HOMOLOGATION DIRECTIVE

BV03

ELEKTRONIC

SECURTITYSYSTEMS FOR

HGV'S

SCM, Stichting Certificering Motorrijtuigbeveiliging
Postbus 393
2900 AJ CAPELLE A/D IJSSEL (Netherlands)

PREFACE

Information coming from different sources, like insurers and police forces, indicate a loss of millions of Euro's due to theft off en from HGV's. It is reasonable to accept the fact that these estimations could be too low since the registration of cargo theft is influenced by many factors due to its cross boader aspects.
To reach a well accepted view about the requirements that can be opposed by insurers to get a sufficient level of security, it is necessary to get the right information about the possibilities to use electronic and mechanical security devives and also about the Modus Operandi of the criminals that are attracted to the (high) value of the cargo.

In addition to a wide scale of organisational measures that can be taken to limit the chances of theft, we can use a lot of techno preventive measures on the vehicle.
These technical measueres against theft can be divide in two categories:

- Electronic security systems
- Mechnical security devices

This security will only be effective when applied in combination.

For an overview of the possibilities to prevent theft from and of HGV's, we refer to the report "Prevention against theft from and of HGV's", available at the SCM-office (only in Dutch).
For the requirements for mechanical security devices we refer to the SCM-Directive MP03.

The SCM-Directive BV03 is created with the intention to set minimum requirements to the theft preventive quality of electronic security systems for HGV's. Under HGV's we gather vehicles , specially constructed to carry cargo with a minimum weight of 3500 KG.
Vehicles with a weight up to 7500 KG. Or with a battery supply of 12 Volt may also use the Directive AA03 for passenger cars.

In setting up this directive, two points are essential:

1. Insurers need, for advsing their customers, a clear and simpel system to differentiate the good from the poor systems, including the installation.

2. Testing and certification of the security systems for HGV's must be in line with the other developments in the area of vehicle security.

The approval scheme requires a Homologation Directive to be set up by the SCM and approval certificates to be issued by the SCM. Testing can be performed by accredited test houses which hold a contract with the SCM. In this contract all the aspects for the quality control are determined.
For more detailed information see the passenger car Directive AA03 – appendix 1.

INTRODUCTION

The SCM Homologation Directive on "Heavy Goods Vehicles", hereinafter referred to as: the "Directive", is issued by SCM-Stichting Certificering Motorrijtuigbeveiliging (Institute for the Certification of Vehicle security systems).

This Directive has, under the auspices of the College of Experts of the SCM, been drawn up by the sub work-group “Electronic security systems for HGV’s”. This workgroup is composed of representatives from:

* Importers of security systems
* HGV importers
* SCM
* Transport organisations
* Insurers

This Homologation Directive can be divided in three parts:

-	Scope and Definitions	Chapter 2 - 3
-	Technical and administrative requirements	Chapter 4 - 5
-	Testprocedures	Chapter 6

In Scope and Definitions all relevant information about the SCM Directive is mentioned.

In the Technical and administrative requirements, procedures and requirements are written down, applicable for the type approval and the production of approved systems as well as rules and conditions for manufacturers and / or importers of approved systems.
For this there is a distinction in two categories of systems:

A. OE-systems
B. AM-systems

In Testprocedures the conditions for testing and the procedures are published.

2 SCOPE

2.1 General

This Directive is applicable for security systems to be used for installation in vehicles (OE and AM) in use for carrying passengers or goods with a maximum mass of 7500 KGs.

Automotive components used to set and unset securitysystems are considered to be system components and must therefor be submitted for homologation.

All system components must meet the Homologation Requirements and be delivered complete in one package. Type identifications and/or the brandname under which the type approval is granted, must be provided on the most significant, not visible from the outside, parts while parts, visible from the outside (e.g. US-sensors) shall not be marked with a recognisable identification.

The PC board or the housing of the CCU and the siren must be provided with a production code. This could be a software code

If the system or a system component is integrated with equipment intended for other purposes, such equipment shall meet the homologation requirements to the extent it affects system operation.

Security systems that can be unset by means of remote control shall have a second unsetting method, installed in the vehicle. This is not applicable for transponder operated systems nor for OE-systems in vehicles where the manufacturer guarantees a Europe wide working 24 hour mobility system.

2.2 Term of Validity and Entrance date of the Homologation Directive

The entrance date of this Directive BV03 is January 1st, 2003. At that date the present Directives will be no longer valid. Existing approvals under BV02 will be valid until July 1st, 2004.
In this period the existing BV02 approval van be transferred to BV03, with the necessary additional testing.

The approvals issued under this Directive shall be valid up to and including one year after the lapse of the Directive. During this year, repeat inspections can be carried out on the basis of the homologation requirements according to which the type approval has been issued.

2.3 Legal requirements

If a particular system or system component should be subject to any requirements pursuant to Dutch or European legislation, they should meet such requirements (e.g. EU 95/56 and EU 95/54).

If the security system uses radio frequencies, e.g. for unsetting or detection, these systems shall comply with the relevant European standards.

System components that exert influence on vehicle components, which are of importance to road safety and defined as such by legislation, shall have an approval granted by the Rijksdienst voor het Wegverkeer (Department for Road Traffic).

The security system shall be designed and installed in such a way that any vehicle, after installation, will continue to comply with the vehicle type approval.

2.4 Roadsafety requirements

The security system shall in no state (set or unset) cause any harm to road safety.

The system shall not interfere with or be connected to (any part of) the brake system of the vehicle unless with written consent of the manufacturer of that vehicle.

The audible warning device shall not cause any confusion as to the reason of the warning and shall therefore not have any similarity to warning signals used by the police, fire brigade or ambulances and the like, nor to any existing horns used for traffic warning.

The use of anti-kidnap or panic functions, for activating the warning devices during the unset or set condition, is only permitted if this switch is mounted in the vehicle.

The use of high beam/low beam lights for optical warning shall not be permitted.

It is not permitted to start the vehicle from the outside with the remote control that belongs to the securitysystem.

2.5 Documents

The system must be supplied with user manual and installation instructions, specific to the system supplied, and drafted in at least the Dutch language. In case of vehicle bounded instructions the installation instruction may be in one of the official European languages.

The user manual shall at least include:

- operating conditions
- operating instructions
- prevention of unnecessary alarm
- actions to be undertaken in case of malfunction / defects
- a summary of system components, relevant to the user

The installation instructions shall at least include:

- plan of the system components
- installation and wiring diagrams
- testing with checklist
- trouble shooting
- periodic maintenance with checklist
- a summary of the system components

3. DEFINITITIONS OF TERMS

3.1 Definitions

- Alarmcondition: condition of the system in which the warning devices have been activated. This occurs immediately after the detection of a detector. The immobilisation stays active during this condition.
- Alarmcycle: time in which the audible warning occurs.
- Alarmsystem: an electronic securitysystem for passengercars with a powersupply of max. 24 V DC, at least consisting of a CCU, a siren, perimeter- and interiordetection, an in- and unsetting system, switch (es), suitable for bonnet / luggagecompartment, a cableharness as well as a statusdisplay of the systemcondition. In addition a users direction and (in case of after market) an installation manual.
- AM-system: system installed after deliverance of the vehicle.
- Anti-hijacksystem: system where an alarm is activated if the driver does not deactivate the system within a certain timelimit.
- Approvalholder: principal for a test on a securitysystem that has been approved.
- Attack time: the time in which a lock withstands an attack test in such a manner that the system is not unset.
- Audible warning device: warning signal by means of a siren.
- Battery backup siren: a device which, if the powersupply by the vehicle battery should fail, supplies the siren with electric power and activates it.
- Cable: single core wire for transport of energy in a vehicle.
- Change in alarmcondition: detection by a different detector or group of detectors.
- CCU: central control unit of the securitysystem.
- Coded link: a signal (only for cableconnections) with a minimum number of changes in voltagelevel per timelength.
- Compactsystem: securitysystem in which the CCU and siren are in one housing.
- Detection: technical method for detecting a (attempted) burglary or other manipulations to the vehicle with the intention to break in or steal the vehicle.
- Detector: a system component designed for detection.
- Double immobilisation: an immobilisation of the startermotor and an additional interruption, not being the startermotor.
- Driving condition: condition in which the system is unset and the vehicle can be started and driven under normal operating conditions.
- Energysupply: electric power for the system supplied by the powersupply unit of the vehicle.
- Enginemanagementsystem: the electronic control of the engine, if interrupted in line with the attacktest, that equates a multiple interruption.
- Glassbreak detection: detector that responds to breaking glass.
- Immobilisation: electronic device that, possibly with mechanical components, is capable for interrupting the startermotor, fuelsupply or ignition (only with Otto engines) and will be activated automatically.
- Homologation requirements: all requirements as described in this Homologation Directive.
- Hoodswitch: switch that detects the opening of the hood.
- Immobilisation condition: condition in which the car is immobilised.
- Immobilizer: an electronic securitysystem for passengercars with a powersupply of max. 24 V DC, at least consisting of a CCU, an in- and unsetting system, switch (es), a cableharness as well as a statusdisplay of the systemcondition (only after market). In addition a users direction and (in case of after market) an installation manual.
- Inclinationdetection: a detector that monitors the angle of inclination of the vehicle.
- Interior: passengerscompartment of a vehicle, not including the separate luggagecompartment.
- Interiordetection: detection of the interior that responds if access is gained to the interior, in any manner whatsoever, or if any movement occurs within the interior.
- Key: device for operating a lock.
- Keypad: device installed in the vehicle, to unset the system by entering a digital code.
- Lock: key switch or electronic switch for setting or unsetting the system or system components.

