Public version

25, chemin de Pouvourville - BP 4215
31432 TOULOUSE CEDEX 04 - (FRANCE)
Fax : (33) 05 61 55 42 31 - Tél. (33) 05 61 17 61 61

SECURITY TARGET

IS2000

	By	Date	Sign		Ref. ACTIA	Index
Draw	SJan			**SECURITY TARGET** **IS2000**	**P204406**	**F** Public
Verif	JKun					
Valid	ERom					
Appr	SBab					Format A4

TABLE OF CONTENTS

I. FOREWORD

I.1 INTRODUCTION

This document is the public version of the security target of the ACTIA IS2000 product. Some information are not available because of restricted character.

The IS2000 is a recording equipment (tachograph) motion sensor (MS) conforming to Annex 1B of Council Regulation (EEC) n° 3821/85 as last amended by Council Regulation (EC) n° 1360/2002. The IS2000 interface with a vehicle unit (VU) is compliant with ISO 16844-3.

This security target is derived from Appendix 10 to above Council Regulation which contains a motion sensor ITSEC generic security target. The IS2000 security target is intended to be in full compliance with the motion sensor ITSEC generic security target.

I.2 REFERENCE DOCUMENTS

[CC] ..... Common Criteria version 2.2, revision 456 – January 2004

[3821_1B] ..... Annex 1B of Council Regulation (EEC) n° 3821/85 as last amended by Council Regulation (EEC) n° 432/2004 of 05/03/2004,

[1B_MB] ..... Main Body of [3821_1B] "Requirements for construction, testing, installation, and inspection"

[1B_10] ..... Appendix 10 to [3821_1B] "Generic security targets"

[1B_11] ..... Appendix 11 to [3821_1B] "Common security mechanisms"

[ISO 16844-3] ..... ISO/TC22/SC3 document : ISO/DIS 16844-3 – Road vehicles – Tachograph systems – Part 3 : Motion Sensor Interface.

[TDES] ..... National Institute of Standards and Technology (NIST). FIPS Publication 46-3 : Data Encryption Standard. Draft 1999.
ANSI X9.52, Triple Data Encryption Algorithm Modes of operation. 1998.

[JIL] ..... Joint Interpretation Library. Security Evaluation and Certification of Digital Tachographs. Version 0.9 September 2002.

I.3 CONVENTIONS AND TERMINOLOGY

Throughout this document (req. xxx) means requirement (marginal) xxx of [1B_MB] and (AAA_xxx) means requirement AAA_xxx of [1B_10].

The text in [3821_1B] addressed by these references is to be considered as an integral part of the ST. This method is used to provide sense and clarification to the text of the ST while avoiding redundancy or incompatibility with this superseding document.

II. ST INTRODUCTION

II.1 ST IDENTIFICATION

Title : .....**Security Target - IS2000**

Reference :.....P204406

TOE Identification.....ACTIA IS2000 Motion Sensor

921442 ind_A IS2000 L:23,8 R:0
921443 ind_A IS2000 L:25 R:0
921444 ind_A IS2000 L:63,2 R:0
921445 ind_A IS2000 L:19,8 R:1,2
921446 ind_A IS2000 L:25 R:1,2
921447 ind_A IS2000 L:35 R:1,2
921448 ind_A IS2000 L:63,2 R:1,2
921449 ind_A IS2000 L:90 R:1,2
921450 ind_A IS2000 L:115 R:1,2
921451 ind_A IS2000 L:136,8 R:1,2
921460 ind_A IS2000 L:25 R:1,8

Where L is the length of the part dipping into the gearbox and R is the thickness of the washer.

Key words : .....Road transport vehicle, Digital tachograph, Recording Equipment, Motion Sensor, Security Target

EAL level : .....**E3hAP (See [JIL]);**

Strength of functions : .**SOF-high**

CC conformance :.....CC version 2.2, revision 456 – January 2004, Parts 1 to 3.

II.2 ST OVERVIEW

This document contains a description of the IS2000 and its security environment.

It specifies the security objectives for the IS2000 and its environment, that address the environmental considerations.

It specifies the security functional measures offered by the IS2000 and security assurance measures enforced during its development, that satisfy the stated security objectives.

It states the claimed minimum Strength Of Functions (SOF) and the required level of assurance for the development and the CC evaluation.

III. TOE DESCRIPTION

III.1 IS2000 DESCRIPTION AND METHOD OF USE

The IS2000 is intended to be installed in road transport vehicles. Its purpose is to provide a Vehicle Unit (VU) with secured motion data representative of vehicle's speed and distance travelled.

The IS2000 is a motion sensor designed to be screwed in the gearbox housing of the vehicle, and sealed. The rotation of a target inside the gearbox is used to generate the speed signal.

The IS2000 metal housing contains:
- a detection cell, which is located in the part dipping into the gearbox, close to the target,
- other electronic components which are located on a PC board in the part outside the gearbox.

The IS2000 is permanently powered by the vehicle unit it is connected to.

