EUROPEAN CONFERENCE OF MINISTERS OF TRANSPORT
COUNCIL OF MINISTERS

Council of Ministers

IMPROVING SECURITY FOR ROAD FREIGHT VEHICLES

This document is presented under item 7. of the Council of Ministers’ Draft Agenda of 29-30 May 2001 in Lisbon, for information.
# TABLE OF CONTENTS

EXECUTIVE SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS .............................................. 3

1. INTRODUCTION .......................................................................................................................... 5

2. NATURE OF THE PROBLEM ..................................................................................................... 6

3. LEGAL REQUIREMENTS, GUIDELINES, STANDARDS ............................................................. 7

4. PREVENTIVE ANTI-THEFT DEVICES ....................................................................................... 11

5. AFTER-THEFT SYSTEMS .......................................................................................................... 15

6. IMPLEMENTATION ISSUES; CONCLUSIONS AND RECOMMENDATIONS .............................. 19

ANNEXES

<table>
<thead>
<tr>
<th>Annex</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex 1</td>
<td>Vehicle Identification Systems</td>
<td>25</td>
</tr>
<tr>
<td>Annex 2</td>
<td>Glossary</td>
<td>30</td>
</tr>
<tr>
<td>Annex 3</td>
<td>References</td>
<td>31</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

1. The range and sophistication of anti-theft devices and after-theft systems available on the market is increasing rapidly; in particular, there are new developments to track the goods themselves throughout transport.

2. More goods vehicles are being equipped with such devices but goods vehicle crime is still increasing.

3. There are barriers to the wider introduction of these systems and equipment: Hauliers often underestimate the risks; manufacturers do not want to fit them as standard; insurance companies do not always give premium reductions; technical standards do not yet exist.

4. It is not possible to evaluate the cost effectiveness of the equipment used since there is not enough evidence on the extent of crime, or on the way the equipment is used and works.

5. Fitting anti-theft devices to vehicles and developing after-theft systems are only a part of a broader strategy to combat road freight transport crime. Such a strategy, to be successful, requires coordination and cooperation of many actors. At present this cooperation is not widely developed.

RECOMMENDATIONS TO TRANSPORT AUTHORITIES:

1. Set quantified targets for goods vehicle crime reduction, in cooperation and coordination with other authorities.

2. Create partnerships with other authorities and actors – in particular, appoint a coordinator of anti-crime activities in the Ministries of Transport.

3. Accelerate technical work in the framework of CEN and UN/ECE on standardisation of security equipment, on marking of vehicles and components and also work on legal requirements for fitting heavy goods vehicles with specific security equipment and on related issues - e.g. accreditation of responsible testing organisations to international standards.

4. In cooperation with the operators associations and the Police authorities examine the truck parking areas in their territory, to see what further security steps need to be taken. Improve these parking areas and indicate the degree of protection provided e.g. by a star or grading system. Use such an evaluation to improve further the joint IRU-ECMT booklet on safe parking areas.

1. See Chapter 6 for more details.
5. Together with the Police and the operators associations provide and disseminate advice and guidance to operators, especially on safe routes, parking areas with high security, precautions to take and appropriate equipment.

6. Lobby police and interior ministries to provide more police attention and resources to monitoring, preventing and solving goods vehicle crime.

7. Examine the possibility of introducing incentives for meeting minimum security standards for goods vehicles at international level, linked to the ECMT multilateral quota.

8. Follow and support developments in technology to track the goods themselves throughout transport.

REQUESTS TO OTHER AUTHORITIES AND ACTORS:

1. **Operators:**
   - provide security advice to drivers on the risks and on good practice for achieving high security;
   - verify and monitor security records of staff and agency drivers;
   - improve depot and port area security, e.g. installation of Closed Circuit TV (CCTV) and disseminate information on the subject to operators.

2. **Manufacturing industry:**
   - continue to participate in a dialogue on fitting devices at manufacturing stage with the objective to improve the level of security of vehicles.

3. **Insurance industry:**
   - use their records and data to improve the dissemination of information on the extent of the problem;
   - provide advice and guidance to operators on appropriate precautions and equipment.
1. INTRODUCTION

The Council of Ministers of ECMT has adopted two resolutions on Crime in Transport - at its meetings in Berlin in 1997 and Warsaw in 1999. One of the recommendations in Warsaw was a request for the Committee of Deputies to set up appropriate methods and structures so that the Council of Ministers could contribute to the fight against crime, through focused actions on the particular issues identified.

This resolution led to the establishment of a “Crime in Transport” Steering Group with representatives of the different interests concerned, including governments (Ministries of Transport, Economics and Interior), International organisations (EU, UN/ECE, EUROPOL, INTERPOL) transport operators, insurance companies and others.

The Steering Group identified immediate priorities for its work. These included an examination of how the introduction of anti-theft devices and vehicle-tracking systems could help to reduce goods vehicle crime. A study was undertaken with the purpose of:

- Providing information on anti-theft devices and vehicle tracking systems and on the contribution they can make to reducing vehicle-related transport crime.
- Assessing the cost effectiveness and commercial acceptability of the various anti-theft devices and tracking systems currently available.
- Reviewing and reporting on ways in which major European transport insurers, vehicle manufacturers and transport companies could support and encourage the introduction of effective security devices to prevent and minimize crime in transport.
- Considering ways to encourage the introduction and utilization of the most effective devices and systems, which are supported by insurers, manufacturers and operators.

This report is focused mainly on security for road freight transport vehicles and structured as follows: Chapter 2 sets out the background and framework to the work. Chapter 3 describes the existing legal situation as regards vehicle security. Chapter 4 sets out the range of equipment that is available now to prevent vehicles being stolen, while Chapter 5 deals with the equipment and devices that are available to track and recover stolen vehicles. Chapter 6 contains the general conclusions and recommendations.

This report has focussed mainly on the vehicles. The goods transported are of course of equal or often of much greater value. Many of the techniques described here protect the goods as well as the vehicles. There is, and this is referred to where relevant in this report, a substantial and growing amount of work being done to protect and track goods.
2. NATURE OF THE PROBLEM

The report providing the available data on the topic shows that the theft of goods vehicles and their loads is a serious problem resulting in losses valued at many millions of Euros annually. Though comparative statistics are not reliable-the data show that in several countries up to 1% of the fleet is stolen each year. There is evidence too that the situation is getting worse in some countries and that the crimes are carefully organised since high value loads are targeted. However, the risks of theft vary widely and depend among other things on the location, on the goods carried, and on the level of security.

Theft of goods vehicles is part of a wider problem. According to 1996 statistics from the European Insurance Committee vehicle theft is a serious problem. In nine major European countries, 1 million vehicles were stolen in 1995, of which over half a million were never recovered. It is estimated that this type of crime results in an annual economic loss of over four billion Euro.

It is a problem that affects many countries and numerous companies. The partial evidence available indicates too that criminals act in increasingly sophisticated ways at both national and international levels to identify suitable loads, steal them and dispose of them. There is a large “market” for stolen goods, and not only high value goods.

The evidence available indicated that this problem is not given a high priority by police forces, though the economic losses are very high.