- Multiple immobilisation: an immobilisation that will work on at least two essential electrical circuits.
- OE-system: system installed in the factory or under the responsibility of the carmanufacturer in his organisation (= not in the dealernetwork).
- Optical warning device: warningsignal by means of the direction indicators as provided on the vehicle.
- Perimeter protection: a protection activated by switches, as soon as one of the doors, the bonnet, luggage-compartment or fifth door is opened.
- Random code: a system whereby a, with help of an algorithm calculated, code for setting and unsetting, will not be used within a certain time.
- Relay: a device activated by a signal, makes or breaks a connection.
- Rollingcode: a system whereby a used code for setting and unsetting will not be used within a certain timelimit.
- Second way of unsetting: separate way to unset the system, independent of the remote control and not operated by batteries.
- Set: immobilisation-, wake- and alarmcondition.
- Setting: bringing the system into the set condition.
- Siren: an electronic audible warning device exclusively intended and suitable to be mounted outside the interior.
- Start interruption: possibility for the interruption of the electric circuit, or part of it in such a way that the engine cannot be operated via the steering-wheel ignition lock.
- Strand: a cableloom in one cover.
- Supplier: a company that supplies the approved product in Holland
- System: immobilizer or alarm system
- System code: a code given to the system by the manufacturer.
- System component: a complete operating component of the system that is connected to other system components by a cable harness.
- System condition: driving condition, immobilisationcondition, wakecondition and alarmcondition.
- Tamperalarm: alarmsignal activated, if in wakecondition the powersupply to the CCU or siren is interrupted.
- Tow-away detection: a detection that will respond to the movement of the wheels.
- Type identification: individual identification of a system component.
- Unset: driving condition
- Unsetting: bringing the system into the driving condition.
- Wakecondition: condition in which the system can be brought into the alarmcondition by tampering of detection by a detector. In this condition the immobilizer is active.
- Warning signal: audible and optical
- Z-system: alarmsystem without immobilizer (or only one immobilisation circuit) meant for installation in vehicles that already have an SCM-approved immobilizer.

4. TECHNICAL REQUIREMENTS

4.1 Categories of security systems

The (additional) requirements for the different categories of systems may vary depending of the application and the type of vehicle. For this the technical requirements are divided in 3 categories:

4.2 Original Equipments Systems (OE-systems)
4.3 After Market Systems (AM-systems)
4.4 ADR-Vehicles (transport of dangerous goods)

4.2 Original equipment systems

4.2.1 Classification

Class B1

comprising of an automatic setting system that prevents the movement of the vehicle, no detection and no alarm
- at least interruption of the fuel injection system or fuel supply +
- interruption of the startermotor circuit +
- attack resistance min. 5 minutes

Class B2

comprising of an automatic setting system that prevents the movement of the vehicle, alarm with back-up siren, perimeter and interiordetection, extended with cabin tilt detection or hooddetection (depending of the construction)
- immobilisation in line with class B1 with attack resistance 5 minutes +
- perimeter detection and interior detection +
- cabin tilt detection / hooddetection +
- optical warning +
- audible warning with back-up siren

Class B3

comprising of an automatic setting system that prevents the movement of the vehicle, alarm with back-up siren, perimeter and interiordetection, extended with cabin tilt detection or hooddetection (depending of the construction)
- immobilisation in line with class B1 with attack resistance 15 minutes +
- perimeter detection and interior detection +
- cabin tilt detection / hooddetection +
- optical warning +
- audible warning with back-up siren

Class B4 **B1 in combination with a tracking & tracing system**
Class B5 **B2 / B3 connected to a tracking & tracing system**

NB. Until July 1st, 2004 class B2 with be regarded as equal to class B3

4.2.2 Attackresistance

The security system shall resist tampering or manipulation in such a way that the vehicle can not be driven under its own power within five (5) minutes (class B1 and B2) or fifteen (15) minutes (class B3). To test this, an evaluation will be performed to the attack possibilities by the testhouse in line with appendix 4.

If the engine can be started before the immobilizer is activated, this shall not last longer then three (3) seconds for the first time and one (1) second for the next attempt(s).

Manipulation of, from the outside of the vehicle accessible, in- or outputs of the system shall not lead to more than one alarmcycle and not activate the battery backup siren.

The system shall not be rendered inoperative by short-circuiting of the audible and / or optical warning signals or any other accessory connected to the CCU.

It shall not be possible to unset the system or switch off the battery backup siren by overwiring or disconnecting one or more wires to the siren.

After and while interrupting the power-supply (+30) or mass-connection (-31) at least five (5) times when in the set or alarm condition during interruption times ranging from half a (0.5) second to at least twelve hours, the immobilizer shall remain active.

During wake- and alarmcondition it shall not be possible to remove the fuses, provided to protect the CCU and siren, from a system having a backup siren, without at least audible warning.

4.2.3 Technical specifications

During and after interruptions of 0,1 to 10 seconds of the +30 or -31 to the securitysystem in the unset condition (driving), only the status of the interruption of the startermotor is allowed to change.

The vehicle battery shall supply power of the system.

The use of primary batteries (non-rechargable) for the battery backup siren is allowed.

The energy consumption of the alarmpart of the system in set condition is limited to max. twenty (20) mA.

The CCU shall have at least two (2) separate, indepently operating circuits for detection groups.

At the end of the alarm cycle, the system shall automatically return to the set condition, while the reset time shall not exceed fifteen (15) seconds.

The alarmpart shall have no influence on the immobilizerpart

The alarmpart of the system shall be provided with an optical display indicating whether the alarmsystem is set or unset. This signal is of such a form or can be provided in such a manner that it is clearly visible from the outside of the vehicle.

4.2.4 Setting and unsetting procedures.

4.2.4.1 Setting

Setting the alarmsystem may proceed optionally via either a lock, switch, remote control or automatic with closing the last door / luggagecompartment.

Setting the immobilisation will be done automatically within sixty (60) seconds from switching off the engine or within the same period after opening the driver's door (with the engine switched off). In this case automatic setting will take place within ten (10) minutes after switching off the engine.

The alarmsystem shall be in the set condition within sixty (60) seconds after setting it, counting from the moment all actions have been performed to arm the system.

Setting and unsetting the alarm system may be made visible outside the vehicle for max. three (3) seconds.

If for setting and unsetting the immobilisation a device is used that is directly connected to the key (e.g. transponderkey), setting the immobilisation will take place immediately upon taking out the key or switching off the engine.

Other setting or unsetting procedures shall have the same securitylevel.

4.2.4.2 Unsetting (general)

Unsetting the immobilisation circuits is only allowed by the authorised way of unsetting the securitysystem.

If, after unsetting, within two (2) minutes no action from the driver on the startercircuit has followed, the immobilizer circuits will come in directly and automatically. This is not applicable for systems using a keyconnected mechanism (e.g. transponderkey).

If the detection of the interior and/or the cabin tilt detection can be switched off separately by the user, this will only be admitted during the unset condition or within sixty (60) seconds after setting the system.

If the alarmsystem can be partially unset in this period by opening a door or luggagecompartment (in an unauthorised way), this part of the system shall be reactivated at closing this door or the luggagecompartment.

If the detection of the interior and/or the cabin tilt detection can be switched off separately by the user, the whole system shall be automatically and fully reactivated when being subsequently set.

4.2.4.3 Remote control

The remote-control device shall have a coded transmitter signal featuring at least one hundred thousand (100,000) different codes.

