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

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.

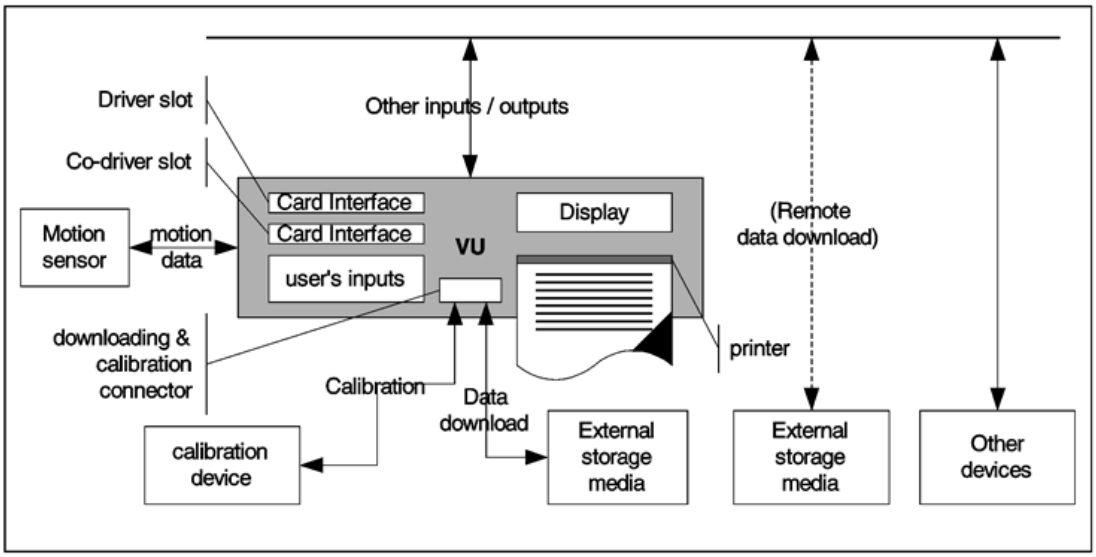
It is connected to a motion sensor with which it exchanges vehicle's motion data.

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.

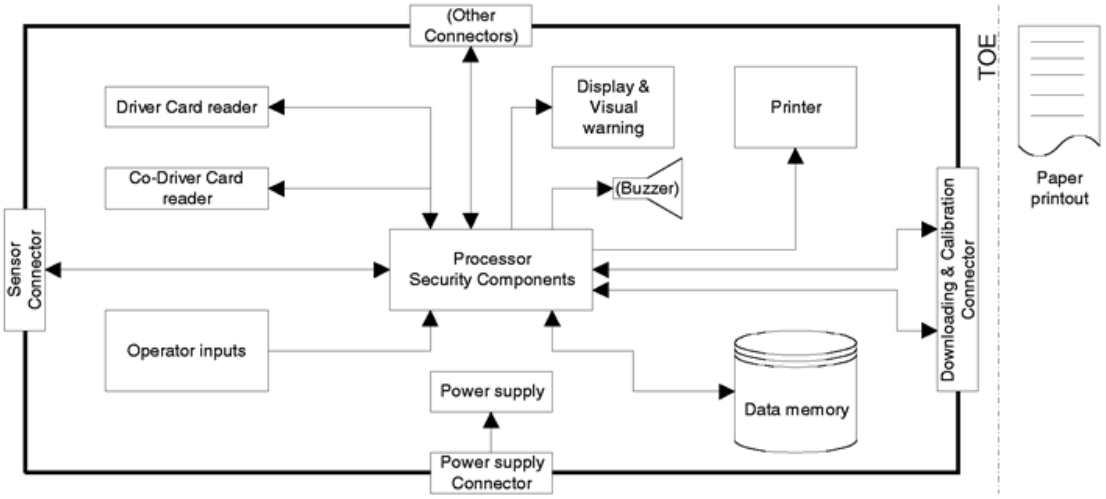
The vehicle unit's operational environment while installed in a vehicle is described in the following figure:



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.