This report sets out some of the precautions that can be taken by the different actors involved. The focus of the report is mainly on the aids that are available to reduce the risk of crime and to increase the chances of recovery of stolen vehicles. But, in compiling the report, it became very clear that these aids were only a part of the solution.

There are numerous actors with responsibilities for the safe shipment of goods – the manufacturers, the shippers, the transport operators, the public and private authorities responsible for ports, stations and other places of transit, the police, the customs authorities, the insurance companies and the different government departments involved.

All of the groups named above have responsibilities and possibilities to reduce crime. Actions taken together can have synergistic effects. The technical equipment described later will be more effective when it is used properly and when it is combined with other measures that create additional difficulties to criminals. Some of these are set out in Chapter 6.

The technologies set out here are for the most part available now – often quite cheaply. There are difficulties in implementation including the technical and legal issues set out in Chapters 4, 5 and 6. But there is a more basic difficulty of getting all those involved in transport to reduce the risks and take appropriate precautions.
3. LEGAL REQUIREMENTS, GUIDELINES, STANDARDS

3.1. Introduction

This chapter first describes the international legal requirements for fitting security devices to vehicles and the specifications for these devices. It also describes international and national guidelines, codes of practice and standards in some countries.

3.2. Regulations for security devices

UN/ECE and EU regulations prescribe the conditions that vehicle alarm systems must meet; they do not say that such devices should be fitted. There is no legal requirement in this area except the necessity to have a Vehicle Identification Number (VIN).

3.2.1. UN/ECE

Adoption of international standards for construction and approval of power driven vehicles and their equipment and parts, as well as the classification and definition of vehicle categories is the responsibility of the World Forum for Harmonisation of Vehicle Regulations (WP.29), which works in the framework of the UN/ECE.

The classification and definition of power-driven vehicles and trailers are contained in the Consolidated Resolution on the construction of vehicles (R.E.3), annex 7/Rev.2 (document TRANS/WP.29/78/Rev.1/Amend.2).

The UN/ECE system of Regulations for vehicles and their equipment and parts functions in the framework of the Agreement of 20 March 1958 (amended as of 16 October 1995), entitled: “Agreement concerning the adoption of Uniform Technical Prescriptions for wheeled Vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions” (document E/ECE/324-E/ECE/TRANS/505/Rev.2).

There are currently 112 ECE Regulations annexed to the 1958 Agreement. Two of these Regulations concern uniform conditions for type approval of devices intended to protect vehicles against unauthorised use:

Regulation No. 18: "Uniform provisions concerning the approval of motor vehicles with regard to their protection against unauthorised use" (document E/ECE/324-E/ECE/TRANS/505/Rev.1/Add.17/Rev.2).

Regulation No. 97: "Uniform provisions concerning the approval of Vehicle Alarm Systems (VAS) and of motor vehicles with regard to their alarm systems (AS)" (documents E/ECE/324-E/ECE/TRANS/505/Rev.1/Add.96 and Amend.1 and Amend.2).

“Regulation No. 18 concerns mechanical locking devices, whilst Regulation No. 97 addresses electronic alarms and immobilisers. A new Regulation for passenger vehicles and light-duty vehicles has already been finalised by WP.29 which will combine mechanical and electronic
devices. Once the internal European Community procedures have been completed, this document will be finalised.

No ECE Regulation exists for the approval or certification of tracking equipment installed to protect a payload and/or for tracking systems. If installed in vehicles, such systems would most likely be subject to type approval pursuant to ECE Regulation No. 10: “Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility” (document E/ECE/324-E/ECE/TRANS/505/Rev.1/Add.9/Rev.2 and Amend.1, Corr.1); this ECE Regulation is fully aligned with the European Community Directive 95/54/EC.

3.2.2. EU Directives

The Vehicle Identification Number (VIN) - one of the special security markings - is a fixed combination of 17 alpha-numeric characters assigned to each vehicle by the manufacturer to ensure that every vehicle can be clearly identified by the manufacturer for a period of 30 years. EC Directive 76/114/EEC amended by Directive 78/507/EEC requires all manufacturers trading in the EC to firmly fix a manufacturer’s plate in a conspicuous and readily accessible place on a part not subject to replacement in use. Amongst other information, the manufacturer’s plate will show the full 17 digit VIN in characters of at least 4 mm in height. The above Directives also define rules concern the visibility of the VIN, which components should be marked, and so on.

Immobiliser - Directive 95/56 EC.

The Directive relates to devices to prevent unauthorized use of motor vehicles and amends Directive 74/61/EEC. The directive defines the requirements for a "device to prevent unauthorised use". A "device to prevent unauthorised use" means a system designed to prevent unauthorised normal activation of the engine or other source of main engine power of the vehicle in combination with at least one system which locks the steering, locks the transmission or locks the gear shift control. It therefore requires the application of an 'immobiliser' and a "mechanical locking device". The directive also defines requirements for a Vehicle Alarm System (VAS) which are optional.

The scope of the directive applies to passenger cars and to small commercial vehicles. These vehicles have to comply with the requirements of fitting a mechanical device and an immobiliser. A “VAS” can be optionally fitted. However, if immobilisers or VAS are fitted to other vehicle categories, they have to comply with the requirements of the directive.

3.3. European standardisation for after-theft devices

Numerous new technologies and after-theft systems are coming on the market and aim to supply means and information to law enforcement agencies in order to recover stolen vehicles. Faced with this situation, the European standardisation committee, which deals with matters related to transport and road telematics (CEN/TC278), has created a Working Group, WG14 dedicated to after-theft systems.

WG14 has the mission to draw up European Standards for after-theft systems in order to harmonise their main characteristics, get maximum interoperability between such systems as well as specify performance and security characteristics against attack, with the following objectives:
− to provide European coverage of detection operations and after-theft systems services, given the ability of vehicles to cross borders;
− to reduce the number of different technologies and harmonise information that may be operated by law enforcement (e.g.: A vehicle stolen in Germany must be capable of being detected by the means operated by French law enforcement agencies);
− to facilitate the fitting of these devices on new vehicles in manufacturing by the vehicle manufacturers;
− to reduce the cost of these devices by a large implementation in Europe;
− to ensure guaranteed reliability and quality of these Devices (e.g.: to avoid false alarms ...), as a basis for official accreditation and homologation of these Systems in Europe;
− to avoid monopoly positions.

WG14 involves about fifty Experts from 18 European countries, representing police officers, insurance associations, car manufacturers, transport associations, car rental association, consumers representatives as well as systems and products providers. Also it is working in co-ordination with others European and international organisations such as EPCWG (European Police Co-operation Working Group) EUROPOL, INTERPOL, CEA (European Insurance Association), VDA (German Car Manufacturers Association) and ECMT/Steering Group “Crime in Transport”.

The scope of standardisation work is restricted to technical aspects and does not concern the information exchanged between the European Law Enforcement Agencies. The standardisation work must also take into consideration the legal restrictions in force in each country such as Rules of privacy and protection, safety regulations for e.g. remote de-grading devices...

This standardisation work started in 1997 and has today compiled an inventory of Users requirements in Europe and specified the architecture of these Systems. Definition of the standards is scheduled for 2002-2003, though some countries would like faster progress.