It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

After each transmission of a signal by the remote control, the code used for unsetting will change. For this a random keycode will be chosen of at least sixty-four (64) bit.
Transponderkeys are regarded as remote controls and will have to satisfy the same (legal) requirements.

Removal of the transponder from the key shall lead to permanent visible damage.

4.2.4.4 Keypad

The number of combinations on the keypad must be at least 10.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

Short-circuiting or other manipulations with (the wires to and from) the keypad, shall not unset the immobilizer.

If the system is supplied with a standard code upon delivering that can be changed by the customer, this first code shall only last ten (10) times.

4.2.4.5 Electronic code keys

The number of combinations on the coded keys must be at least 50.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

Short-circuiting or other manipulations with (the wires to and from) the keyreceptor, shall not unset the immobilisation.

4.2.4.6 Second unsetting method.

Unsetting procedures aimed at unsetting the system in an alternative way will have to satisfy the same standards for security as the standard unsetting procedures.

4.2.5 Immobilisation.

Dependent of the classification, one or two separate working immobilizer circuits are required.

The immobilisation shall be in operation during the set and alarm condition, and shall be automatically set.

If the wiring to the siren should be disconnected in the set or alarm condition, the immobilisation shall continue to operate.

The system components that effect the immobilisation shall not change their status if there should occur any variations in the rated battery voltage of +/- 25%.

Activating and deactivating the immobilisation shall continue to be possible at battery voltages ranging from 11 to 15 Volts (at 12 V rated systems), resp. 22 to 30 Volts (at 24 V rated systems).

4.2.6 Detection

Activation of the audible and optical warning devices shall be realised by perimeter detection and interior detection via separate, independently operating detection groups of the CCU.

Additional detection by means of inclination detection, tow-away detection, ignition detection and glassbreak detection is permitted.

Voltage-drop detection, shock and vibration detection on behalf of perimeterdetection is not permitted. If the CCU should separately include such features, they shall be provided in a switched-off condition and it shall not be permitted to provide the possibility to activate them from the outside of the CCU.

4.2.6.1 Perimeter detection

Perimeter detection takes place via (existing) switching contacts of doors, luggage-compartment and bonnet. If there are no original switches, approved switches shall be delivered.

Any detection of the perimeter detection in the set condition shall lead to an alarm condition.

4.2.6.2 Interior detection

Interior detection shall be done by using sensors to be mounted in the interior.

Any detection of the interior detection control during the set condition shall lead to an alarm condition (see 4.2.7.1).

The use of adjustable sensors shall only be permitted if adjusting them cannot be effected easily and only by using tools.

4.2.6.3 Cabin tilt detection

Any detection by the cabin tilt sensor(s) during the set condition shall lead to an alarm condition (see 4.2.7.1).

Cabin tilt detection takes place by means of sensors that respond to any change in the angle of inclination of the vehicle with respect to the parked position. This goes for the lengthways as well as across.

The change in the angle of inclination at which detection is to occur amounts is minimum two (2) and maximum four (4) % = 4 cm. deviation per metre (= 1,1 – 2,3 °).

The position of the vehicle shall not affect the cabin tilt detection.

Slow changes in the position of the vehicle (< 0,2 % per sec.) shall not affect the inclination detection.

The activation of the cabin tilt detection may be delayed in view of mechanical changes in the inclination of the vehicle. Such delayed activation shall not exceed ninety (90) seconds.

4.2.6.4 Tow-away detection

Any detection by the tow-away module during the set condition shall lead to an alarm condition (see 4.2.7.1).

Tow-away detection will take place by sensors that will react upon a displacement of at least one (1) and max. two (2) rotations of the wheel.

4.2.6.5 Glassbreak detection

Any detection of the glassbreak sensor during the set condition shall lead to an alarm condition (see 4.2.7.1).

Glassbreak sensors shall cause no unnecessary alarm.

4.2.7 Signalling

4.2.7.1 General.

The alarm condition shall be activated immediately during the wake condition as soon as a detector detects an interference. This applies at no more than sixty (60) seconds after setting the system.

In the alarm condition, both audible and optical warning devices will be activated immediately.

Except for the perimeter detection, the audible warning shall not sound more than ten (10) times within one and the same setting period.

Unsetting the system by the authorised user switch off the warning devices immediately.

4.2.7.2 Audible warning

Only an electronic siren shall effectuate the audible warning.

The siren shall satisfy the requirements of the EU 95/56 with a minimum sound level of 105 dB(A) while the sound level will be measured after the corrosion and endurance test.

Installed in the vehicle the sound level will be at least eighty-five (85) % of the result of the EU-test, taken from the side of the vehicle where the siren is mounted.

It shall not be possible in the set condition to deactivate the battery backup siren without activating the tampera-larm.

The audible warning device shall become active immediately in the alarm condition for at least twenty-five (25) seconds and no more than thirty (30) seconds.

For all systems a coded link is an obligation for the connection between the siren and the CCU.

If the status of one and the same input of the CCU does not change, the audible warning shall be limited to one (1) cycle.

The capacity of the battery backup siren shall be sufficient for uninterrupted audible warning for at least five

(5) minutes during which the loss of sound level will be max. two (2) percent.

4.2.7.3 Optical warning

The optical warning shall be activated immediately in the alarm condition for no more than five (5) minutes.

The minimum duration of optical warning will be determined by the duration of the audible warning cycle(s) (25 - 30 sec. per warning cycle).

For optical warning, the direction indicators of the vehicle shall be used only.

4.2.7.4 Radio alarm

The audible and / or optical warning can be combined with a silent alarm by means of radio transmission.

This radio transmission will have to comply with the legal requirements.

4.3 After market systems

4.3.1 Classification

Class B1

comprising of an automatic setting system that prevents the movement of the vehicle, no detection and no alarm

- at least interruption of the fuel injection system or fuel supply +
- interruption of the startermotor circuit +
- attack resistance min. 5 minutes

Class B2

comprising of an automatic setting system that prevents the movement of the vehicle, alarm with back-up siren, perimeter and interiordetection, extended with cabin tilt detection or hooddetection (depending of the construction)

- immobilisation in line with class B1 with attack resistance 5 minutes +
- perimeter detection and interior detection +
- cabin tilt detection / hooddetection +
- optical warning +
- audible warning with back-up siren

Class B3

comprising of an automatic setting system that prevents the movement of the vehicle, alarm with back-up siren, perimeter and interiordetection, extended with cabin tilt detection or hooddetection (depending of the construction)

- immobilisation in line with class B1 with attack resistance 15 minutes +
- perimeter detection and interior detection +
- cabin tilt detection / hooddetection +
- optical warning +
- audible warning with back-up siren

Class B4 B1 in combination with a tracking & tracing system

Class B5 B2 / B3 connected to a tracking & tracing system

NB. Until July 1st, 2004 class B2 with be regarded as equal to class B3

4.3.2 Attackresistance

The security system shall resist tampering or manipulation in such a way that the vehicle can not be driven under its own power within five (5) minutes (class B1 and B2) or fifteen (15) minutes (class B3). To test this, an evaluation will be performed to the attack possibilities by the testhouse in line with appendix 4.

The immobilizerpart of the system shall have at least one of the following specifications:

- **permanently** filled with resin or other material
- in a metal casing and closed by a minimum of 4 one tour screws or a similar, attack resistant construction
- combined with an immobilizercircuit, not on the startermotor, to be fitted separately from the CCU and activated by a coded link.

The CCU shall have at least two screw apertures.

Wiring to the immobilizer part of the system (-31, +15, +30 and immobilizer wires) shall be in one strand and be of one and the same colour and diameter with removable colour- or numbercodes.

Manipulation of, from the outside of the vehicle, accessible in- or outputs of the system shall not lead to more than one alarmcycle and not activate the battery backup siren.

The system shall not be rendered inoperative by short-circuiting of the audible and / or optical warning signals or any other accessory connected to the CCU.

It shall not be possible to unset the system or switch off the battery backup siren by overwiring or disconnecting one or more wires to the siren.

After and while interrupting the power-supply (+30) or mass-connection (-31) at least five (5) times when in the set or alarm condition during interruption times ranging from half a (0.5) second to at least twelve hours, the system shall not change status.

During wake- and alarmcondition it shall not be possible to remove the fuses, provided to protect the CCU and siren, from a system having a backup siren, without at least audible warning.

4.3.3 Technical specifications

4.3.3.1 General

During and after interruptions of 0,1 to 10 seconds of the +30 or -31 to the securitysystem in the unset condition (driving), only the status of the interruption of the startermotor is allowed to change.

