VU shall ensure that temporary storage objects can be re-used without this involving inadmissible information flow.

4.6. Accuracy

4.6.1. Information flow control policy

The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:

— vehicle motion data,
— VU's real time clock,
— recording equipment calibration parameters,
— tachograph cards,
— user's inputs.

The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal — current insertion (requirement 050a).

4.6.2. Internal data transfers

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

If data are transferred between physically separated parts of the VU, 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.

4.6.3. Stored data integrity

The VU shall check user data stored in the data memory for integrity errors.

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

4.7. Reliability of service

4.7.1. Tests

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

The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU 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 (except in calibration mode) (VU internal fault),
— Preserve the stored data integrity.

4.7.2. Software

There shall be no way to analyse or debug software in the field after the VU activation.

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

4.7.3. Physical protection

If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of six months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).

If the VU 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).

After its activation, the VU shall detect specified (TBD by manufacturer) hardware sabotage.

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

4.7.4. Power supply interruptions

The VU shall detect deviations from the specified values of the power supply, including cut-off.

In the case described above, the SEF shall:
— generate an audit record (except in calibration mode),
— preserve the secure state of the VU,
— maintain the security functions, related to components or processes still operational,
— preserve the stored data integrity.

4.7.5. Reset conditions

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

4.7.6. Data availability

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

The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016)

In the case described above, the SEF shall generate an audit record of the event.

4.7.7. Multiple applications

If the VU 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.

4.8. Data exchange

This paragraph addresses data exchange between the VU and connected devices.

4.8.1. Data exchange with motion sensor

The VU shall verify the integrity and authenticity of motion data imported from the motion sensor

Upon detection of a motion data integrity or authenticity error, the SEF shall:
— generate an audit record,
— continue to use imported data.

4.8.2. Data exchange with tachograph cards

The VU shall verify the integrity and authenticity of data imported from tachograph cards.

Upon detection of card data integrity or authenticity error, the VU shall:
— generate an audit record,
— not use the data.

The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

4.8.3. Data exchange with external storage media (downloading function)

The VU shall generate an evidence of origin for data downloaded to external media.

The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.

The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.

4.9. 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 VU shall be in accordance with a specified algorithm and a specified key size.

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

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

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

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

5. Definition of security mechanisms

Required security mechanisms are specified in Appendix 11.

All other security mechanisms are to be defined by manufacturers.

6. Minimum strength of security mechanisms

The minimum strength of the Vehicle Unit security mechanisms is *High*, as defined in (ITSEC).

7. Level of assurance

The target level of assurance for the Vehicle Unit 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.

[X1

		Threats																		IT Objectives									
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Physical personnel procedural means																													
Development				x	x	x																							
Manufacturing					x	x																							
Delivery													x																
Activation		x											x																
Security data generation																	x												
Security data transport																	x												
Card availability			x																										
One driver card			x																										
Card traceability			x																										
Approved workshops							x		x																				
Regular inspection calibration							x		x			x				x			x										
Faithful workshops							x		x																				
Faithful drivers			x																										
Law enforcement controls			x				x		x	x		x		x		x		x	x										
Software upgrade																			x										
Security-enforcing functions																													
Identification and authentication																													
UIA_201	Sensor identification										x		x											x					x
UIA_202	Sensor identity										x		x											x					
UIA_203	Sensor authentication										x		x											x					x
UIA_204	Sensor re-identification and re-authentication										x		x											x					x
UIA_205	Unforgeable authentication										x		x											x					
UIA_206	Authentication failure										x		x										x					x	
UIA_207	Users identification	x	x								x										x			x					x
UIA_208	User identity	x	x								x										x			x					
UIA_209	User authentication	x	x								x										x			x					x
UIA_210	User re-authentication	x	x								x										x			x					x
UIA_211	Authentication means	x	x								x										x			x					
UIA_212	PIN checks	x	x				x		x												x			x					
UIA_213	Unforgeable authentication	x	x								x										x			x					
UIA_214	Authentication failure	x	x								x												x						
UIA_215	Remote user identification	x	x																		x			x					x
UIA_216	Remote user identity	x	x																		x			x					
UIA_217	Remote user authentication	x	x																		x			x					x
UIA_218	Authentication means	x	x																		x			x					
UIA_219	Unforgeable authentication	x	x																		x			x					
UIA_220	Authentication failure	x	x																										

Editorial Information

X1 Substituted by Corrigendum to 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 (Official Journal of the European Communities L 207 of 5 August 2002).