The general drawing of the IS2000 housing is provided below :

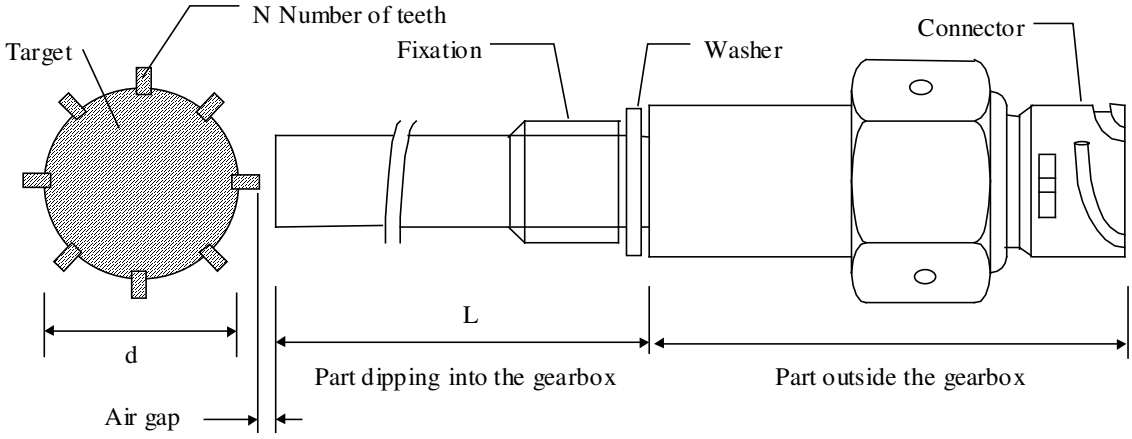

Figure 1 IS2000 Physical description

To take into account various gearbox configurations, different versions of the IS2000 exist with all the same characteristics but the length (L) of the part dipping into the gearbox which varies.

The IS2000 interface (physical, electrical and protocol levels) is compliant with ISO 16844-3. Input / Output signals are exchanged through an ISO 15170-1 Standard (DIN 7285-1) 4 pin connector.

The IS2000 provides real time speed pulses to the vehicle unit it is connected to.

A secured, bi-directional communication line allows data to be exchanged between the IS2000 and the vehicle unit (for IS2000/vehicle unit pairing and mutual authentication, integrity control of measured speed data...).

The functional block diagram of the IS2000 is shown below :

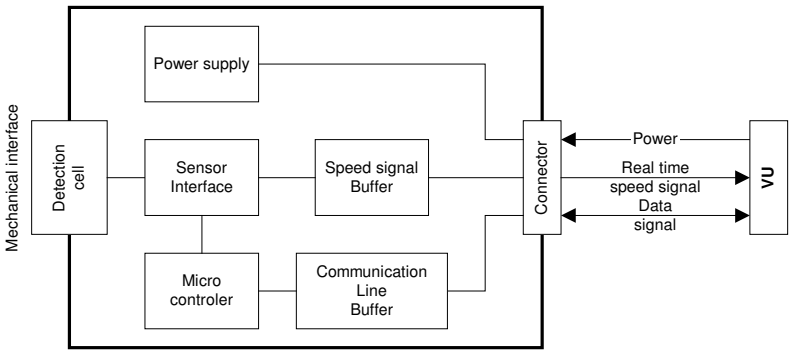

Figure 2 IS2000 functional block diagram

The functions provided by the IS2000 are the following :
- pulse detection and transmission to the VU,
- pairing with a VU,
- counting pulses transmitted,
- sending data at VU request,
- self tests,
- power supply management.

The data held by the IS2000 are classified as follows :
- identification data (approval number, serial number),
- security data :
  - ***static data*** : serial number encrypted with the master key, cleartext-form pairing key, pairing key encrypted with the master key ;
  - ***dynamic data*** : the session key sent by the vehicle unit, the random number embedded within VU commands,
- pairing data (first paired and currently paired VU approval and serial numbers),
- temporary audit data,
- transmitted pulses counter.

III.2 IS2000 LIFE CYCLE

The life cycle of the IS2000 is described in the following figure :

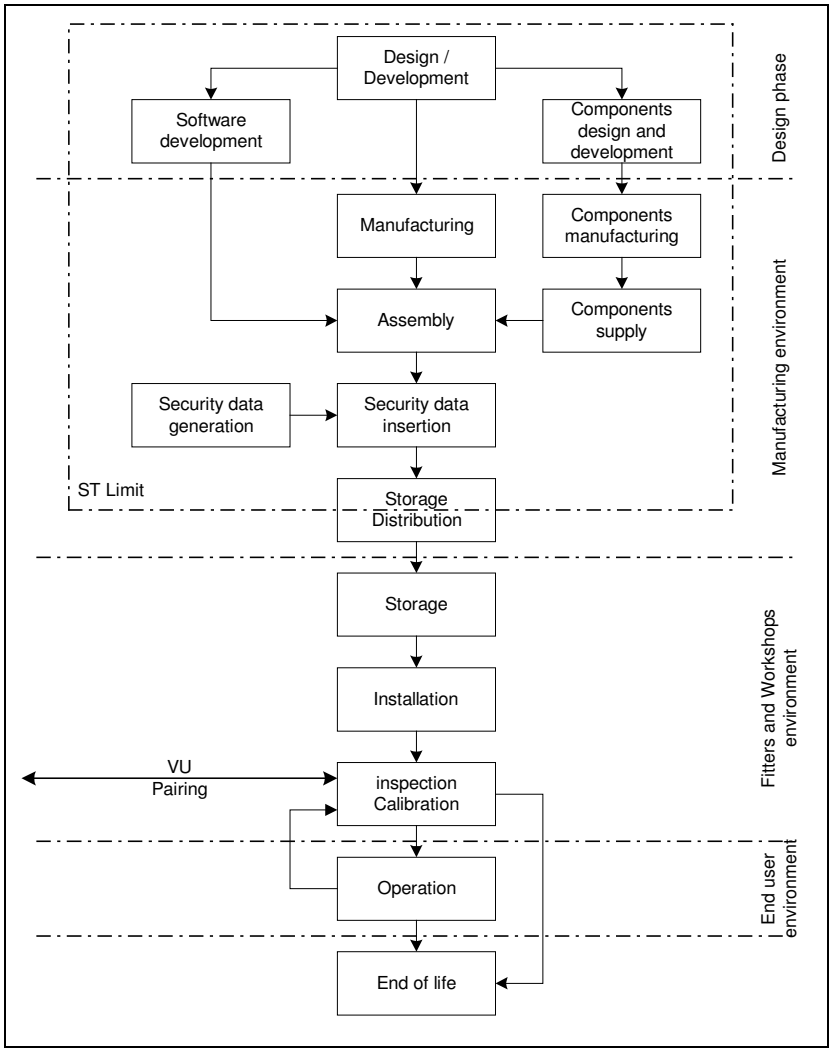

Figure 2: IS2000 typical life cycle

ST limit : the purpose of the security functions, designed and manufactured within this area, is to control and protect the TOE during its operational life (product usage). The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases. This is why this ST addresses the functions used during product usage but developed and manufactured within the ST limit.