The vehicle battery shall supply power of the system.

The use of primary batteries (non-rechargable) for the battery backup siren is allowed.

The energy consumption of the system in set condition is limited to max. twenty (20) mA.

The CCU shall have at least two (2) separate, indepently-operating circuits for detection groups.

At the end of the alarm cycle, the system shall automatically return to the set condition, while the reset time shall not exceed fifteen (15) seconds.

The alarmpart of the system shall have no influence on the immobilizerpart.

The system shall be provided with an optical display indicating whether the system is set or unset. This signal is of such a form or can be provided in such a manner that it is clearly visible from the outside of the vehicle.

4.3.3.2 Coded link (wiring)

The number of different levels will be min. ten (10) per second.

The number of code combinations shall be at least 10.000

During set condition (re) programming or replacing of (parts of) the system shall not lead to a change of status of the system.

4.3.4 Setting and unsetting procedures.

4.3.4.1 Setting

Setting the alarmsystem may proceed optionally via a lock, switch, remote control or automatic with closing the last door / luggagecompartment.

Setting the immobilisation will be done automatically within sixty (60) seconds from switching off the engine or within the same period after opening the driver's door (with the engine switched off). In this case automatic setting (for security) will take place within ten (10) minutes after switching off the engine.

The alarmsystem shall be in the set condition within sixty (60) seconds after setting it, counting from the moment all actions have been performed to arm the system.

Setting and unsetting the alarm system may be made visible outside the vehicle for max. three (3) seconds.

If for setting and unsetting the immobilisation a device is used that is directly connected to the key (e.g. transponderkey), setting the immobilisation will take place immediately upon taking out the key or switching off the engine.

Other setting or unsetting procedures shall have the same securitylevel.

4.3.4.2 Unsetting (general)

Unsetting the security system is only allowed in the authorised way.

If, after unsetting, within two (2) minutes no action on the startercircuit has followed, the immobilisation will directly and automatically be activated. This is not applicable for systems using a keyconnected mechanism (e.g. transponderkey).

If the detection of the interior and/or the inclination detection can be switched off separately by the user, this will only be admitted during the unset condition or within sixty (60) seconds after setting the system.

If the alarmsystem can be partially unset (in an unauthorised way) in this period by opening a door or luggage-compartment, this part of the system shall be reactivated at closing this door or the luggagecompartment.
If the detection of the interior and/or the inclination detection can be switched off separately by the user, the

whole system shall be automatically and fully reactivated when being subsequently set.

4.3.4.3 Mechanical locks (**only in the interior)**

Only locks to be fitted in the interior of the vehicle are allowed to be used for unsetting the system and will have to be approved according to this Directive, including the attacktest.

The cylinder part of the lock and the switching mechanism shall be assembled so as to form one solid system component.

A lock shall not be operable by a key that differs only one (1) permutation from the key matching the lock.

Cylinders shall be provided with a cylinder drill obstruction.

The key profile shall have at least thirty thousand (30,000) permutations.

The permutation interval is at least half a (0.5) mm.

A lock shall be provided with at least six (6) pins or blocking plates.

The cylinder of the lock shall not protrude by more than one (1) mm from the cowling. The protruding part shall be conical so as to ensure that tools cannot get any hold on it.

The joint between the cylinder core and the cylinder casing shall be able to withstand a tensile force of seven (7) kN.

The switching mechanism shall have at least ten thousand (10.000) protection codes or code combinations.

4.3.4.4 Remote control

The remote-control device shall have a coded transmitter signal featuring at least one hundred thousand (100,000) different codes.

It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

After each transmission of a signal by the remote control, the code used for unsetting will change. For this a random keycode will be chosen of at least sixty-four (64) bit.

Transponderkeys are regarded as remote controls and will have to satisfy the same (legal) requirements. Removal of the transponder from the key shall lead to permanent visible damage.

4.3.4.5 Keypad

The number of combinations on the keypad must be at least 10.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

Short-circuiting or other manipulations with (the wires to and from) the keypad, shall not unset the

immobilisation.

If the system is supplied with a standard code upon delivering and to be changed by the customer, this first code shall only last ten (10) times.

4.3.4.6 Electronic code keys

The number of combinations on the coded keys must be at least 50.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth (0.1) %, the correct code that can unset the system.

Short-circuiting or other manipulations with (the wires to and from) the keyreceptor, shall not unset the immobilisation.

4.3.4.7 Second unsetting method.

Unsetting procedures aimed at unsetting the system in an alternative way will have to satisfy the same standards for security as the standard unsetting procedures.

4.3.5 Immobilisation.

4.3.5.1 General

A minimum of two (2), independent working, immobilisation circuits are required.

The immobilisation shall be in operation during the set and alarm condition, and shall be automatically set.

If the wiring to the siren should be disconnected in the set or alarm condition, the immobilisation shall continue to operate.

The system components that effect the immobilisation shall not change their status if there should be any variations in the rated battery voltage of +/- 25%.

Activating and deactivating the immobilisation shall continue to be possible at battery voltages ranging from 11 to 15 Volts (at 12 V rated systems), resp. 22 to 30 Volts (at 24 V rated systems).

4.3.5.2 Startermotorinterruption

The CCS shall have at least one immobilizercircuit, suitable for a power load of at least ten (10) Amp. during at least three (3) seconds (this maximum powerload is not applicable for immobilization systems working on the engine management systems, to be judged by the SCM).

4.3.6 Detection

Activation of the audible and optical warning devices shall be realised by perimeter detection and interior detection via separate, independently operating detection groups of the CCU.

Additional detection by means of inclination detection, tow-away detection, ignition detection and glassbreak detection is permitted.

Voltage-drop detection, shock and vibration detection on behalf of perimeterdetection shall not be permitted. If the CCU should separately include such features, they shall be provided in a switched-off condition and it shall not be permitted to provide the possibility to activate them from the outside of the CCU.

4.3.6.1 Perimeter detection

Perimeter detection takes place via (existing) switching contacts of doors, luggage-compartment and bonnet. If there are no original switches, approved switches shall be supplied.

With respect to the perimeter detection, a hoodswitch shall be supplied and tested with the system.

Any detection of the perimeter detection in the set condition shall lead to an alarm condition.

4.3.6.2 Interior detection

Interior detection shall be done by using sensors to be mounted in the interior.

Any detection of the interior detection during the set condition shall lead to a alarm condition (see 4.3.7.1).

The use of adjustable sensors shall only be permitted if adjusting them cannot be effected easily and only by using tools.

4.3.6.3 Cabin tilt detection

Any detection by the cabin tilt sensor(s) during the set condition shall lead to an alarm condition (see 4.3.7.1).

Cabin tilt detection takes place by means of sensors that respond to any change in the angle of inclination of the vehicle with respect to the parked position. This goes for the lengthways as well as across.

The change in the angle of inclination at which detection is to occur amounts is minimum two (2) and maximum four (4) % = 4 cm. deviation per metre (= 1,1 – 2,3 °).

The position of the vehicle shall not affect the inclination detection.

Slow changes in the position of the vehicle (< 0,2 % per sec.) shall not affect the inclination detection.

The activation of the cabin tilt detection may be delayed in view of mechanical changes in the inclination of the vehicle. Such delayed activation shall not exceed ninety (90) seconds.

4.3.6.4 Tow-away detection

Any detection by the tow-away module during the set condition shall lead to an alarm condition (see 4.3.7.1).

Tow-away detection will take place by sensors that will react upon a displacement of at least one (1) and max. two (2) rotations of the wheel.

4.3.6.5 Glassbreak detection

Any detection of the glassbreak sensor during the set condition shall lead to an alarm condition (see 4.3.7.1).

Glassbreak sensors shall cause no unnecessary alarm.

4.3.7 Signalling

4.3.7.1 General.

The alarm condition shall be immediately activated during the wake condition as soon as a detector detects an occurrence. This applies at no more than sixty (60) seconds after setting the system.

In the alarm condition, both audible and optical warning devices will be immediately activated.

Except for the perimeter detection, the audible warning shall not sound more than ten (10) times within one and the same setting period.

Unsetting the system by the authorised user switch off the warning devices immediately.

4.3.7.2 Audible warning

Only an electronic siren shall effectuate the audible warning.

The siren shall satisfy the requirements of the EU 95/56 with the restriction that the sound level will be tested after the corrosion and endurance test.

The audible warning device shall become active immediately in the alarm condition for at least twenty-five (25) seconds and no more than thirty (30) seconds.