		Threats																	IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
UIA_221	Management device Identification	x	x																		x			x					
UIA_222	Management device Authentication	x	x																		x			x					
UIA_223	Unforgeable authentication	x	x																		x			x					
Access control																													
ACC_201	Access control policy	x					x		x									x		x	x								
ACC_202	Access rights to functions	x					x		x												x								
ACC_203	Access rights to functions	x					x		x												x								
ACC_204	VU ID																			x	x								
ACC_205	Connected sensor ID										x									x	x								
ACC_206	Calibration data	x					x													x	x								
ACC_207	Calibration data						x													x	x								
ACC_208	Time adjustment data								x											x	x								
ACC_209	Time adjustment data								x											x	x								
ACC_210	Security data																	x		x	x								
ACC_211	File structure and access conditions	x					x											x		x	x								
Accountability																													
ACT_201	Drivers accountability																					x							
ACT_202	VU ID data																					x	x						
ACT_203	Workshops accountability																					x							
ACT_204	Controllers accountability																					x							
ACT_205	Vehicle movement accountability																					x							
ACT_206	Accountability data modification																			x				x			x		
ACT_207	Accountability data modification																			x				x			x		
Audit																													
AUD_201	Audit records																						x						
AUD_202	Audit events list	x						x				x	x		x	x				x			x						
AUD_203	Audit records storage rules																						x						
AUD_204	Sensor audit records																						x						
AUD_205	Audit tools																						x						
Re-use																													
REU_201	Re-use																	x								x	x		

		Threats																	IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	(intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Accuracy																												
ACR_201	Information flow control policy							x			x		x														x	x	
ACR_202	Internal transfers														x										x	x	x	
ACR_203	Internal transfers														x								x					
ACR_204	Stored data integrity																			x				x			x	
ACR_205	Stored data integrity																			x			x					
Reliability																												
RLB_201	Manufacturing tests				x	x																					x	
RLB_202	Self tests			x								x				x			x								x	
RLB_203	Self tests											x				x			x				x					
RLB_204	Software analysis					x													x								x	
RLB_205	Software input																		x						x	x	x	
RLB_206	Case opening					x				x		x			x			x	x	x					x		x	
RLB_207	Hardware sabotage											x															x	
RLB_208	Hardware sabotage											x											x					
RLB_209	Power supply interruptions															x											x	
RLB_210	Power supply interruptions															x							x					
RLB_211	Reset			x																							x	
RLB_212	Data availability																									x	x	
RLB_213	Card release																										x	
RLB_214	Card session not correctly closed																						x					
RLB_215	Multiple applications																										x	
Data exchange																												
DEX_201	Secured motion data import												x															x
DEX_202	Secured motion data import												x										x					
DEX_203	Secured card data import							x																				x
DEX_204	Secured card data import							x															x					
DEX_205	Secured data export to cards							x																				x
DEX_206	Evidence of origin														x										x			
DEX_207	Evidence of origin														x										x			
DEX_208	Secured export to external media														x										x			

		Threats																	IT Objectives								
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply (intentionally left blank)	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Cryptographic support																											
CSP_201	Algorithms																									x	x
CSP_202	key generation																									x	x
CSP_203	key distribution																									x	x
CSP_204	key access																									x	x
CSP_205	key destruction																									x	x

]]]

Status:
Point in time view as at 01/05/2006.

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