3.4. Recommendations, codes of practice


“Authorities responsible for vehicle regulations:

− to examine forms of vehicle identification which would make removal or falsification as difficult as possible;
− to examine security procedures that can prevent stolen vehicles being given new identities under their existing Vehicle Identification Number (VIN);
− to take initiatives to make the alteration or removal of a VIN a crime;
− to take initiatives to make the current voluntary practice of VIN to trailers over 750 kg compulsory (based on the EU Directive 76/114 on statutory plates);
− to encourage the voluntary marking of major components and the definition of a common European specification for making the VIN more visible;
− to encourage the development of European requirements for security features such as effective door and luggage compartment locks;
– to take measures for exchange of computerised information among registration authorities with a view to preventing registration of stolen vehicles and other vehicle-related fraud.

Road transport operators, through their national and international organisations:
– to work on introducing modern communication systems from vehicles and for tracking vehicles in international transport.

Vehicle manufacturers and equipment suppliers:
– to provide improved anti-theft systems on vehicles as indicated by EU Directive 95/56 of 8 November 1995 and ECE Regulations 18 and 97;
– to examine the possibilities for improving the security of vehicle identification systems;
– to test, for example in the context of the EU technological programmes, devices and equipment that can reduce the possibilities of theft or falsification.

Insurance companies:
– to encourage and provide incentives to operators to use effective anti-theft devices and systems;
– to provide information to operators on these systems and on good practice.”

3.5. National guidelines

Some countries have issued recommendations to those involved in vehicle security intended especially for manufacturers and operators. This defines and describes areas of HGV security worthy of consideration by manufacturers - Perimeter security, immobilisation, accessories and general equipment, special security markings, manufacturer’s replacement key policy. Also in the United Kingdom the insurance industry has published guidelines (Axa Insurance) for operators and drivers.
4. PREVENTIVE ANTI-THEFT DEVICES

Anti-theft security devices are available for Heavy Goods Vehicles (HGV’s) throughout Europe. There is a considerable market for products covering all aspects of security for vehicles and trailers, from a simple padlock to a fully integrated alarmed and immobilized locking system. Anti-theft devices, depending on the age of the vehicle, may have been installed at time of manufacture or through after-market installation. They can be mechanical, electrical or electronic. There is a wide choice of products including locking devices for handbrakes and steering locks. The more sophisticated security systems require to be installed by accredited installers, which may take several hours to be fitted properly. Nowadays practically all new commercial vehicles are equipped with antitheft devices which meet the condition of Directive 95/56/EC or the equivalent UN/ECE Regulations Nos. 18 and 97. But no single device is sufficient to provide adequate security for goods vehicles.

4.1. Anti theft devices include:

- **Air Brake Immobilisers.** The air brake lock once activated prevents the vehicle from being driven by locking the brakes on. The activation has several methods of operation, switching off the ignition system can automatically set the lock, with or without the driver’s knowledge. The main advantage is no additional responsibility for the driver in setting the locking device. Earlier technology relied on the driver setting the locking mechanism separately from the ignition system. More sophisticated devices are controlled by chip technology. The Air Brake locking mechanism may also rely on the driver presenting the chip to control the locking device. The chip can be readily concealed, for example in the ignition key. This technology is also compatible with alarm systems, including the setting of the alarm as one operation by the driver.

- **Alarms.** There are two distinct functions for alarms fitted to vehicles - audible siren and vehicle immobilisation. The audible alarm is to deter the thief by emitting loud noise. The immobilising alarm system activates devices that prevent the vehicle from being driven away. Alarms can include both facilities, audible and immobilising, which delays or prevents the attempt to steal the vehicle. The alarms are either set mechanically by a key or similar device, or by using a remote control facility. Both types of setting mechanism are subject to technological improvement. As with the case of keys, the variations are almost limitless. Current technology can extend the alarm function to other parts of the vehicle, such as the load area of a box van, which can be fitted with sensors detecting presence in the load-carrying compartment. The same sensor systems might also be used to detect stowaways during international journeys. It is also possible to fit silent alarms and radio paging systems.

  The after market in alarms caters for all eventualities, including attack by cutting the wires and the overt problems of power sources - the vehicles batteries being on open view.

  The alarm system routinely requires a back-up power source in the event of the vehicle batteries being subjected to interference or theft. Unlike building alarms, those fitted to goods vehicles have to be robust, designed to withstand extremes of temperature and disturbance caused by road journeys including high power truck washing.

- **Alarm sensors.** Alarm sensors including panic buttons are components used to activate the actual alarm system. These include movement sensors that, depending on the sensitivity of the setting, will operate the alarm function. Ultrasonic sensors work by emitting and receiving high frequency sound waves, any interruption of the frequency pattern outside of set limits will activate the alarm system. Being sensitive to atmospheric pressure, this type of alarm sensor is prone to false alarm activation
through high winds. In some cases microwave sensors may be more reliable. There are various limitations as to their use in a loaded goods area, which reduces the scope of the sensor.

Panic buttons can be installed. The system requires monitoring of the sending unit, backed up by the ability to establish where the call has come from and its effective use has to be balanced against the availability of response to the alarm activation. This type of system is more common in the cash in transit industry.

- **Cab locks.** Depending on the age of the vehicle, more sophisticated locks are now available to be fitted at the time of manufacture, or after, depending on the customer's requirements. Deadlocks or Slamlocks may require physical use of a key or remote controlled device, which can be linked to include the setting of an integrated alarm system. Additional locking security in the cab includes mechanical devices such as hand brake and steering locks, which are locked in place by the driver. Other security devices associated with the HGV cab, include fuel locks, starter motor and ignition isolators.

Depending on the level of security these devices can be activated by solenoids at the time of setting the alarm system. These systems are aimed at preventing the physical driving away of the vehicle with the load security and alarming an additional consideration depending on the type of vehicle. Clearly, a rigid box vehicle could have all the relevant alarm systems installed linked to the cab system. The financial commitment is dependent on the load, or potential goods being transported. Clearly goods valued in excess of Euro 100,000 should attract appropriate security investment.

- **Cab tilt locks.** The HGV cab unit on a truck is capable of being tilted forward to allow access to the engine compartment of the vehicle. For added security, access to this area can be prevented by locking the tilt mechanism.

- **Container Locks.** Containers are the steel structure boxes routinely used for the import and export of goods by sea. The containers are compatible with specially constructed trailers for the conveyance of goods of virtually every description and value. Routinely the containers are serviced by two doors at one end of the structure. The doors are designed to have locking devices and identification (Customs) seals fitted that can be put in place for cross-border road haulage. The locks used can be a simple padlock as the lowest level of security up to substantial locking devices, securing the doors against sustained attack. The locks may also be connected to an audible sounding alarm to alert the driver.

The various locking systems also serve to prevent potential thieves from examining the container for goods worth stealing. Conversely, drivers may leave the container unlocked when empty or where the goods would not be attractive to a thief. Invariably the containers are the property of a container or shipping line company and are routinely serial marked and identifiable. The identification of containers routinely forms part of an audit trail, including the goods being carried. The container locks may also have a security seal with a unique identification number, which was installed at the time of loading, designed to be tamper proof for visual inspection throughout its journey. Locks that produce a random combination are also available for securing the doors.