In the set condition disconnecting one or more wires to the battery backup siren will automatically lead to a tampersignal

A coded link is mandatory for the connection between the siren and the CCU.

If the status of one and the same input of the CCU does not change, the audible warning shall be limited to one (1) cycle.

The capacity of the battery backup siren shall be sufficient for uninterrupted audible warning for at least five (5) minutes during which the loss of sound level will be less than fifteen (15) percent.

4.3.7.3 Optical warning

The optical warning shall be activated immediately in the alarm condition for no more than five (5) minutes.

The minimum duration of optical warning will be determined by the duration of the audible warning cycle(s) (25 - 30 sec. per warning cycle).

For optical warning, the direction indicators of the vehicle shall be used only.

4.3.7.4 Radio alarm

The audible and / or optical warning can be combined with a silent alarm by means of radio transmission.

This radio transmission will have to comply with the legal requirements.

4.3.8 Cable works

The system shall be provided with a cable harness with wiring and terminals. For the security part of this cabling the following is applicable:

- a minimum length of two (2) meters
- in case of vehicle specific cabling deviation is possible
- wires for the various functions are provided in one (1) colour and diameter with colour or number codes that will be removable.
- a core diameter of a minimum cross-section of one (1.0) mm^2 or so much more as required according to the application.

4.4 ADR-Vehicles (transport of dangerous goods)

It is known that the transport of dangerous goods under the ADR laws, might get in conflict with the efectivness of the security system. In several talks with the Ministry of Traffic and the Department of Road Traffic (RDW) SCM has received a solution for this.

The solution excist of the following specifications voor VLG (ADR)-vehicles and is accepted by the RDW.

1. The securitysystem shall be connected to a VLG-currentlimitor (this limits the currentconsumption and is independent of the VLG-mainswitch).
2. The optical warning signal shall only be conected via the VLG-mainswitch.
3. The acoustic warning signals shall only be transmitted by the battery backup siren.

ad. 1 The max. currentconsumption of the currentlimitor is set at 1 Amp. at 30 V.

5. ADMINISTRATIVE PROCEDURES

5.1 General

5.1.1. Testing

Type approval testing can be performed according to this Directive with annexes by a testhouse of the approval holder.

5.1.2 Choice of testhouse

A list of testhouses is available at the SCM with which the SCM has signed an agreement to accept results from this testhouse.

5.1.3 Application of this Directive

If any systems or system components or the operation thereof should not or not directly fall within the scope of this Directive or in case of coincidence with other SCM Directives, they will be evaluated separately by the Technical Committee of the SCM (eventually in consulting the supplier or the testhouse). The College of Experts of the SCM will publish adjustments and interpretations of this Directive within 30 days after acceptance in numbered Annexes.

5.1.4 Publication / Listing

SCM ensures the publication of the systems, which meet the requirements of this Directive, after the reception of the signed Approval Agreement. SCM will publish the approved systems in the list of approved systems, hereinafter referred to as: 'the List'. The list will be published via www.scm.nl. New products will be listed within 5 working days after the reception of the final testreport from the test house.

5.1.5 Disputes

In case of differences or obscurities in the English version, the original Dutch version will be leading.
In case of legal disputes, Dutch Law will be applicable.

5.2 Type approval

5.2.1 Application for type approval

For the type approval the applicant shall apply directly to a testhouse as published by the SCM.

5.2.2 The applicant

For each securitysystem only one (1) applicant can be registered. As soon as a type approval has been granted (see 5.2.5), the applicant will be named the approval holder.

If the applicant is not the manufacturer of the system, both the applicant and the manufacturer (by way of authorisation) shall sign the application.

If the application relates to a system of a manufacturer not established in the European Union, the manufacturer shall authorise a legal entity established in the European Union to file the application on its behalf.

5.2.3 Type approval

For the type homologation, three complete security systems shall be submitted to the testhouse. One system shall be stored as reference sample.

At least the following information shall be supplied to the testhouse:

- Commercial documentation of the product including all programming modes. This is to decide whether there are options, not allowed under this Directive and to be activated by the user.
- User manual and installation manual (might be in draft)
- Complete technical documentation of the supplied system
  For OE-systems other arrangements can be made with the testhouse.

5.2.4 The testreport

In case of a positive result, the applicant can submit the report to the SCM. This report will mention at least the following items:
The version of the Directive used and the number of the annex (es)
Systemdescription
Applications of the system
Name of the applicant
Name of the approvalholder
Name of the responsible testengineer
Final user manual and installation manual
Result of the test
Appendices with testresults
Photograph of the system in colour

5.2.5 The approval agreement

After receiving and checking the testreport, SCM will send a **Certificate of approval.**
Before the approved product will be placed on the List, the approval holder and supplier will sign an approval agreement with the SCM.
In the approval agreement all rights and duties of the SCM and the approval holder and the supplier are mentioned.

5.2.6 Rights and duties of the approval holder / supplier.

Within the limits of this Directive the approval holder has the following rights and duties:

- is entitled to use the name “SCM-goedgekeurd”
- is entitled to be included on the list of approved systems and suppliers as published by the SCM
- shall be obliged to provide the approval label on each approved product supplied on the Dutch market.

In case of OE-systems, it is possible to derive from this after consulting the SCM.
- is obliged to ensure that all technical modifications that might effect the typeapproval, before introduction be reported in writing to the SCM and the testhouse (where the typeapproval has been performed).
- shall adhere to the requirements with respect to retesting of the approved systems.

5.2.7 Certification agreement.

Before ordering approvallabels, the approval holder and the supplier shall sign an approval agreement with the SCM. In this agreement the rights and duties of the supplier and the SCM are registered.

5.2.8 Rights and duties of the supplier / approval holder.

- is entitled to use the name "SCM-goedgekeurd".
- shall ensure that all systems for the Dutch market shall be equipped with the approvallabel. In case of OE-systems, it is possible to derive from this after consulting the SCM.

The following requirements are applicable for the conduct of business of the supplier who distributes the approved product in the Netherlands.

5.2.8.1 Guarantee, repair and service.

- All products supplied shall, within the guarantee period of minimum 1 year, calculated from the day of purchase, be repaired or replaced at no cost by the same or a similar product. Repair or replacement should be carried out within 10 workdays.

- All supplied products should, within 5 years after the date of purchase, be able to be repaired or replaced. Repair or replacement should be carried out within 10 workdays.

- If the supplier decides to stop delivering, this service should still remain for 5 years. If another supplier will distribute an approved product, for whatever reason, this new supplier shall take over all existing service obligations for all products in the market and together with the manufacturer sign a new certification agreement.
-

5.2.8.2 Education and dealersupport.

Helpdesk support for suppliers and customers during office hours by means of direct personal contact. Direct availability is mandatory.

The supplier takes care of a thorough, product technical training for her installers. A specimen of the training documentation is submitted to the SCM

Technical schemes shall be send to or be available within 1 hour for installers, registered at the suppliers.

Publicity of the schemes through e.g. Internet is not permitted.

5.2.8.3 Workshop.

The supplier shall have at his disposal a workshop with ambient lighting where research or trouble shooting at a car will be possible.

The area where technical information of systems and installation will be stored, shall be protected with an electronic securitysystem and connected to a registered and certified control centre (PAC).

5.2.8.4 Other obligations.
Each supplier shall prove to the SCM the existence of a company liability insurance with a cover of at least 2,5 million Euro per event.

This company activity (car security) shall fit within the company objectives as registered in the abstract of the Chamber of Commerce. This abstract shall be submitted to the SCM for approval.

5.2.8.5 Non fulfilment
In case of non fulfilment of one or more of the above mentioned obligations, the following sanctions are possible:

Withdrawal of the type approval
Mandatory recall of the denounced products from the market.
Removal of the product of the List of approved products.

5.3 Using the name of SCM

The approval holder and the supplier will be permitted to use the wording "SCM approved" for the approved systems. In the event said approval should be withdrawn or the provisions of the Homologation Directive should not be complied with, the approval holder and the supplier shall no longer be permitted to use the name of SCM.

Before doing so, the approval holder and the supplier shall be obliged to submit to SCM for review purposes the proofs of all publications in which the use of the name of SCM as hereinbefore described is to occur. If the publication is not in compliance with the conditions, SCM shall provide a written refusal.

Using the figurative mark of SCM shall not be permitted but on the approval label unless otherwise agreed by approval holder or the supplier and SCM.