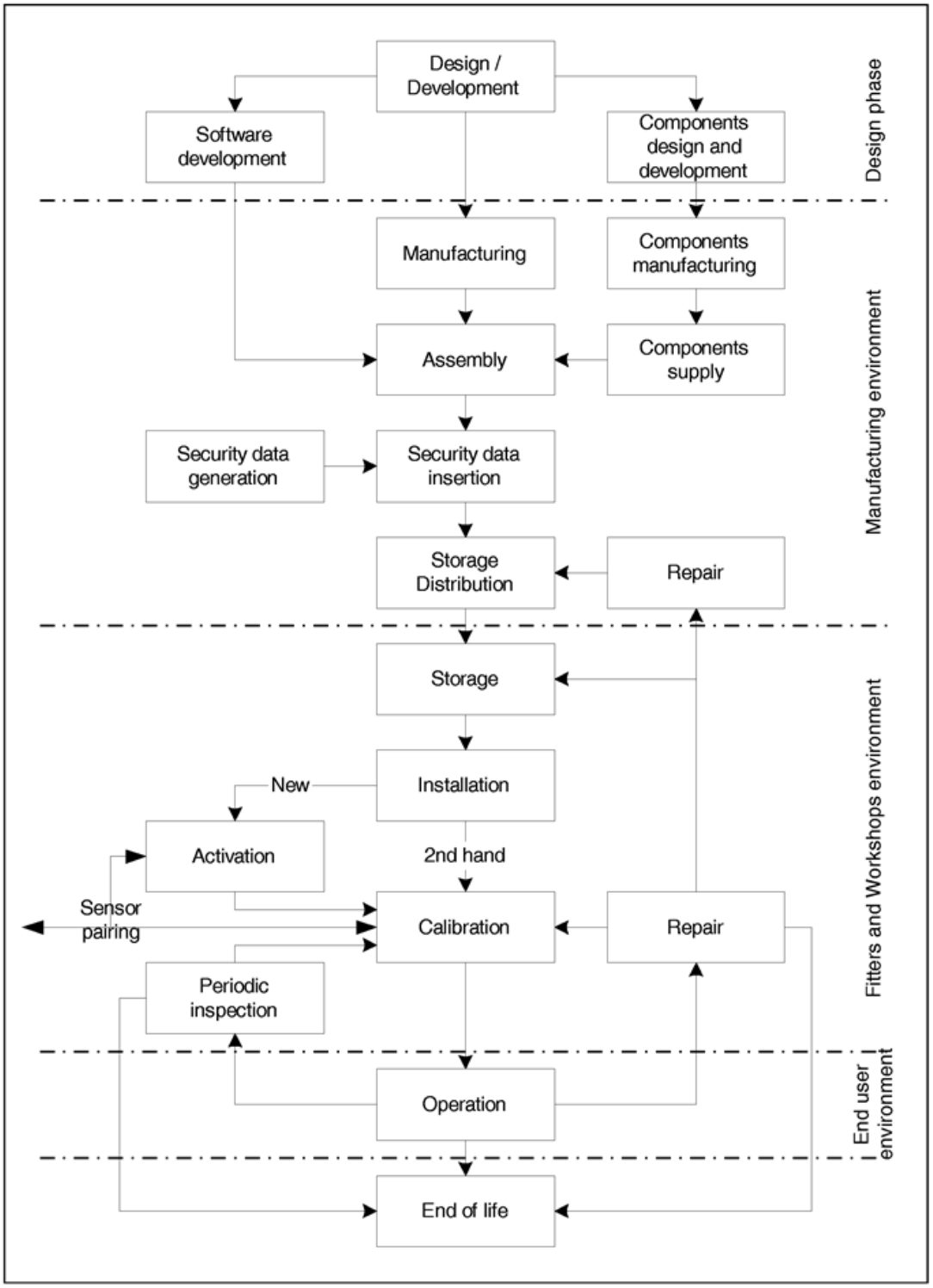
The typical VU is described in the following figure:



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.**]]**

Changes to legislation:
There are currently no known outstanding effects for the Council Regulation (EEC) No 3821/85, Division 3..