During the design phase, the TOE is administrated by the development department.

During the manufacturing phase, the TOE is administrated by the manufacturing department. The main responsibility related to TOE administration during this phase relates to TOE personalisation and insertion of security data.

The TOE is then delivered.

IV. TOE SECURITY ENVIRONMENT

This chapter describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. It includes a description of assumptions on the environment of the TOE, of threats to the assets against which specific protection within the TOE or its environment is required, and of organisational security policies.

IV.1 SECURE USAGE ASSUMPTIONS

This paragraph describes the secure usage assumptions on the environment of a Motion Sensor, as defined in [3821_1B].

A.Controls ..... Law enforcement controls will be performed regularly and randomly, and will include security audits as well as visual inspection of the equipment.

A.Periodic_Inspections ..... Periodic inspections of the equipment fitted to the vehicles will take place at least once within two years (24 months) of the last inspection.

A.Trusted_Workshops ..... The Member States will approve, regularly control and certify fitters and workshops to carry out installations, checks, inspections and repairs.

IV.2 THREATS

This paragraph describes the threats to the assets against which specific protection within the TOE or its environment is required. A threat is generally described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack.

The main assets to be protected are the data, held in or measured by the IS2000. Derived assets to be protected are the IS2000 software and hardware. Security data supporting security mechanisms are secondary assets to protect.

The threat agents to these assets may be:

- Authorised users with no expertise, who can try to tamper with motion sensors installed in their vehicles,
- Hostile users or companies with high expertise, motivation and large resources.

All these threats are derived from the document [1B_10] (chapter 3.3, p.8) and address the user data described above.

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

T.Faults ..... Faults in hardware, software, communication procedures could place the IS2000 in unforeseen conditions compromising its security.

T.Tests ..... The use of non invalidated test modes or of existing back doors could compromise the IS2000 security.

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

T.Environment..... Users could compromise the IS2000 security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical…).

T.Hardware..... Users could try to modify IS2000 hardware.

T.Mechanical ..... Users could try to manipulate the MS input (e.g. unscrewing it 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 IS2000 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 IS2000 software.

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

IV.3 ORGANISATIONAL SECURITY POLICIES

The following security policy is derived from the global security analysis of the whole tachograph system and is compliant to the main security objectives assigned to a motion sensor by [1B_10] (Chapter 3.4, p.9).

P.IS2000_Main..... The data transmitted by the IS2000 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.

V. SECURITY OBJECTIVES

This chapter defines the security objectives for the TOE and its environment. The security objectives address all of the security environment aspects identified, are suitable to counter all identified threats, and cover all identified organisational security policy and assumptions.

V.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives the IS2000 shall achieve are the following. These objectives are derived from the document [1B_10] (chapter 3.5, p.9).

O.Access..... The IS2000 shall control connected entities' access to functions and data.

O.Audit..... The IS2000 shall audit attempts to undermine its security and should trace them to associated entities.

O.Authentication ..... The IS2000 shall authenticate connected entities.

O.Data_Exchange..... The IS2000 shall secure data exchanges with the VU.

O.Phys_Protection..... The IS2000 shall be designed such that it is not openable, and that any attempt to open it, will be clearly identifiable through visual inspection.

O.Processing..... The IS2000 shall ensure that processing of input to derive motion data is accurate.

O.Reliability ..... The IS2000 shall provide a reliable service.

O.Mech_Interface..... Means of detecting physical tampering with the mechanical interface must be provided (for example, using seals).

V.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The security objectives that the IS2000 environment shall achieve are the following. These objectives are derived from the document [1B_10] (chapter 3.6, p.9).

V.2.1 Design phase

OE.Dvpt_Security ..... IS2000 developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

OE.Reliable_Design..... IS2000 developers should design the MS such as to minimise potential design flaws.

OE.Software_Analysis ..... IS2000 design shall be such that there shall be no way to analyse or debug software in the field.

OE.Software_Upgrade..... Software revisions shall not be possible for the IS2000.

V.2.2 Manufacturing phase

OE.Data_Generation..... Security data generation algorithms shall be accessible to authorised and trusted persons only.

OE.Data_Transport ..... Security data shall be generated, transported, and inserted into the IS2000, in such a way to preserve its appropriate confidentiality and integrity.

OE.Mnft_Security ..... The IS2000 manufacturer shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the IS2000 is protected from physical attacks which might compromise IT security.

OE.Manufacturing ..... The IS2000 manufacturer shall ensure that manufacturing conforms with design.

OE.Personalisation ..... The IS2000 manufacturer shall personalise the equipment before delivery. The personalisation shall be feasible once only, during the manufacturing phase.

OE.Tests_Points..... All commands, actions or test points, specific to the testing needs of the manufacturing phase of the IS2000 shall be disabled or removed before delivery. It shall not be possible to restore them for later use.