5.4 Approval Labels

5.4.1 General

By signing the certification agreement, the principal shall undertake to provide all mass-produced systems of the approved type, destined for the Dutch market, with a properly attached approval label to be provided by SCM, taking into account the pertinent provisions of the Directive.

The aforesaid approval label shall contain the following information:
- a text as determined by SCM
- rising serial number

5.4.2 Issue of approval labels

The first series of approval labels can be issued as soon as the signed certification agreement has been received by the SCM. Series will usually consist of 500 labels. If, however, the monthly production of the applicant (manufacturer) should exceed 1,000 pieces, more approval labels can be issued up to a maximum of 5,000.
For new approval holders, the maximum order is 250 labels for the first delivery. If, at ordering a second labelbatch, less than 60 % of the labelled systems has not been installed, the order might be refused.

5.4.3 Ordering approval labels

The approval labels can be ordered from SCM using an approval-label order form. The time of delivery will be max. 1 week.

5.4.4 Prices of approval labels

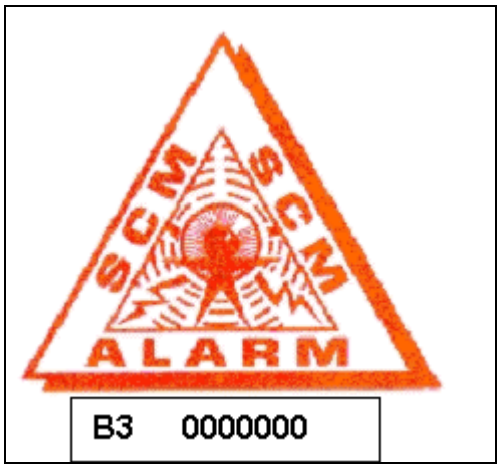
The price of the approval label is stated on the approval-label order form and might be adjusted yearly.

5.4.5 Model of approval label

The approval label is a self-adhesive orange sticker with a black imprint which can attached to a hard base.

Dimensions: Width 40 mm.
Length at least 40 mm (depending on the amount of details)

5.4.6 Example of approval label



5.5 Modification of systems

Any modification, either to the production method or the system itself, shall be notified to SCM and the testhouse in writing before actual implementation. This is also applicable for changes in the user manual and the installation manual.

Such modification shall be reported by submitting:

- A brief description of the modification concerned and/or, at the discretion of the testhouse, followed by submitting the system or part as modified.
- Drawings of the parts as modified:
  * Original drawings of the part on which the modification concerned has been clearly indicated.
  * If new parts are to be used; drawings of the new part, together with an assembly drawing on which any parts to be deleted or added have been clearly indicated.
  * On the drawings, all modifications shall be properly numbered and dated.

Upon evaluating the modification on the basis of the information supplied, the testhouse shall inform the approval holder whether the modification concerned can be implemented in the production process by an administrative test without performing additional testing (a report to the approval holder and SCM then being issued only); or whether a completely new or partial test shall be performed for the account of the approval holder.

5.6 Product control of approved systems

5.6.1 Product control - General

In accordance with the Directive, after homologation, approved systems in the production phase will be controlled by means of so-called product control. Product control comprises of two parts, i.e.: periodic production control and random tests. This product control will be carried out by the testhouse that performed the original type approval.
SCM will inform the approval holder and the testhouse of the necessity for production control based on the number of installed systems. The testhouse will inform SCM about the outcome of the production control.

5.6.2 Production Control

For the purpose of the production control, the approval holder will be requested to submit to the testhouse one (1) security system per 2,500 security systems provided with a SCM-approval label having the same approval number, with a maximum of one (1) such system per calendar quarter and a minimum of one (1) such system per calendar year. For the first batch of a new approval number this production control will take place in the first 250 supplied systems. During the production control, an investigation will be made to determine whether the system still meets the requirements and/or the system still conforms to the security system as supplied for type approval.
After consulting SCM and the testhouse is will be permitted to make different arrangements.

5.6.3 Submission of samples.

Within 6 weeks after the request of SCM, the approval holder shall submit the products to the testhouse for production control.

5.6.4 Random tests

In addition to the regular production control, SCM reserves the right to perform tests on approved systems obtained on the market, if circumstances so should warrant. The costs of these tests are on behalf of SCM.

5.6.5 Rates of production control

The rates of the product control are charged by the testhouse without intervention of the SCM.

5.6.6 Procedures in the event of deviations/defects of the systems

5.6.6.1 If the system has been modified without notification
If, due to unreported modifications, it should turn out that any one of the systems does not correspond with the type as approved, SCM shall have the right to deny the approval holder the continues use of the name of SCM; the type approval of the type concerned can then be withdrawn.

5.6.6.2 If the system has not passed the test successfully
If any one of the systems should not pass with positive results the tests to which it was subjected, SCM shall have the right to temporarily deny the approval holder the use of the name of SCM (blocking); the issue of approval labels shall cease immediately.

If the approval has been blocked, the approval holder shall:
- immediately institute an investigation to determine whether any deviations in the production process or in the materials used occur, and shall repair them immediately if so required. A written report on the investigation conducted and the conclusions thereof as well as on the measures taken shall be sent to the testhouse.
- have the tests, which were not concluded with positive results, repeated by the testhouse, for the account of the approval holder, on three other systems from the same production series (production control).

If all three systems pass the production control successfully, the temporary suspension, if any, of the use of the name of SCM shall be revoked (un-blocking), and the issue of approval labels shall be resumed.

If one or several of these three systems should fail to pass said repeat inspection successfully, SCM shall have the right to deny the approval holder the continued use of the name of SCM; the type approval of the system concerned will then be withdrawn.

5.7 Withdrawal of the type approval

If the approval holder should not adhere to the provisions as laid down in this Directive, the type approval can be withdrawn with immediate effect, if necessary after consultation between the testhouse and SCM. Such withdrawal shall apply to all systems falling under the same type approval number.
Withdrawal of an approval implies that all duties and rights of the approval holder as defined in subsection 5.2 and 5.3 of this Directive shall be cancelled with immediate effect.

6. TESTS

6.1 General

6.1.1 The sequence of the tests to be performed shall be determined by the testhouse.

6.1.2 The system components shall be tested in the form as installed and delivered.

6.1.3 The positioning of the system components during the tests to be performed shall be determined by the testhouse in accordance with the installation instruction if possible. If the manufacturer should have any special wishes, evidence shall be provided that, when installing, the position, in which the tests were performed, will be adhered to.

6.1.4 System components shall be tested according to the testmatrix.

6.1.5 During each test, all system components shall function normally and shall not cause any unnecessary alarms, while the system shall not change its status other than in the usual way or in the way as intended.

6.1.6 After completion of each test, the system components shall function according to the manufacturer's specifications and shall not have suffered any deformations and/or changes which may adversely affect the proper functioning of the system components at that moment or after the lapse of some time.

6.2 Testmatrix

Part	Testmodule																
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11a	T11b	T12	T13	T14	T15	T16
Complete system	X	X	X	X		X	X	X	X					X		X	
Hoodswitch										X							
Remote		X							X								
Siren	X	X	X	X	X	X	X	X	X	X	X	X					
Cabin tilt	X	X	X	X		X	X	X									
Interruption startermotor																	X
Engine parts	X	X	X	X	X	X	X	X	X	X							

T1	Vibration and shock Components on the engine	Conform EU 95/56, par. 5.2.8.2.1 Conform EU 95/56, par. 5.2.8.2.2
T2	Low temperature	Conform EU 95/56, par. 5.2.2.1
T3	High temperature	Conform EU 95/56, par. 5.2.2.2
T4	High temperature with condensation	Conform EU 95/56, par. 5.1.3
T5	High temperature (components under the hood)	Conform EU 95/56, par. 5.2.2.3
T6	Voltagedrop	Conform EU 95/56, par. 5.2.14
T7	Powersupply	Conform ISO 7637-2
T8	HF-radiation (EMC)	Conform EU 95/54 with higher level: see 6.3
T9	Endurance	see 6.4
T10	Corrosion	see 6.4
T11	Sound level	Conform EU 95/56, after corrosion and endurance. Min. 105 db(A), 85 % for mounted systems. Conform EU 95/56, annex 4.3.1
T12	Droptest remote	see 6.4
T13	Interior detection	Conform EU 95/56, par. 5.2.11, 5.2.13 en 5.2.15
T14	Cabin tilt detection	To the test house
T15	Attack test	See 6.5
T16	Interruption starter motor	To the test house

6.3 EMC testprocedure

Method of measurement of the susceptibility of security systems passengercars to electromagnetic radiation

General
The system shall comply with the following test methods:

1. Bulk current injection testing in the frequency range 20 Mhz - 200 MHz
2. Radiated electromagnetic field testing in the frequency range 200 MHz - 2000 MHz

State of system under test
The system shall be tested both in activated condition and rest condition, being a simulation of both normal operating conditions.