- **Double locks.** A lock that is operated solely by the use of a key, to unlock or lock a door. The construction and installation of this type of lock is an effective means of preventing unauthorised entry. The Double lock relies on the driver literally turning the key to activate it; otherwise, it remains insecure. Correctly installed double locks can be very effective. However, if the driver does not lock it, the vehicle and load are exposed.
• **Driver recognition systems.** The driver is equipped with a smart card, similar to a credit card with an embedded chip. The chip can also be in a key fob or similar holder carried by the driver. The HGV cab is equipped with an aerial type detector unit that responds to the chip on recognition of the driver who has full command of the vehicle and its systems.

In the absence of the chip, the vehicle cannot be moved, despite unlocked doors and including keys left in the ignition. The same technology is available for door locks, including goods doors of various descriptions for box vans and similar constructed load areas.

• **Identification Systems.** These systems allow the unequivocal identification of a vehicle as being the “registered stolen vehicle”. This may be by means of a secure process that allows the unique vehicle data to be read, e.g. by electronically reading the VIN, registration number, and other data like theft status, model, color and, if possible, position. ²

• **Key-switches.** High security key-switches have in excess of 100,000 combinations. Replacement of the unique key is frequently only available from the supplying factory and not through normal key cutting services.

• **King Pin Locks.** A mechanical locking device for the Articulated Trailer designed to prevent the coupling to the towing unit. The King Pin Lock is secured to the male coupling link of the trailer, similar to securing a wheel clamp, immobilising the vehicle by preventing a towing unit from coupling up. The construction of the locks is mechanical, with a key, and requires to be fitted by hand. The fitting of this type of lock is not the most attractive of tasks for drivers, which can lead to non-use.

• **Security Curtains.** Heavy-duty security curtains with varying degrees of attack resistance. They can be fitted to an alarm system, which indicates when small wires that have been imbedded within the curtain material are cut.

• **Slam locks.** The locking of HGV doors by closing shut the door (slamming) which then requires to be unlocked to regain entry. The locking system takes the onus of locking the vehicle door from the driver, every time the vehicle is left unattended. The delivery driver does not have too physically “lock up” each time the doors are closed. This type of security is becoming the norm for parcel carriers and other multi-drop delivery vehicles and is normally fitted at time of manufacture. Slam locks are capable of being fitted to most vehicle doors, including panel vans, and barn and shutter doors at the rear or side of load carrying areas.

• **Security window grills.** Grills are available for making windows less vulnerable to attack, depending on the extent of security required. This type of grill security is common in the conveyance of cash-in-transit, where the crew are more exposed to personal attack whilst with the vehicle. Many vehicle manufacturers now built vans with all metal doors with windows as an option.

Bulkhead grills are more common in box type vans, with a dual purpose of safety and visual access. Apart from affording visual control of the load, the grill also serves to protect the occupant from the potential of the load shifting into the cab area.

---

• **Trailers, curtainside** are the frequent preference for hauliers for the ease of access to the load from either side of the trailer or rigid vehicle and maximising the vehicles load (weight) carrying capacity. Consequently, the ease of access and the construction of the curtainside make them vulnerable to theft. This is despite similar locking systems and alarm systems that are available offering varying degrees of protection to the load. The material used for the curtain varies in strength in preventing access to the load. It is not uncommon for sharp knives to be used to cut open and expose goods for theft. This is a common crime because of the ease of gaining access to the load.

The levels of security have the potential of being greatly advanced by the marketing of new products such as security curtains, and, a new product which has a type of gull wing construction, mechanically operated opening up to roof height throughout the length of the storage area. This product appears to have an added advantage of quicker access to the load area compared to curtainsides requiring numerous buckle and belt type securing. The Gull Wing is of metal construction, which should be readily compatible, to all other security and locking devices. However, weight limitations and costs may impede the take-up of this product.

Most if not all anti-theft devices described above are used in varying forms by international road hauliers throughout Europe. The cost of these items varies from country to country and Transport companies are well advised to seek expert advice on the efficacy of particular anti-theft devices. The cost effectiveness of anti-theft devices can not be readily measured unless adequate data is available for detailed analysis. Vehicle manufacturers have reported they would welcome such information to demonstrate the case for the fitting of improved anti-theft devices to HGV’s prior to sale.

Improvements can certainly be made to the level of anti-theft devices fitted as standard by vehicle manufacturers, but acceptance of the cost of such devices, which would reduce with demand, is dependent on a better appreciation of the true cost of Crime in Transport and its consequences. The enhancement of the available information on the scale of crime in transport should have the affect of convincing both vehicle manufacturers and the buyers of such vehicles that improvements in vehicle security is a cost effective option.

There is a debate on the viability and value of the introduction of a legal requirement to fit improved anti-theft devices to HGV’s by vehicle manufacturers. At present truck manufacturers argue that they obtain limited returns on the investment made by installing additional anti-theft devices in their vehicles. They also maintain that truck manufacturers already face onerous legislative burdens to satisfy existing requirements. If further requirements are to be imposed, the timescale enacted should be realistic. More discussion may be required with vehicle manufacturers, insurers, international haulage operators and transport companies before recommendations can be made.

There seems to be a reluctance by the truck manufacturers to fit any more than an electronic type of immobilisation system as standard equipment. This is understandable due to the fact that apart from tractor units, the manufacturers are unaware of the type of operation the vehicle will carry out. Furthermore the majority of vehicles will then have a specialist body fitted. The type of body fitted will vary greatly; additional security will typically be provided by specialist companies in the aftermarket.
5. AFTER-THEFT SYSTEMS

After-theft systems aim to provide to law enforcement authorities means, information and services in order to assist detection and recovery of stolen vehicles. They act when the anti-theft device has broken down or been bypassed by the thief and when the theft has been registered (theft registration) or eventually detected by sensors (theft warning). Unlike anti-theft devices, the on board equipment of these systems interact with external communication means and information systems. Usually these systems involve security agencies or security service providers but in all cases involve the law enforcement for security and legal procedures (theft registration, control, detection, official statement, impound, arrest...).

Generally speaking, these systems consist of a radio device on vehicle, detection equipment (hand-held, mobile on vehicle or stationary) or infrastructure telecommunication network and operating centres operated by service providers or directly by the law enforcement agency.

Their electronic features allow the automatic detection of stolen vehicles and consequently reduce the routine controls operated by the law enforcement and insurance agencies.

5.1. Two types of operations

Short range operation

The short range operations are operated only in the vicinity (direct line of sight, less than one hundred meters) of vehicles with the help of detection equipment (hand-held, on police vehicle or stationary) usually used directly by law enforcement. So the law enforcement operations are restricted and located in their immediate vicinity during their own priority security mission. Short range radio technologies are used for these operations.

Long range operation

The long range operations are operated at distance normally greater than line of sight (up to several kilometres), and are generally associated to location functions. The long range radio technologies are used for these operations such as existing and standardised network (GSM, satellite system, soon the future technologies GPRS, UMTS, …), or other specific and property networks and protocols.