V.2.3 Delivery

OE.Users..... Users shall be informed of their responsibility when using the TOE. Fitters and Workshops shall particularly be informed of their responsibility related to proper sealing of the mechanical interface.

V.2.4 Product usage phase

OE.Controls ..... Law enforcement controls shall be performed regularly and randomly, and shall include security audits as well as visual inspection of the equipment.

OE.Periodic_Inspections.. Periodic inspections of the equipment fitted to the vehicles shall take place at least once within two years (24 months) of the last inspection.

OE.Trusted_Workshops.. The Member States shall approve, regularly control and certify fitters and workshops to carry out installations, checks, inspections and repairs.

VI. IT SECURITY REQUIREMENTS

This chapter defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

VI.1 TOE SECURITY REQUIREMENTS

VI.1.1 TOE Security Functional Requirements

These requirements are derived from the document [1B_10] (chapter 4, p.11 to 13).

The chosen components are described below.

Component	Description	Operation
FAU_GEN.1	Audit data generation	Yes
FAU_SAR.1	Audit review	Yes
FCS_CKM.1	Cryptographic key generation	Yes
FCS_CKM.2	Cryptographic key distribution	Yes
FCS_CKM.3	Cryptographic key access	Yes
FCS_CKM.4	Cryptographic key destruction	Yes
FCS_COP.1	Cryptographic operation	Yes
FDP_ACC.2	Complete access control	Yes
FDP_ACF.1	Security attribute based access control	Yes
FDP_IFC.1	Subset information flow control	Yes
FDP_IFF.1	Simple security attributes	Yes
FDP_SDI.1	Stored data integrity monitoring	Yes
FDP_UIT.1	Data exchange integrity	Yes
FIA_AFL.1	Authentication failure handling	Yes
FIA_UAU.2	User authentication before any action	
FIA_UAU.3	Unforgeable authentication	Yes
FIA_UID.2	User identification before any action	Yes
FPT_AMT.1	Abstract machine testing	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
FPT_PHP.1	Passive detection of physical attack	
FPT_TST.1	TSF testing	Yes
FTP_ITC.1	Inter-TSF trusted channel	Yes

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events :

a) Start-up and shutdown of the audit functions.

b) All auditable events for the *minimum* level of audit ; and

c) *none*.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information :

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

Note : In accordance with (AUD_103) and (AUD_104), the audit record is sent to the VU for storage by the VU, which is able to time stamp the event. The Motion sensor will not be able to provide a reliable dating by itself. An alternate means will consist in adding in the record a random number given by the V.U. that will be associated to an effective date.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the following audit relevant information :*

- *none*

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide *authorised users* with the capability to read *appropriate audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet the following:

Purpose	**Algorithm and size**	**Key generation specification**
Diversified Transport Key	2 Key TDES	TDES

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified key distribution method that meets the following:

Distributed key	**Distribution method / Reference**
Pairing key to Vehicle Unit	[ISO 16844-3] 7.4.3

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform *cryptographic key accesses* in accordance with a specified cryptographic key access method that meets the following :

Key	**Key access method and reference**
Pairing Key	Stored during IS2000 personalisation.
Session Key	Sent by vehicle unit (encrypted), and temporarily stored. [ISO 16844-3] 7.4.4
Transport key	Stored during manufacturing (hard coded).
Diversified Transport Key	Internally computed from Transport key.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following :

Key	**Key destruction method**
Session key	Replacement
Diversified Transport Key	Modification of key value

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *cryptographic operations* in accordance with a specified cryptographic algorithm and cryptographic key sizes that meets the following :

Cryptographic operations	**Crypto algorithms, and key size**
Encryption Decryption	Triple DES – 2 key option ECB and CBC modes.
MACs	Triple DES – 2 key option.

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the *functions_access_policy* on *functions* and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the *MS_data_access_policy* on *data memory* and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the *file_structure_policy* on *data memory* and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 **Security attribute based access control**

FDP_ACF.1.1 The TSF shall enforce the *functions_access_policy* to objects based on *the connected entity identity.*

The TSF shall enforce the *MS_data_access_policy* to objects based on *data types.*

The TSF shall enforce the *file_structure_policy* to objects based on *files attributes.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

- *functions_access_policy : the 'send data' and 'pairing' functions are accessible to authenticated VUs.*
- *MS_data_access_policy :*
  - *identification data, static security data and pairing data related to first pairing are written once only*
  - *security data may not be read from outside.*
- *file_structure_policy : Application and data files structure and access conditions are created during the manufacturing process, and then locked from any future modification or deletion.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules : *none*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules : *none.*

FDP_IFC.1 **Subset information flow control**

FDP_IFC.1.1 The TSF shall enforce the *VU_data_exchange_policy* on *motion data sent to the vehicle unit.*

The TSF shall enforce the *pairing_data_policy* on the *initial authentication process.*

The TSF shall enforce the *data_flow_policy* on the *data transfers and processings.*

FDP_IFF.1 **Simple security attributes**

FDP_IFF.1.1 The TSF shall enforce the *VU_data_exchange_policy* based on the following types of subject and information security attributes : *data attributes,*

The TSF shall enforce the *pairing_data_policy and the data_flow_policy* based on the following types of subject and information security attributes : *none.*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold :

- *VU_data_exchange_policy : The motion sensor shall export motion data to the vehicle unit with security attributes, such that the vehicle unit will be able to verify its integrity and authenticity.*

FDP_IFF.1.3 The TSF shall enforce the *additional information flow control rules:*

- *data_flow_policy : The IS2000 shall ensure that motion data may only be processed and derived from its mechanical input.*

FDP_IFF.1.4 The TSF shall provide the following *additional SFP capabilities:*

- *pairing_data_policy : The IS2000 shall, as part of the authentication process, update, as needed (ACT_102), pairing data stored in its memory.*

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules : *none.*

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules : *none.*

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.A a) Minimal : *stored data integrity error*

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for *integrity errors* on all objects, based on the following attributes : *data type (with a checksum).*

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the *VU_data_exchange_policy* to be able to *transmit* user data in a manner protected from *modification, deletion and insertion* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *none* has occurred.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1A a) Minimal : *the reaching of the threshold for the unsuccessful authentication attempts*.