Connection of the wiring
The system under test shall be arranged and connected according to its requirements and no additional grounding connections are allowed. The test wiring should simulate, as closely as possible, the real vehicle wiring. All wires should be terminated as realistic as possible.
A special cable for testing purposes (without extra shielding) will be connected between the system and its terminations. This special cable will have a length of about 1,1 meter and will be connected directly to the system.

Test signal characteristics
Tests shall be performed using a continues wave signal, modulated with a 1 kHz sinus wave at 80% modulation depth.

1. Bulk current injection testing
The bulk current injection tests are carried out in accordance with the standards ISO 11452-1 (1995) and ISO 11452-4 (1995). For the bulk current injection tests, the following test specifications comply:

Test method	• Substitution method (calibrated injection probe method)
Test level	• 100 mA (In a 50 Ohm system)
Frequency band	• 20 MHz to 200 MHz
Frequency step size	• 1% of the previous frequency
Frequency mode	• Ramp method (-2 dB)
Dwell time	• Minimal 2 seconds
Modulation type	• 80% AM, 1 kHz sine-wave
Peak conservation	• yes, peak power conservation
Calibration mode	• Forward power
Supply voltage	• 12 VDC or 24 VDC
Ambient temperature	• 23 (+/-5) Degrees Celsius

2. Radiated electromagnetic field testing

The radiated electromagnetic field tests are carried out in accordance with the standards ISO 11452-1 (1995) and ISO 11452-2 (1995). For the radiated electromagnetic field test, the following test specifications comply:

Test method	• Substitution method
Test level	• 50 V/m
Frequency band	• 200 MHz to 2000 MHz
Frequency step size	• 1% of the previous frequency
Frequency mode	• Ramp method (-2 dB)
Dwell time	• Minimal 2 seconds
Modulation type	• 80% AM, 1 kHz sine-wave
Peak conservation	• yes, peak power conservation
Height of EUT above ground	• 0,8 meters
Antenna distance to EUT	• Minimum 1 meter
Calibration mode	• Forward power
Supply voltage	• 12 VDC or 24 VDC
Ambient temperature	• 23 (+/-5) Degrees Celsius

6.4 Specific tests

ENDURANCE TEST

Test method per cycle:	20 times setting and unsetting
Duration per cycle:	15 minutes
Number of cycles:	250
Warning condition:	unset, set and alarm conditions
Test conditions:	per cycle 1 alarm given

CORROSION TEST

Test method per cycle:	in a climate-controlled testing room
System components:	to be used for installation outside the interior
Duration per cycle:	144 hours
Number of cycles:	1
Test conditions:	DIN 50021 SS

DROPSHOCK TEST ON HAND-HELD TRANSMITTER

Test method per cycle:	free fall on concrete surface
Duration per cycle:	15 sec.
Number of cycles:	50
Test conditions:	drop height 1 metre

COMITÉ EUROPÉEN DES ASSURANCES

SECRETARIAT GENERAL
3bis, rue de la Chaussée d'Antin F 75009 Paris
Tél. : +33 1 44 83 11 83 Fax : +33 1 44 83 11 85
Web : cea.assur.org

DELEGATION A BRUXELLES
Square de Meeûs, 29 B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

CEA Recommended Practice for

ELECTRONIC SECURITY SYSTEMS

CEA01

Comité Européen des Assurances
3bis, rue de la Chaussée d'Antin
F 75009 PARIS (France)

1. DESCRIPTIONS

1.1 Definitions

- Attack time: the time in which a lock / security system withstands an attack test in such a manner that the system is not unset.
- Attack test: validation of the security level afforded by a security system by attempting to unset or bypass the immobilizer.
- CCU: central control unit of the security system.
- Coded link: a signal (only for cable connections) with a minimum number of changes in voltage level per time length.
- Control equipment: equipment necessary for the setting and/or unsetting of an immobilizer.
- Energy supply: electric power for the system supplied by the power supply unit of the vehicle.
- Engine management system: the electronic control of the engine.
- Immobilisation condition: condition in which the car is immobilised.
- Immobilizer: a device that is intended to prevent driving away of a vehicle powered by its own engine.
- Immobilizer code: a code transmitted to and from immobilizer control unit and engine control unit.
- Key: any device designed and constructed to provide a secure method unsetting the immobilizer.
- Key code: the code transmitted by an electronic key or read from an electrical/electronical key.
- Keypad: device installed in the vehicle, to unset the system by entering a digital code.
- Lock: keys witch or electronic switch for unsetting the system or system components.
- Multiple immobilisation: an immobilisation that will work on at least two essential electrical circuits.
- Normally accessible: a connection or point that is accessible to a potential thief without requiring the dismantling of major items of trim or equipment. Such connections would normally include ignition, transceivers, key switches, direct contact receptacles, power supply, fuses, warning devices, status indicators, etc.
- OE-system: system installed in the factory or under the responsibility of the car manufacturer in his organisation (= not in the dealer-network).
- Overwiring: manipulation of electrical wiring that can include the application of simple signals to the wiring.
- Random code: a system whereby a, with help of an algorithm calculated, code for unsetting, will not be used within a certain time.
- Relay: a device activated by a signal, makes or breaks a connection.
- Rolling code: a system whereby a used code for unsetting will not be used within a certain time limit.
- Second way of unsetting: separate way to unset the system, independent of a remote control.
- Set: the state in which the vehicle cannot be driven under its own power.
- Setting: bringing the system into the set condition.
- Specifications: all requirements as described in the CEA Specifications
- Start interruption: the interruption of the electric circuit, or part of it in such a way that the engine cannot be started via the ignition lock.
- Substitution: replacing (a part of) the security system by prepared components
- System code: a code given to the system by the manufacturer.
- System condition: set condition or unset condition.
- Type identification: individual identification of a system component.
- Unset: the state in which the vehicle can be driven normally.
- Unsetting: bringing the system into the unset condition.

2. GENERAL REQUIREMENTS FOR SECURITY SYSTEMS

2.1 Attack resistance

The security system shall resist tampering or manipulation in such a way that the vehicle can not be driven under its own power within at least five (5) minutes. To test this, an evaluation will be performed to the attack possibilities by the test house in line with chapter 3.

The system shall not be rendered unset by short-circuiting or disconnecting of any cables or accessory connected to the CCU.

If the engine can be started before the immobilizer is activated, this shall not last longer then three (3) seconds for the first time and one (1) second for the next attempt(s). Such a sequence is however limited to a maximum of 20 attempts.

2.2 Setting and unsetting procedures

2.2.1 General

Setting the immobilisation shall be done automatically within sixty (60) seconds from switching off the engine or extracting the key from the ignition lock or within the same period after opening the driver's door (with the engine switched off). As a back-up, automatic setting shall take place within ten (10) minutes after switching off the engine.

It shall not be possible to prevent the automatic setting of the immobilizer by any manipulation, in the set or unset condition.

Setting and unsetting the security system may be made visible outside the vehicle for max. three (3) seconds.

Unsetting the immobilisation circuits is only allowed by the authorised way of unsetting the security system.

If for unsetting the immobilisation a device is used that is directly connected to the key (e.g. transponder key), setting the immobilisation shall take place in less then one (1) second upon taking out the key or switching off the engine.

If, after unsetting, within two (2) minutes no action from the driver on the starter circuit has followed, the immobilizer circuits shall be re-set automatically. This is not applicable for systems using a key connected mechanism (e.g. transponder key).

2.2.2 Remote control

The remote-control device shall have a coded transmitter signal featuring at least one hundred thousand (100,000) different codes.

It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth of 1 % (0.1 %), the correct code that can unset the system.

After each transmission of a signal by the remote control, the code used for unsetting shall change. For this a random key code shall be chosen of at least sixty-four (64) bit.

Transponder keys are regarded as remote controls and will have to satisfy the same requirements.

Removal of the transponder (or the relevant electronic parts) from the key shall lead to permanent visible damage without opening the key.

2.2.3 Keypad

The number of combinations on the keypad shall be at least 10.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth of 1 % (0.1 %), the correct code that can unset the system.

A delay is ten (10) minutes is required in case of an input of three (3) incorrect codes.

The button / controls of the keypad shall not mark readily in order to avoid unauthorised identification.