5.2. Short range systems

When the theft registration has been reported, two types of detection are possible:

Detection by signalling

The device of a stolen vehicle is remotely activated in alarm status via an infrastructure telecom. So during their service, the law enforcement can use short range hand-held detection devices and automatically detect this alarm when this stolen vehicle is located in their vicinity.
Detection by consulting

The data file of registered stolen vehicles integrated within the detection unit is updated. So the law enforcement agencies can use this hand held device that automatically interrogates all the vehicles in vicinity, compares the identifications sent by these vehicles, with its database and detect stolen vehicles.

The identification function can be operated in all cases independently of whether the vehicles are stolen or not:

The unequivocal identification of a vehicle can be checked using a reader in the vicinity. These hand held devices allow the identification data programmed in secure memory of on board equipment such as vehicle identification number, model, colour, main components of the vehicle and other data to be recorded. (See Annex 1 for more detailed information on these identification systems).

5.3. Long range systems

Location by geographic position (tracking systems)

When the theft registration has been reported, the device on the stolen vehicle is remotely activated. So the geographic position and the tracking of this vehicle can be displayed in real time on a mapping station located in the operating centre (head quarters of the law enforcement or security agency).

These systems use the location technologies based on either the Global Positioning System (GPS), soon the future technologies Low Earth Orbiting (LEO) satellites, GALILEO European Satellite System, or other specific location networks. The GSM, GPRS and UMTS may be also used for an approximate location.

In the fleet management area, these systems are already being operated to improve the quality and profitability of the transport function. Unlike fleet management systems, after-theft location systems must resist criminal attacks on the antenna, power supply, jamming, breakdown, data, false alarms...

Location by homing (tracking systems)

When the theft has been reported, the device of the stolen vehicle is remotely activated. So with the help of a mobile detection on a police patrol vehicle, the direction and range of the detected vehicle is known and displayed in real time. Thus the law enforcement agency can track and intercept this vehicle without the necessary use of landmarks or absolute geographic references.

These systems use the homing technologies based on specific and property networks and protocols.

Remote degrading

When the theft has been reported, the device of a stolen vehicle is remotely activated. So the on board device can command electronic degrading actions for this stolen vehicle.

These systems should be subject to legal conditions in order to preserve safety (e.g. immobilise the vehicle when the key is removed, not immobilise the vehicle whilst in motion unless through a progressive reduction of engine performance, etc. The regulations required for setting up these new
technologies are not yet fully drawn up or harmonised in Europe. The UN/ECE’s WP.29 is already working on possible conditions for such a harmonisation.

**Theft indication**

These systems act independently of the theft registration. Once the vehicle has been subjected to abnormal use, vehicle sensors set off an alarm. The device on the vehicle relays the warning message to the operating centre via a radio communication network.

This function is usually attached to location systems (geographic position or homing) and can be considered as one service among the other transport management services such as time, temperature, delivery site, loading/unloading time...

### 5.4. After-theft systems particularities

**Actors involved** - The setting up of after-theft systems involves multiple actors such as law enforcement agencies, insurance companies, vehicle manufacturers, Telecom operators and service providers in security. During the successive operating steps, the functions and services supplied by the after-theft systems and private service providers are voluntarily restricted to give to law enforcement the information for detection and recovery. By legislation, the law enforcement agency is the one authority able to proceed to arrest and recovery of the registered stolen vehicles. Therefore, the global efficiency of after-theft systems depends in part on resources capability, priority missions and availability of the law enforcement authorities.

The European Law Enforcement Agencies (LEA) have underlined the following principles:

- there is no obligation on the LEA to respond to the operation of such a device;
- the system does not place an unwarranted burden on LEA resources through its operation, data handling or LEA response.

**Security** - With respect to security considerations, after-theft systems differ from the other systems for road telematics such as automatic toll collection, road traffic management, fleet management... Such systems are not subjected to illicit tampering: they operate in a co-operative environment.

On the other hand, after-theft systems must resist possible threats from thieves or organised gangs through: breakdown, interference, jamming, copy, simulation, decoys, alteration, discovery (case of hidden device)... Their design and operation must include security devices and procedures and also strict approval procedures for security agencies or companies that operate these systems.

**Regulation** - The installation of on-board electronic devices that allow automatic detection and, in some cases, the location of vehicles, must be designed and operated in order to take into account rules on civil liberties, prevent possible fraudulent uses and individual security in road transport.

**Power supply** - Most after-theft devices require a power source, which is usually the vehicle’s battery. If this power supply is interrupted or broken for any reason, the on-board device must be able to continue to operate for a certain duration. The European standardisation (see below) will specify that.

For loads normally transported in containers on articulated trucks or in canvas sided (tilt) trailers, both of which may be easily detached from the tractor unit (motorised cab), the design of a self-power supply for the after-theft device is a serious difficulty, mainly for the long range systems which require a
significant radio power. On the other hand, some existing short range devices include a self-power supply giving self-operation over 5 years.

5.5. Economic considerations

The investment costs required to implement and operate such systems must be compared with the resulting benefits, taking account of the value of the vehicle and goods carried as well as the real impact on crime in road freight transport. In all cases, the amount for investment and operations must remain small compared to the damage costs.

Numerous parameters determine the costs: vehicle device cost with installation, detection equipment cost, communication network cost, operating cost, service providers cost (in any case, the annual subscription), as well as the additional costs spent by the law enforcement agencies. On the other hand, the benefits parameters concern: impacts on recovery rate and response/recovery time, arrest rate, theft rate, economic benefit for insurance companies, carriers, consumers, and for authorities, the improvement of security by the reduction of crime.

It would be very difficult to quantify each of these parameters considering the number and complexity of the factors involved and the fact that many are not easily measurable. Moreover, the cost/benefit parameters differ according to the type of after-theft systems operated and depend on regulation, law and procedures in place in each country. For information, the following cost scale of the device on vehicle is given for each type or technology of after-theft systems:

- Active tag for short range operations: 10 - 30 Euro
- Vehicle device for location by homing: 100 - 300 Euro
- Vehicle device for location by geographic position: 300 - 1,000 Euro
- Others vehicle specific devices: > 1,000 Euro
6. IMPLEMENTATION ISSUES, CONCLUSIONS AND RECOMMENDATIONS

General conclusions

The report examines the extent to which the road haulage industry is using modern technology to combat the risk of theft of vehicles and goods.

Practically all new commercial vehicles are equipped with anti-theft devices. Increasingly vehicle alarm systems and tracking systems are also being fitted. The range and sophistication of available equipment is increasing rapidly and the information to hand indicates a steady take up in this equipment. However, it is not possible to evaluate the cost effectiveness of the equipment used since there is not enough evidence on the extent of crime, on whether the equipment used actually foiled determined theft attempts or contributed to recovering goods once stolen.

The evidence that vehicle crime is increasing, implies that it is necessary to improve security and to reduce barriers to the introduction of systems that can contribute to lessening the risks.

The information in Chapter 4 and especially in Chapter 5, shows the promising possibilities offered by new technology. Introducing these technologies faces obstacles of several kinds: technical (standardisation, performance characteristics), economic (cost and especially benefits are very difficult to calculate), institutional (many agencies involved, different implications for each of them), public policy (privacy, coordination of institutions).