FIA_AFL.1.1 The TSF shall detect when *at most 20 consecutive* unsuccessful authentication attempts occur related to *VU authentication.*

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

- *Generate an audit record of the event,*
- *Warn the entity,*
- *Continue to export non secured motion data to the VU (real time speed signal).*

FIA_UAU.2	**User authentication before any action**
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.3	**Unforgeable authentication**
FIA_UAU.3.1	The TSF shall *detect and prevent* use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall *detect and prevent* use of authentication data that has been copied from any other user of the TSF.
FIA_UID.2	**User identification before any action**
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
FPT_AMT.1	**Abstract machine testing**
FPT_AMT.1A	a) Minimal : *test failure (IS2000 internal fault).*
FPT_AMT.1.1	The TSF shall run a suite of tests *during initial start-up, and during normal operation* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF *(RLB_102).*
FPT_FLS.1	**Failure with preservation of secure state**
FPT_FLS.1	The TSF shall preserve a secure state when the following types of failures occur: *power supply deviation (RLB_109, RLB_110).*
FPT_PHP.1	**Passive detection of physical attack**
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_TST.1	**TSF testing**
FPT_TST.1A	a) Minimal : *test failure (IS2000 internal fault).*
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up, and during normal operation* to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code *(RLB_102).*

FTP_ITC.1	**Inter-TSF trusted channel**
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *the VU* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for : *none*.

VI.1.2 TOE Security Assurance Requirements

The assurance level required by the European Regulation for a Motion Sensor is an ITSEC E3 High level ([1B_10]).

A CC assurance package, providing a technical correspondence as close as possible from the required ITSEC assurance level, has therefore been selected from Common Criteria part 3, with a minimum strength of functions claim of **SOF-high**, consistent with the TOE Security Objectives.

Class	**Component**	**Description**
ACM Configuration management	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL.2	Detection of modifications
	ADO_IGS.2	Generation log
ADV Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_TAT.1	Well-defined development tools
ATE Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.4	Highly resistant

ADO_IGS.2 is selected with the interpretation / refinement according to [JIL] 41.
No other refinement are made to the above security assurance requirements.

VI.2 TOE ENVIRONMENT SECURITY REQUIREMENTS

There is no security functional requirements for the IT environment.

VII. TOE SUMMARY SPECIFICATION

The main purpose of this section is to specify the TOE-specific solution to the identified security needs, showing how the TOE provides the security functions and assurance measures to satisfy the defined TOE security requirements.

VII.1 TOE SECURITY FUNCTIONS

The TOE security functions are not described in this public version of the document, however these functions are listed in section IX.3 “Security functions rationale”.

VII.2 ASSURANCE MEASURES

This section providing a general mapping from the documentation or evidence the developer intends to provide to the appropriate assurance measures is not available in the public version of the document.

VIII. PP CLAIMS

None.

IX. RATIONALE

IX.1 SECURITY OBJECTIVES RATIONALE

These rationale are derived from the document [1B_10] (chapter 8, p.15 & 16). These rationale demonstrate that the identified security objectives are suitable, addressing all aspects of the security needs as specified in the TOE Security Environment.

IX.1.1 Mapping the security objectives to the TOE security environment

			TOE Security Environment														
			Assumptions			Threats											Policy
			A.Controls	A.Periodic_Inspections	A.Trusted_Workshops	T.Access	T.Faults	T.Tests	T.Design	T.Environment	T.Hardware	T.Mechanical	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	P.IS2000_Main
Security Objectives	TOE	O.Access				X											X	
		O.Audit				X											X	
		O.Authentication				X												
		O.Data_Exchange											X					X
		O.Phys_Protection							X	X	X				X	X	X	
		O.Processing															X	X
		O.Reliability					X			X				X			X	X
		O.Mech_Interface										X						
	TOE Environment	OE.Dvpt_Security					X		X		X					X		
		OE.Reliable_Design					X			X				X			X	
		OE.Software_Analysis														X		
		OE.Software_Upgrade					X									X		
		OE.Data_Generation													X			
		OE.Data_Transport													X			
		OE.Mnft_Security							X		X				X	X		
		OE.Manufacturing					X				X					X		
		OE.Personalisation											X		X			X
		OE.Tests_Points						X										
		OE.Users										X						
		OE.Controls	X						X		X	X		X				
		OE.Periodic_Inspections		X					X		X	X		X				
		OE.Trusted_Workshops			X							X						

IX.1.2 Policies

P.IS2000_Main..... The data transmitted by the IS2000 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.

The O.Data_Exchange secures data exchanges. The O.Processing and the O.Reliability objectives contribute to addressing the policy by ensuring the accuracy of the whole process. The OE.Personalisation provides the IS2000 with necessary permanent identification data.

IX.1.3 Threats

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

T.Access is addressed by the O.Authentication objective to ensure the identification of the user, the O.Access objective to control access of the user to functions and the O.Audit objective to trace attempts of unauthorised accesses.

T.Faults..... Faults in hardware, software, communication procedures could place the IS2000 in unforeseen conditions compromising its security.