Short-circuiting, disconnecting or other manipulations with (the wires to and from) the keypad, shall not unset the immobilizer or prevent setting if in the unset status.

If the system is supplied with a standard code upon delivering that can be changed by the customer, this first code shall only last ten (10) times.

2.2.4 Electronic code keys

The number of combinations on the coded keys must be at least 100.000. It shall not be possible to generate, within twenty-four (24) hours with a chance greater than one tenth of 1 % (0.1 %), the correct code that can unset the system.

Short-circuiting, disconnecting or other manipulations with (the wires to and from) the key receptor, shall not unset the immobilisation or prevent setting if in the unset status.

2.2.5 Second unsetting method.

Unsetting procedures aimed at unsetting the system in an alternative way will have to satisfy the same standards for security as the standard unsetting procedures.

2.3 Additional

In addition to the technical requirements of the EU 95/56 and EU 95/54 the security product has to comply with the tests as described in Appendix 2 (drop test and corrosion).

3. ATTACK RESISTANCE EVALUATION OF SECURITY SYSTEMS

3.1 Scope

This section specifies attack tests [procedures and conditions] for original equipment immobilizer intended for installation on class M1 vehicles and N1 vehicles with 12V electrical systems. In case of 24 V vehicles the relevant voltage level will be increased.

3.2 Security Testing

3.2.1 Background

Studies of vehicle theft techniques in the Europe have concluded that thieves may identify critical path methods to overcome security systems, and then consistently repeat this method on further vehicles. Weak areas of security must therefore be eliminated. This is especially important wherever immobilizers are fitted as standard on a range of vehicles For this reason the CEA developed this document to enable the assessment of the time needed to bypass or overcome security devices.
Through liaison with other Research Organisations and the Police, information about new attack methods shall be recognised and the test regime may be updated as appropriate.
The increasing theft resistance has also lead to other ways get control over a vehicle, i.e. key theft, insurance fraud, carjacking, etc. Especially insurance fraud has therefor to be taken into consideration when attacking a vehicle.

3.2.2 General conditions

All tests are applicable to all vehicle control systems or control units that control or share the immobilisation function or alarm function.

The state of the system shall be set.

Tests shall be applied separately or in sequential combination.

Attacks may be applied as a combination of installation and component dependent attack tests.

All mechanical attack techniques may be utilised as part of any of the tests.

The attack tests will be carried out using all tools that are normally available in a garage or workshop. In addition to these standard tools a list is specified (chapter 3.3) for special tools.

During testing the vehicle environment shall be simulated as appropriate:
- Good ambient lighting and temperature
- Unrestricted access to vehicle
- Full range of tools in close proximity to vehicle

Other items:

- Full system knowledge (including pre-testing) prior to attack (including Workshop Manual, Repair Manual and technical applicant file, provided by the manufacturer)
- Two engineers who may work simultaneously
- Damage to system/vehicle at low cost (less than 10 % of vehicle value) with respect to overall vehicle value
- Any alarm noise to be disregarded
- Start of timing : from opening of any door, bonnet or hood
- End of timing: see 3.2.4 Pass / fail criteria
- Door locks and steering locks are not taken into consideration
- Additional protection devices (hood locks, brackets, etc) will be involved in the attack test

3.2.3 Attack Testing

Applied to Control equipment

- Mechanical impact (min. three (3) times).
- High electromagnetic field [up to 50V/m at the control equipment] See appendix 1.
- Magnetic field [small permanent »rare-earth» magnet] Min. Remanence (mT) 1150 - 1200
- Open circuit of umbilical connection to the immobilizer control units
- Short circuit of umbilical connection to the immobilizer control units to +12V and 0V (+24 V and 0 V for 24 V systems)

Applied to all »Normally Accessible Connections»

- Voltage removal with re-instatement [constant and rapid intermittent]
  Interruption and reconnection of the connections repeatedly for varying intervals and frequencies, up to 0.1s to 600s nominally.

- Over-voltage and reverse voltage
  Application of [up to] ±36V for 60s. 12 V systems: up to ±24 V; 24 V systems up to ±36 V.
  Instantaneous application and removal

- Short circuiting to +12V and 0V, resp. +24 V and 0 V.
- Open circuiting

- Open circuiting of any single or multiple fuses
  Main immobilizer control unit or separate immobilizer control module fuses, or any other vehicle fuses. Also re-instatement of fuses

- Key code/immobilizer code sequential scanning
- Key code/immobilizer code copying and re-transmission
- Key code/immobilizer code, prediction of next valid code, and transmission

- Mechanical attack on key switch

Applied to electronic coded immobilisation.

These attack tests are in addition to the above and apply to »Software lock» immobilisation.

Default or Limp home modes of the immobilised vehicle control system or control unit shall not be activated under deliberate manipulation or attack to enable normal or nearly normal operation of the vehicle.

Additional tests:

- Open circuiting of the coded input or inputs to the original vehicle control system or control unit.
- Short circuiting to +12V and 0V(resp. +24 V and 0 V) of the coded input or inputs to the original vehicle control system or control unit.
- Overwiring [including application of simple changing or periodic signals].

Substitution of security components

Substituted immobilizer and / or vehicle control unit[s], e.g.:
- same connector pin-out and different code.
- same connector pin-out and »don't care» input.
- different connector pin-out and interface interconnection module.
- originally disconnected from a vehicle with an unset immobilizer.
- substituted, partial or complete immobilisation and/or vehicle control system from any source, original or manipulated.

3.2.4 Pass / fail criteria

The security system and its installation shall resist the attack tests for a minimum duration of 5 minutes (300 seconds) against unsetting or bypassing the security system in order to provide normal or partly normal vehicle operation. This includes partial re-mobilisation of the vehicle to allow the vehicle to be moved in a reasonably controlled mode under its own power. The system will be considered to be bypassed or unset if it can be moved under its own power, even at low speed, a distance of 1 kilometre over a one-hour period without undue engine stalling or restriction of steering control. Therefore default or limp home modes of vehicle operation shall be considered when specifying immobilisation attack resistance.

Up to 3 separate sequential attack attempts shall be conducted.

- If in the first attempt, the time to overcome the system will be **more than 10 minutes**, the system is passed.
- If in the second or third attempt the time to overcome the system will be **less than 5 minutes**, the system has failed, otherwise it has passed the criteria.

After each attempt, the security system shall be brought back into the initial state.

3.3 List of attack tools

In this list tools will be specified if they cannot be considered as normal hand tools in a garage or workshop.
The test house will submit, upon request of the manufacturer, the actual list of mechanical tools that might be used in the attack test.

0-36V power supply
0-20 MHz function generator [square wave, sinus wave, saw tooth, pulse]
Piezo-electric spark generator
Electromagnetic field generator
Code scanners
Code grabbers [with analysis, processing and re-transmission capability]
Multimeter
Laptop PC
PC software
PC input/output devices
Diagnostic equipment [OE or independent]

Magnet:	strong permanent magnet, Min. Remanence (mT) 1150 - 1200
Keys	Keys of the same type as the immobilizer
Aerosol foam	quick setting foams or gels
Freezing agent	

Tools may be altered by shaping, drilling, bending or grinding so that they are more appropriate to a particular application.

Power drill	battery powered [HSS bit, max. 13mm and hole cutters]
Angle grinder	battery powered
Jigsaw	battery powered

Lock puller	hand held
Pick manipulation	
Car key jigglers	
Mini jigglers	
«Majestic» lock pick set	
Tubular picks	
Curved shims	

Component substitution:
Any electrical, electronic or mechanical components that are:

- available through any direct or indirect channels
  or
- fabricated or modified from freely available materials or components.

This shall include electrical or electronic control units

4. DOCUMENTATION

For this paper, the CEA Anti-theft working group used the following documentation:

- EU Directives EU 95/56 and EU 95/54
- European Insurers Specifications for security systems to protect against motor vehicle theft, Comité Européen des Assurances, Draft, 01/03
- Classification Rules for Anti-theft Protection systems - SRA/CNPP, 1/94
- The British Insurance Industry Criteria for Vehicle Security, Issue 2, The Motor Insurance Repair Research Centre, 1/96 (incl. updates).
- Immobilisation system specification - Allianz Zentrum fur Technik, 7/93 and 6/94).
- Homologation Directive Security Systems for Passenger Cars , SCM, AA-03, 1/99
- Draft Rules for the Classification of Systems of Protection of Motor Vehicles against Theft, Draft ANIA, 11/94
- Specification Profile for Electronically Coded OEM Immobilizers, AZT, Update 6/97