The need for, and level of security that is appropriate varies due to the nature of the goods carried and the routes used. There is, therefore, no need for a uniform level of anti-theft protection. For example, companies transporting valuable goods often take two drivers or use GPS and other special devices. Some insurance companies insist on particular levels of security in particular cases; others have scales of protection depending on the value of the loads concerned. Operators themselves are often best placed to decide on the level of protection that is appropriate. But sometimes, operators are not aware of the risks and are careless. Criminals too are always looking for new opportunities.

Fitting anti-theft devices to vehicles and developing after-theft systems are only parts of a broader strategy to combat road freight transport crime. Such a strategy is necessarily complex, partly because it involves many actors. In this regard it is widely agreed that there is a need for all those concerned to work more closely together to prevent thefts and to help to recover vehicles and goods if they are stolen.

There is an important role for the authorities in co-ordinating anti-crime activities, in providing a consistent framework for operators, in setting clear guidelines to manufacturers and others, and in working together to reduce the likelihood of crime and to solving it when it occurs.

While all are agreed on the need for more co-ordinated measures, there is not yet a full consensus on these measures or on the roles of the different actors. This report then should be seen as a contribution to work that needs to continue.
6.1 The role of transport authorities and ministries

Transport ministries are one of the actors involved and they can play an important role in several areas. These are set out below:

- **Set quantified targets for goods vehicle crime reduction**

  This is not simple, since neither the extent of crime nor the cost of reducing it are known with any precision. Nevertheless, quantified objectives can drive policy and help ensure that resources are made available.

  While such a target depends on individual circumstances, and obviously must be set in conjunction with the police and other actors, it is suggested that a target along the lines of reducing goods vehicle related crime by 50% in 5 years is both challenging and feasible.

- **Set up partnerships and closer co-operation with authorities and actors**

  A clear conclusion of this work is that more coordination and closer cooperation is needed between different groups which have, after all, the shared aim to reduce vehicle related crime.

  There are many possibilities for such improved cooperation including with interior ministries, the police, operators, insurance companies and manufacturers. An essential starting point should be to create a coordination and contact point in the Ministry to deal with the topic. Without this, the different efforts and initiatives risk to be inefficient.

- **Accelerate standardisation of equipment and markings/accreditation**

  For heavy goods vehicles there are no legal requirements to fit specific alarm equipment. At present only a Vehicle Identification Number (VIN) is required. New cars and small trucks are required to be fitted with immobilisers and alarms (EU Directive 95/56 and UN/ECE Regulations Nos. 18 and 97.). There is a voluntary provision in this directive to fit Vehicle Alarm Systems (VAS) and some manufacturers are now doing this. There is discussion underway on extending this Directive to trucks. This is a logical extension of the present rules and it would seem appropriate that it be applied to heavy vehicles too.

  There is also discussion on whether identification of vehicles should be extended to key vehicle components. Police favour this as vehicles are often broken into parts for resale, while manufacturers oppose it on the grounds of extra cost. On balance, the identification of a small number of specific parts should not pose a severe cost burden and could be of significant benefit. The recommendations made by the Council in 1997 on this topic still need to be implemented and work should be intensified here. Discussion on this should continue.

  Technical work on after-theft devices is going on, in the European Standardization Committee (CEN) and elsewhere and should be followed and if possible, accelerated.

  Another issue is accreditation, whereby, once a specification has been agreed, the systems should be accredited by approved testing centres. Each such center should test the equipment to agreed criteria. Approved equipment and testing organisations should be accredited to international standards where they exist.
Aftermarket installation engineers should also be accredited for quality of installation. Random checks need to be carried out by accredited inspectorates to ensure that installations are being carried out to the required standard.

For example, in the U.K. the VSIB (Vehicle Security Installation Board) and Mobile Electrical Security Federation (MESF) currently operate a code of practice for aftermarket security installation. The Freight Transport Association (FTA) carries out random checks on aftermarket installation. The interested companies have been working with the DETR (Department of the Environment, Transport and the Regions) since 1997 with a view to changing legislation with reference to immobilising a vehicle when the ignition is in the ‘on’ position.

- Improve safe parking areas.

The second edition of the joint IRU-ECMT booklet on safe parking areas has just been published. There is a need to continue to improve these parking areas and indicate the degree of protection provided (for example by a star or grading system). Each Ministry, in co-operation with the profession and the Police authorities might examine the areas indicated in their territory to see what further steps need to be taken. In the UK such a verification was undertaken and showed that none of the indicated parking places met the security standards of the UK police guidelines for parking. Agreed guidelines for such parking places could be drawn up.

- Provide advice to operators

Together with the Police and the operators associations, the transport Ministry should provide guidance and advice on safe routes, safe parking, precautions to take, equipment and advice on agency drivers. Co-operation with the police on risky locations or routes, on dubious companies or staff is often very limited and could easily be improved.

As security in general improves the way criminals operate will probably change. Vehicles fitted with an immobiliser will be more difficult to steal. It is likely that criminals will therefore target vehicles in transit, because the immobiliser has already been deactivated. There is therefore a risk that the amount of hi-jack related thefts will increase. Consideration should be given on how best to prevent this type of crime.

- Lobby police

In most countries the police give very few resources to dealing with goods vehicle crime. Transport Ministries need to campaign with their colleagues in other departments for more police attention and resources to be given to monitoring vehicle crime, to preventing it and to solving it. The creation in the UK of a Joint Action group on lorry theft is an example that other countries might consider following.

- Examine incentives at international level

Other initiatives could be studied, for example, the idea that vehicles benefitting from the ECMT multilateral quota would be of a high standard of security.

The discussion indicated that a technical requirement to fit specific devices to vehicle using the quota would be complicated because the appropriate equipment would be difficult to define and also because of the problem of verification. Nevertheless, the idea is consistent with the principle in the multilateral quota that the vehicles used should be the best quality available. Further study of this issue could be continued in the ECMT Road Transport Group.
There is also a proposal that countries with a good security record might be given a bonus in the number of licences distributed. While this is also consistent with the political wishes of Ministers, there are practical problems to implement this idea including the poor quality of data on crime, but it could be pursued in ECMT’s Road Transport Group.

6.2. Role of other actors

6.2.1 Operators

In addition to fitting appropriate equipment, operators can do a lot to reduce the risk of crime. The vehicle driver, the transport company’s employees and depot security all must be considered, together with route selection and secure overnight parking facilities.

Security advice to drivers (raising awareness). In addition to the use of anti-theft devices to combat transport crime, education of drivers could reduce crime. Training schemes in which drivers are made aware of the risks to their cargo, the vehicle and themselves could help to reduce the problem. Each driver needs to be aware of how they can improve the level of security for their vehicle.

If a driver was made more aware of the danger, and was encouraged by his company, through training initiatives, to check the load at regular intervals, the likelihood of ingress of illegal immigrants into the vehicle would be reduced. Drivers should also be supplied with details of accredited sites for overnight stops. They should be encouraged to plan routes that will allow them to avoid known risky parking areas.

Employee security and agency drivers “Code of conduct”. A further area in which the road transport industry might be encouraged to make changes is with regard to the people they employ. A driver will often be chosen to deliver loads without any consideration to prior record on security matters. For example, a driver who has been the victim of theft more than once, due to poor personal security, could still be commissioned to transport valuable cargo.