T.Faults is mostly addressed by the OE.Reliable_Design, and OE.Dvpt_Security objectives for the environment in order to obtain as good a design as possible, by the OE.Manufacturing objective to ensure that manufacturing will correctly follow the design. The O.Reliability objective contributes to address the threat by providing a fault tolerant design. The OE.Software_Upgrade objective contributes to address the threat by preventing software upgrades.

T.Tests ..... The use of non invalidated test modes or of existing back doors could compromise the IS2000 security.

The OE.Tests_Points objective for the environment ensures that no test modes nor back doors remain usable when the tests are finished during the manufacturing phase.

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

The OE.Dvpt_Security and the OE.Mnft_Security objectives ensure that development and manufacturing maintain security. The O.Phys_Protection objective contributes to address the threat in conjunction with the OE.Controls and OE.Periodic_Inspections objectives.

T.Environment..... Users could compromise the IS2000 security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical…).

T.Environment is mostly addressed by the OE.Reliable_Design objective in order to obtain as good a design as possible, and by the O.Phys_Protection objective to ensure that direct attacks cannot be made inside the equipment. The O.Reliability objective contributes to address the threat by providing a failure tolerant design.

T.Hardware..... Users could try to modify the IS2000 hardware.

T.Hardware is mostly addressed in the user environment by the O.Phys_Protection objective. During design and manufacture, T.Hardware is addressed by the OE.Dvpt_Security, OE.Mnft_Security and OE.Manufacturing objectives. The OE.Controls and OE.Periodic_Inspections help addressing the threat through visual inspection of the installation.

T.Mechanical ..... Users could try to manipulate the IS2000 input (for example, unscrewing it from gearbox).

T.Mechanical is addressed by the O.Mech_Interface objective. The OE.Controls and OE.Periodic_Inspections objectives contribute to addressing the threat by revealing attempts to manipulate the MS input ; the OE.Trusted_Workshops and OE.Users objectives contribute also by ensuring the IS2000 will be and remain properly sealed during installation and normal use.

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

T.Motion_Data is addressed by the O.Data_Exchange objective by securing data exchanges. The OE.Personalisation prevents the use of a fake IS2000.

T.Power_Supply ... Users could try to defeat the IS2000 security objectives by modifying (cutting, reducing, increasing) its power supply.

T.Power_Supply is mainly addressed by the OE.Reliable_Design and the O.Reliability objectives to ensure appropriate behaviour of the IS2000 against the attack. The OE.Controls and OE.Periodic_Inspections allows checking of the IS2000 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.

The OE.Data_Generation limits the generation algorithms knowledge spreading and the OE.Data_Transport secures security data' confidentiality and integrity during generation, transport and insertion in the MS. The OE.Mnft_Security objective ensures security in the manufacturing environment. The OE.Personalisation prevents the use of fake devices. The O.Phys_Protection objective ensures appropriate protection of security data while stored in the IS2000.

T.Software..... Users could try to modify the IS2000 software.

T.Software is mostly addressed in the user environment by the OE.Software_Analysis objective to prevent software analysis in the field and by the O.Phys_Protection to prevent physical tampering with the code. The OE_Software_Upgrade prevents any software upgrade. The OE.Dvpt_Security and OE.Mnft_Security objectives address the threat in the development and manufacturing environments. The OE.Manufacturing requires a conform-to-design manufacturing, preventing software alteration.

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

T.Stored_Data is addressed mainly by the OE.Reliable_Design and O.Access objectives to ensure that no illicit access to data is permitted. The O.Audit objective contributes to address the threat by recording data integrity errors. The O.Processing and O.Reliability objectives contribute also to address the threat. The O.Phys_Protection provides means to prevent physical attacks, which protects stored data.

IX.2 SECURITY REQUIREMENTS RATIONALE

These rationale demonstrate that the identified IT security requirements (and the SFRs in particular) are suitable to meet the identified security objectives and that all dependencies between SFRs and SARs are solved.
The following table demonstrates that the SFRs are necessary to satisfy the security objectives.

				O.Access	O.Audit	O.Authentication	O.Phys_Protection	O.Data_Exchange	O.Processing	O.Reliability	O.Mech_Interface
FAU	**GEN**	**1**	Audit data generation		X						
FAU	**SAR**	**1**	Audit review		X						
FCS	**CKM**	**1**	Cryptographic key generation			X					
FCS	**CKM**	**2**	Cryptographic key distribution			X					
FCS	**CKM**	**3**	Cryptographic key access			X		X			
FCS	**CKM**	**4**	Cryptographic key destruction			X					
FCS	**COP**	**1**	Cryptographic operation			X		X			
FDP	**ACC**	**2**	Complete access control	X					X		
FDP	**ACF**	**1**	Security attribute based access control	X					X		
FDP	**IFC**	**1**	Subset information flow control			X		X	X		
FDP	**IFF**	**1**	Simple security attributes			X		X	X		
FDP	**SDI**	**1**	Stored data integrity monitoring		X						
FDP	**UIT**	**1**	Data exchange integrity					X			
FIA	**AFL**	**1**	Authentication failure handling		X	X					
FIA	**UAU**	**2**	User authentication before any action			X					
FIA	**UAU**	**3**	Unforgeable authentication			X					
FIA	**UID**	**2**	User identification before any action	X	X						
FPT	**AMT**	**1**	Abstract machine testing		X				X	X	
FPT	**FLS**	**1**	Failure with preservation of secure state						X	X	
FPT	**PHP**	**1**	Passive detection of physical attack				X				X
FPT	**TST**	**1**	TSF testing		X				X	X	
FTP	**ITC**	**1**	Inter-TSF trusted channel					X			

The following table demonstrates that the SFRs are sufficient to satisfy the security objectives.

Security objectives	IT security requirements
O.Access	FDP_ACC.2 : .... Controls access to IS2000 data and functions FDP_ACF.1 : ..... Defines security attributes of IS2000 data and functions FIA_UID.2 : ..... Identifies entity or process acting for the entity, before any action
O.Audit	FAU_GEN.1 :.... Generates correct audit records FAU_SAR.1 : .... Provides audit records to authorised user FDP_SDI.1 ..... Provides stored data integrity errors events FIA.AFL.1 : ..... Provides authentication failure events FIA_UID.2 : ..... Identifies entity or process acting for the entity, before any action FPT_AMT.1, FPT_TST.1 : Provide failure events
O.Authentication	FCS_CKM.1 :.... Diversifies the transport key to secure security data import during personalisation. Those security data are used by the authentication process. FCS_CKM.2 :.... Controls distribution of keys by the IS2000 to the VU during the authentication process FCS_CKM.3 :.... Controls access to the keys stored in the IS2000 FCS_CKM.4 :.... Controls destruction of session key, which is no more used FCS_COP.1 : ..... Provides cryptographic operations to authenticate entity FDP_IFC.1, FDP_IFF.1 : Ensure the integrity of identification and security data needed by the authentication process FIA_AFL.1 : ..... Controls authorised number of unsuccessful authentication FIA_UAU.2 : ..... Authenticates entity or process acting for the entity, before any action FIA_UAU.3 : ..... Prevent forgeable authentication of entities

Security objectives	IT security requirements
O.Phys_Protection	FPT_PHP.1 :..... Ensures physical attacks on the IS2000 may be easily detected
O.Data_Exchange	FCS_CKM.3 :.... Controls access to the session key stored in the IS2000 FCS_COP.1 :..... Provides cryptographic operations to secure data exchanges FDP_IFC.1, FDP_IFF.1 : Ensures integrity of commands received from the VU FDP_UIT.1 :..... Controls data exchanges to prevent accepting incorrect data FTP_ITC.1 :..... Ensures trusted channel between the IS2000 and the VU
O.Processing	FDP_ACC.2, FDP_ACF.1 : ..... Control access to IS2000 data and functions FDP_IFC.1, FDP_IFF.1 : Control data flows in the IS2000 FPT_FLS.1 :..... Preserves a secure state of the IS2000 when failure occurs FPT_AMT.1, FPT_TST.1 : ..... Self-tests demonstrate correct operation of data processing
O.Reliability	FPT_FLS.1 :..... Preserves a secure state of the IS2000 when failure occurs FPT_AMT.1, FPT_TST.1 : Self-tests demonstrate correct operation of the IS2000
O.Mech_Interface	FPT_PHP.1 :..... Ensures physical attacks on the IS2000 mechanical interface may be easily detected

The following table demonstrates and justifies that all dependencies between SFRs and SARs are solved.

IT security requirements	Dependencies
FAU_GEN.1	FPT_STM.1 : .....not selected, because the VU it-selfs shall manage reliable time and link it up to the audit received
FAU_SAR.1	FAU_GEN.1 : .....selected
FCS_CKM.1	FMT_MSA.2 : .....not selected, because there is no need for management of security attributes in the IS2000 FCS_CKM.4 : .....selected [FCS_CKM.2 or FCS_COP.1] : both selected.
FCS_CKM.2	FMT_MSA.2 : .....not selected, because there is no need for management of security attributes in the IS2000 FCS_CKM.4 : .....selected [FCS_CKM.1 or FDP_ITC.1] : FCS_CKM.1 selected.
FCS_CKM.3	FMT_MSA.2 : .....not selected, because there is no need for management of security attributes in the IS2000 FCS_CKM.4 : .....selected [FCS_CKM.1 or FDP_ITC.1] : FCS_CKM.1 selected.
FCS_CKM.4	FMT_MSA.2 : .....not selected, because there is no need for management of security attributes in the MS [FCS_CKM.1 or FDP_ITC.1] : FCS_CKM.1 selected.
FCS_COP.1	FMT_MSA.2 : .....not selected, because there is no need for management of security attributes in the MS FCS_CKM.4 : .....selected [FCS_CKM.1 or FDP_ITC.1] : FCS_CKM.1 selected.
FDP_ACC.2	FDP_ACF.1 : .....selected
FDP_ACF.1	FMT_MSA.3 : .....not selected, because there is no need for management of security attributes in the MS FDP_ACC.1 :.....selected as hierarchically inferior to FDP_ACC.2
FDP_IFC.1	FDP_IFF.1 : .....selected

IT security requirements	Dependencies
FDP_IFF.1	FDP_IFC.1 :.....selected FMT_MSA.3 : .....not selected, because there is no need for management of security attributes in the IS2000
FDP_SDI.1	None
FDP_UIT.1	[FCS_ACC.1 or FDP_IFC.1] : ..... FDP_ACC.2 [FTP_ITC.1 or FTP_TRP.1] :..... FTP_ITC.1 selected
FIA_AFL.1	FIA_UAU.1 : .....selected
FIA_UAU.2	FIA_UID.1 :.....selected
FIA_UAU.3	None
FIA_UID.2	None
FPT_AMT.1	None
FPT_FLS.1	ADV_SPM.1 :.....not selected, because assurance requirement not needed at the assurance level sought
FPT_PHP.1	FMT_MOF.1 : .....not selected, because there is no need for management of security functions in the MS
FPT_TST.1	FPT_AMT.1 : .....selected
FTP_ITC.1	None

IX.3 SECURITY FUNCTIONS RATIONALE

These rationale demonstrate that the identified IT security functions cover all security functional requirements and that each IT security function is mapped onto at least one security functional requirement.