However, if a record of employee security is kept, drivers who have previously exhibited low levels of security could then be limited to transporting goods of a lower value. Vice versa, the driver with excellent records of personal security could be commissioned to transport goods of high value. This type of record could be linked-in closely to driver training initiatives previously mentioned.

As some companies rely on obtaining drivers from agencies, this type of information could be kept by these as well. The agency could provide a suitably security cleared driver to match the value and importance of the cargo. This is beneficial to both the haulage companies and the agency; the company will be safe in the knowledge that the driver hired will have appropriate training to transport specific goods. The advantage to the agency is that good practice will instill customer loyalty.

In addition, agencies should be encouraged to set a code of conduct with regard to transport safety. This should take on board all the basic good practices for high security, and all drivers should then be required to follow them. The power of educating drivers to the risks, and then informing them of good practice, should not be overlooked. It is possibly the most cost-effective method of reducing crime.

Depot security - In addition to the direct threat to the goods vehicle whilst on route, further potential weakness are the depot, and ports. Whether the target of the crime is the vehicle itself or the goods to be transported, the depot is often a thieves paradise where the vehicle will be left almost completely unattended. In addition to the low levels of security that can exist at depot sites, there is also the
added incentive to the thief if it is in a sparsely populated location for example on an industrial estate. Low levels of security combined with the location can often allow thieves easy unhindered access to valuable goods and vehicles. This problem can be addressed however.

One deterrent for the criminal in this type of situation is the use of CCTV (Closed Circuit Television Cameras). For individual depots to install CCTV and then provide surveillance teams to watch the monitors twenty-four hours can be expensive.

However, one solution to this problem could lie with local governments and authorities. Most industrial areas are linked in some way to a local scheme of CCTV operations, so it is possible that local authorities and transport companies could be encouraged to work together to set up twenty four hour surveillance. This could prove to be cost-effective for not only the company involved but also the local government who might be able to utilise some form of payment incentive to allow the company to participate in such a scheme.

For example, if the company supplies the cameras on their site, and is then linked up to the town surveillance monitoring, the local authority could charge a small fee to incorporate the depot into the scheme.

To further encourage good security practice within depots and ports, schemes in which depots of high security standards are recognised could be developed. This type of scheme could facilitate centers of excellence and allow transport companies to access data as to which depot site is of high security and which is of low. This type of Bench mark could work in two ways, drivers and companies will be encouraged to store their vehicles and goods on recognised sites – thus reducing the chance of criminal activity, and secondly, depot and port managers themselves will have an incentive to increase security in order to keep and encourage business at their particular site.

The advantage could be further extended for the industry with the help of insurance companies. If insurance companies recognised a quality mark given to secure depot sites, they could reduce premiums for companies using such sites, again reducing the cost for the company and individual drivers. The IRU-ECMT safe parking areas could develop in this sense.

6.2.2 Vehicle manufacturing industry

Legal requirements for security on goods vehicle are not particularly demanding. Vehicles are equipped with a VIN number. In practice, most are equipped with anti-theft devices which conform with EU Directive 95/56/EC or the equivalent UN/ECE Regulation Nos. 18 and 97 though it is not a legal requirement to fit such equipment. There does not seem to be competition among manufacturers on the basis of security features. Manufacturers believe that operators are the best judge of what is needed and they, therefore, oppose legal requirements for additional security.

Industry would prefer to see first more agreement from operators and insurance companies, for mutually recognised and harmonized systems. They could then be in a position to fit systems which would reduce costs and engineering efforts.

The police authorities have requested that some additional measures be adopted to improve security. Police believe that the VIN should be mounted in a fixed and clearly visible place and moreover they have asked that major components be marked also. Industry has opposed these proposals because of the cost. But these costs are extremely small compared to the cost of the components and further discussion on this would seem to be justified.
Manufacturers believe that only minimum regulations are needed i.e. the extension of the scope of Directive 95/56/EC to commercial vehicles. The Directive will then provide for the mandatory application of immobilisation systems.

The recommendation along these lines in ECMT Resolution 97/2 has been implemented by vehicle manufacturers by already voluntary fitting immobilisers according to Directive 95/56/EC and to UN/ECE Regulations Nos. 18 and 97.

6.2.3 Insurance industry

All vehicles and goods need to be insured. Insurance is a key cost component for shippers and operators. Operators claim that there is often no benefit in fitting costly anti-theft devices since there is no reduction in the insurance premium. Insurance companies dispute this and argue that reductions are given but that there is a time lag which depends on achieving a reduction in theft. In any case, insurance companies have an important role and could contribute more actively in several ways, including providing more information on the subject and in giving advice to operators.
Annex 1
(Refers to Chapter 5.2 “Short Range Systems”)

VEHICLE IDENTIFICATION SYSTEMS

1. Source of Information

The German “Verband der Automobilindustrie” (VDA), in which all German car manufacturers are represented, has issued a common paper on Identification Systems, see [2]. The following passages are taken from that paper. Some items were adapted to the special requirements of HGV’s.

2. Goal, Motivation

Electronic identification is one of the cheapest after theft means for the recovery of stolen vehicles. We believe that every European car, truck and trailer as well as construction machinery should be capable of being identified by a secure identification device. In order to recognize stolen vehicles before crossing borders, vehicle-internal transponders in connection with reading equipment form a powerful means of detection.

3. Scope of application of the transponder

3.1. Main application: Identification of vehicles

Reading the VIN and other important identification parameters
Read / write vehicle’s status information (“stolen”, “suspected to be stolen”).

3.2. Optional applications

“Private” identification: (e.g. entrance-/ exit control at car works, haulage companies, vehicle rental organizations...)

3.3. Additional security measures

The transponder should preferably have a vehicle internal interface, connecting it to all relevant Electronic Control Units (ECU’s). At time of manufacture, all ECU’s are announced to each other. Consequently, other ECU’s will rely on the existence of the transponder. In case of destruction or tampering, they will refuse to work correctly. Conversely, if such a transponder is demounted in one vehicle and afterwards installed into a different one, the transponder sets itself a “stolen status” bit, because it does not recognize the other “well-known” ECU’s. From that time on, the vehicle is marked to be stolen or presumed to be stolen and can easily be “filtered out” at borders or other check points.
4. **Transponder properties**

4.1. **Vehicle speed**

Since this specification was developed having passenger cars in mind, the speed up to which the transponder must be capable of being read was specified at up to 250 km/h. This will of course cover HGV’s requirements in any case.

4.2. **Data lengths to be transferred**

The whole protocol comprises four data transfers:

1) 8 bytes from the reader to the vehicle (Random number)
2) 33 bytes from the vehicle to the reader (encrypted VIN, stolen byte, authentication value)
3) 5 bytes from the reader to the vehicle (updated stolen byte, authentication value)
4) 5 bytes from the vehicle to the reader (confirmation of action)

These are tentative minimum data which shall be demonstrated by a prototype. Some delays encountered both in the transponder and the reading device will be inevitable due to encryption.