The following table demonstrates that the identified IT security functions are necessary to satisfy the security functional requirements.

	F.Personalisation	F.Events_Faults_Management	F.Pairing	F.Data_Exchange	F.Self_Tests	F.Power_Supply_Management	F.Seals	F.Tamper_Resistant_Cover
FAU_GEN.1		X		X	X			
FAU_SAR.1				X				
FCS_CKM.1	X							
FCS_CKM.2			X					
FCS_CKM.3	X		X					
FCS_CKM.4	X		X					
FCS_COP.1	X		X	X				
FDP_ACC.2	X		X	X				
FDP_ACF.1	X		X	X				
FDP_IFC.1			X	X				X
FDP_IFF.1			X	X				X
FDP_SDI.1					X			
FDP_UIT.1				X				
FIA_AFL.1				X				
FIA_UAU.2			X	X				
FIA_UAU.3			X	X				
FIA_UID.2			X	X				
FPT_AMT.1					X			
FPT_FLS.1						X		
FPT_PHP.1							X	X
FPT_TST.1					X			
FTP_ITC.1			X	X				

The following table demonstrates that the identified IT security functions are sufficient to satisfy the security functional requirements.

IT security requirements	Security functions
FAU_GEN.1	F.Data_Exchange, F.Self_Tests : Raise events or faults. F.Events_Faults_Management : .....Generates records of events or faults.
FAU_SAR.1	F.Data_Exchange :.....Warns the VU that an audit record is available, and allows the VU to read the audit record
FCS_CKM.1	F.Personalisation : .....Diversifies the Transport key to generate a Diversified transport key.
FCS_CKM.2	F.Pairing : .....Distributes a 'pairing key' to the VU
FCS_CKM.3	F.Personalisation : .....Provides the pairing key for storage in the IS2000 memory, provides the Diversified transport key. F.Pairing : .....Provides the session key.
FCS_CKM.4	F.Personalisation : .....Controls destruction of Diversified transport key when no more needed. F.Pairing : .....Controls destruction of obsolete session key
FCS_COP.1	F.Personalisation : .....Performs TDES decryptions and verifies MACs when importing static security data. F.Pairing, F.Data_Exchange : Perform TDES encryption and decryption of data with a pairing key and/or a session key.
FDP_ACC.2	F.Personalisation: .....Enforces the MS_data_access_policy (1st part), F.Pairing: .....Enforces the MS_data_access_policy (2nd part) and the functions_access_policy (2nd part), F.Data_Exchange :.....Enforces the functions_access_policy (1st part).
FDP_ACF.1	F.Personalisation: .....Enforces the MS_data_access_policy (1st part), F.Pairing: .....Enforces the MS_data_access_policy and the functions_access_policy (2nd part), F.Data_Exchange :.....Enforces the functions_access_policy (1st part).
FDP_IFC.1	F.Pairing : .....Enforces the pairing_data_policy, F.Data_Exchange :.....Enforces the VU_data_exchange_policy, F.Tamper_Resistant_Cover: Enforces the data_flow_policy.
FDP_IFF.1	F.Pairing : .....Enforces the pairing_data_policy, F.Data_Exchange :.....Enforces the VU_data_exchange_policy, F.Tamper_Resistant_Cover: Enforces the data_flow_policy.
FDP_SDI.1	F.Self_Tests .....Verify stored data integrity F.Personalisation, F.Pairing: .....Compute and store checksum when storing data

IT security requirements	Security functions
FDP_UIT.1	F.Data_Exchange :.....Provides data to the VU: ♦ encrypted and with a redundancy function such that the VU will be able to detect modifications, ♦ and with a VU generated random embedded such that the VU will detect deletion or insertion errors.
FIA_AFL.1	F.Data_Exchange :.....Raises an authentication failure event after at most 20 unsuccessful authentication of the VU.
FIA_UAU.2	F.Pairing : .....Authenticates the VU during pairing sequence (initial authentication). F.Data_Exchange :.....Authenticates the VU regularly during normal operation
FIA_UAU.3	F.Pairing, F_Data_Exchange : Will not provide services if authentication data is forged. F.Data_Exchange :.....Verifies the continuity of dialogs with the VU to prevent use of copied data.
FIA_UID.2	F.Pairing : .....Authenticates the VU and establishes its identity during pairing sequence F.Data_Exchange :.....Verifies continuity of dialogs with the VU regularly during normal operation
FPT_AMT.1	F.Self_Tests : .....Runs hardware tests to verify correct IS2000 operation
FPT_FLS.1	F.Power_Supply_Management : .....Ensures the preservation of a secure state and proper reset in case of over-voltage or voltage drop
FPT_PHP.1	F.Seals, F.Tamper_Resistant_Cover : .....Ensure that physical tampering will be easily detectable by visual inspection
FPT_TST.1	F.Self_Tests : .....Runs software tests to verify correct IS2000 operation
FPT_ITC.1	F.Pairing : .....Ensures mutual authentication with the VU and receipt of the session key F.Data_Exchange :.....Uses session key to decrypt or encrypt transmitted data.

X. GLOSSARY

CC ..... Common Criteria
DES ..... Data Encryption Standard
EAL..... Evaluation Assurance Level
IT..... Information Technology
MAC ..... Message Authentication Code
MS..... Motion Sensor
PP..... Protection Profile
SF ..... Security Function
SFP..... Security Function Policy
SOF ..... Strength Of Function
ST..... Security Target
TBD..... To Be Defined
TDES..... Triple DES
TOE..... Target Of Evaluation
TSC ..... TSF Scope of Control
TSF..... TOE Security Functions
TSFI..... TSF Interface
TSP..... TOE Security Policy
VU ..... Vehicle Unit