4.3. **Electrical power management**

4.3.1. **Vehicle in motion**

When the vehicle is in motion, the vehicle battery may supply the transponder. Hence, an active operation (i.e. sending out data using a high power source) is the recommended operation mode: The covered distance and consequently the necessary transferable data length is reached at full speed.

4.3.2. **Parked vehicle**

When the vehicle is parked, the relative speed between the reading device (e.g. in the hands of a policeman) and the vehicle is approx. zero and the distance to be covered will normally be less than 3 meters.

When the vehicle is parked, the transponder should have an extremely low (i.e. « 1 mA) power consumption ("sleep mode"), drawing power preferably only from its own internal battery. Only the receiver and the wake up circuitry are powered.

After having detected the external wake up request, the transponder switches from sleeping mode to the active mode (or a low power active mode), since it is only powered by its internal battery and the reading distance is limited.

The transponder internal battery may consist of a primary cell or preferably an accumulator which can be reloaded when the vehicle is in motion.

The transponder should be able to respond to a reader at least for the duration of three months when the vehicle is parked and receives no power supply from the vehicle battery, and when it is interrogated 100 times a day.
5. Frequencies to be used

Ideally, the frequencies must be legally usable in all European countries. This applies for the so-called Industrial, Scientific and Medical frequency bands (ISM).

- Wake up: This is under discussion: it may be advisable to use the 130 kHz band or the 6,78 or 13,56 MHz (or a higher ISM frequency) if an inductive or radio wake up principle for parked vehicles is used. (The permissive radiated power is highest in these bands). But, the normal operating frequency for data transmission (see below) may be specified as well, if a wake up receiver with very low power consumption can be realized.

- Taking into account the high vehicle speed together with a collision protocol (see section 6.5), a bandwidth of at least 100 kbit/s is necessary. Hence, the only ISM frequencies which fulfill this requirement are 2,45 and 5,8 GHz.

6. Miscellaneous Requirements

6.1 Operating range

When the vehicle is in motion, the operating range should be in the order of at least 10 meters. The real requirement is that on a multilane road, like on highways, different vehicles must be capable of being identified from roadside equipment.

When the vehicle is parked, the operating range should be in the order of at least 3 m.

6.2 Bandwidth and data transfer rate

Rough calculations taking into account the data lengths, transmission range, maximum vehicle speed, encryption/decryption times, and collision protocol capability resulted in data transfer rates of 100 kbit/s minimum.

6.3 Location of antennae

The envisaged location for the antennae is still under discussion. Since no directional characteristics are required, the antenna needs not to be located at the windshield. Hence, the antennae can be hidden in the vehicle.

6.4 Self destruction

The transponder should be constructed and fixed to the vehicle in such a way that removal leads to self destruction. In case of electronic tampering, the transponder should set a “tamper bit”, which is part of the stolen byte.

6.5 Collision protocol

Since it is inevitable that more than one vehicle is within the reading distance of a reader, a collision protocol (like the Aloha protocol or a derivative thereof) must be used to solve the collision problem.
6.6. **After sales market**

The transponders should be capable of being retrofitable to existing vehicles.

7. **Readers**

Readers may be stationary (at borders, harbors, other strategically chosen points) or hand held. Basically, they interrogate transponders and display the read data, like the VIN. But additionally, they may contain a data bank with a list of stolen vehicles. In that case, they will compare the transponder information with the data bank and make an alarm if a vehicle was detected which was reported to be stolen. Also, the readers must be able to write into the transponder the “stolen” information.

7.1. **Stationary readers**

Stationary readers will have a connection to a large police data bank containing information on all stolen vehicles in the EU and are periodically updated via a data net. This data bank may be an adapted version of “EUCARIS” as is demanded in the recommendations given in [4].

7.2. **Handheld readers**

Handheld readers must be capable of reading the vehicle’s VIN and the stolen status byte and display this information. They may or may not contain a “data bank” with VINs of stolen vehicles, depending on the type of reader.

7.2.1. **Handheld reader without data bank**

This presumably very cheap and small reader can read at least the transponder’s stolen status byte and the VIN. At least these two items should be displayed on the reader.

7.2.2. **Handheld reader with data bank**

This type of reader contains a mass storage with all vehicles reported to be stolen within the EU, i.e. approx. 2 million entries of VINs of stolen vehicles.

The reader must be capable of reading both the VIN and the stolen byte from the transponder. The reader compares the read-in VIN with the contents of its data bank and display the VIN and the result (“stolen” or “not stolen”).

Updating of its mass storage may be done via a wired connection to a computer which contains the whole data bank; or the hand held reader shall contain e.g. a pager receiver so the device may be continuously updated in the field.

8. **Encryption**

Encryption must be used throughout the system in order to prevent rebuilding of transponders and to make “eavesdropping” (tapping data transfers) useless, because the data are illegible.
9. In the case of wholesale application of the system, the bottom limit of the cost scale for the Devices on vehicle for short range systems (see conclusions of the Chapter 5.5) i.e. approximately 10 Euro should be achievable.
# Annex 2

## GLOSSARY

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV</td>
<td>Closed Circuit TeleVision cameras</td>
</tr>
<tr>
<td>CEA</td>
<td>Comité Européen des Assurances/European insurance association</td>
</tr>
<tr>
<td>CEN</td>
<td>Comité Européen de Normalisation/European Standardisation Committee</td>
</tr>
<tr>
<td>ECMT/CEMT</td>
<td>European Conference of the Ministers of Transport/Conférence Européenne des Ministres des Transports</td>
</tr>
<tr>
<td>ECU</td>
<td>Electronic Control Unit</td>
</tr>
<tr>
<td>EPCWG</td>
<td>European Police Co-operation Working Group</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>Europol</td>
<td>European Police Office</td>
</tr>
<tr>
<td>GHz</td>
<td>Giga Hertz = (10^9) cycles per second</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Groupe Spécial Mobile (often also: Global Standard for Mobile [phones])</td>
</tr>
<tr>
<td>HGV’s</td>
<td>Heavy Goods Vehicles</td>
</tr>
<tr>
<td>Interpol</td>
<td>International criminal police organization</td>
</tr>
<tr>
<td>IRU</td>
<td>International Road transport Union</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial, Scientific and Medical (frequency bands)</td>
</tr>
<tr>
<td>kbit/s</td>
<td>Kilo bit per second</td>
</tr>
<tr>
<td>LEA</td>
<td>European Law enforcement Agencies</td>
</tr>
<tr>
<td>LEO</td>
<td>Low Earth Orbit (satellites)</td>
</tr>
<tr>
<td>mA</td>
<td>Milli Ampère (unit for electrical current)</td>
</tr>
<tr>
<td>MHz</td>
<td>Mega Hertz (million cycles per second)</td>
</tr>
<tr>
<td>UN/ECE</td>
<td>United Nations/Economic Commission for Europe</td>
</tr>
<tr>
<td>VAS</td>
<td>Vehicle Alarm System</td>
</tr>
<tr>
<td>VDA</td>
<td>Verband Der Automobilindustrie (German car manufacturers association)</td>
</tr>
<tr>
<td>VIN</td>
<td>Vehicle Identification Number</td>
</tr>
</tbody>
</table>
Annex 3

REFERENCES


